ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект, дом 5,
помещение I, комната 33
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс CSP VPN Client. Версия 3.11

Руководство администратора

РЛКЕ.00004-02 90 03

22.09.2014

Содержание

1. Комплект поставки 9

2. Назначение и функции Продукта 10

3. Требования на базовые платформы и совместимость 12

4. Процесс подготовки персонального инсталляционного пакета пользователя 13

5. Подготовка рабочего места администратора безопасности 14

5.1. Контроль целостности дистрибутива 14

5.2. Инсталляция административного пакета 15

6. Атрибуты аутентификации 19

7. Подготовка инсталляционного пакета с предустановленными ключами (Preshared Keys) с помощью утилиты make_inst 20

8. Два сценария подготовки инсталляционного пакета с открытыми ключами (сертификатами) с помощью утилиты make_inst 21

8.1. Первый сценарий 22

8.2. Второй сценарий 24

9. Создание нескольких инсталляционных пакетов одновременно 25

10. Подготовка инсталляционного пакета с помощью графического интерфейса 28

10.1. Первый сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах 29

10.2. Второй сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах 30

10.3. Графический интерфейс 31

10.3.1. Формат заполняемых полей 32

10.4. Вкладка Authentication 33

10.4.1. Аутентификация при помощи сертификатов 33

10.4.2. Аутентификация при помощи Preshared Key 37

10.5. Вкладка Rules 39

10.5.1. Создание и редактирование правила 40

10.6. Вкладка IKE 44

10.7. Вкладка IPSec 46

10.8. Локальная политика безопасности 49

10.8.1. Режим автоматического формирования LSP 49

10.8.2. Режим ручного задания LSP 66

10.9. Вкладка Settings 67

10.10. Вкладка License 69

 Copyright © S-Terra CSP 2003 - 2015

10.11. Advanced project settings 70
10.12. Создание инсталляционного файла 71
10.13. Сохранение данных проекта 73
10.14. Задание расписания для правил фильтрации 74
10.15. Формат задания имен алгоритмов в файле admintool.ini 76
11. Подготовка к инсталляции CSP VPN Client 77
11.1. Подготовка ОС Windows XP Embedded к инсталляции 78
12. Инсталляция CSP VPN Client 79
12.1. Режим basic 81
12.2. Режим normal 85
12.3. Режим silent 90
12.4. Копирование контейнера при инсталляции 91
12.5. Перезагрузка операционной системы 94
12.6. Сообщения об ошибках 94
13. Регистрация пользователя 97
13.1. Интерактивный режим логина в Продукт 99
13.2. Неинтерактивный режим логина в Продукт 100
13.3. Время инициализации VPN сервиса 100
13.4. Неинтерактивный режим логина в ОС 100
14. Стартовый и регламентный контроль целостности продукта 103
15. Отображение текущего статуса Продукта 105
15.1. Изменение положения иконки текущего статуса Продукта 106
15.2. Login/Logout 107
15.3. SA Information 107
16. Деинсталляция CSP VPN Client 110
17. Восстановление CSP VPN Client 111
18. Создание локальной политики безопасности. Конфигурационный файл 112
18.1. Описание грамматики LSP 113
18.2. Структура конфигурации 119
18.3. Заголовок конфигурации 124
18.4. Структура LDAPSettings 129
18.5. Структура IKEParameters 133
18.5.1. Обработка пакетов – ретрансмиссии 137
18.6. Структура SNMPPollSettings 138
18.7. Структура SNMPTrapSettings 140
18.8. Структура TrapReceiver 141

 Copyright © S-Terra CSP 2003 - 2015

18.9. Структура SyslogSettings 143
18.10. Структура RoutingTable 145
18.11. Структура Route 146
18.12. Правила пакетной фильтрации. Структура FilteringRule 148
18.13. Структура FilterEntry 153
18.14. Структура IPsecAction 155
18.15. Структура TunnelEntry 160
18.16. Структуры AHProposal и ESPProposal 162
18.17. Структура AHTransform 163
18.18. Структура ESPTransform 165
18.19. Структура IKERule 168
18.20. Структура IKETransform 174
18.21. Структуры для аутентификации 179
18.22. Структуры AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign 180
18.23. Структура AuthMethodPreshared 184
18.24. Структура IdentityEntry 185
18.25. Структура CertDescription 188
18.25.1. Формат задания DistinguishedName (GeneralNames) в LSP 191
18.26. Работа с сертификатами 194
18.27. Примеры локальных политик безопасности 196
19. Протоколирование событий 202
19.1. Текущие настройки 202
19.2. Общие настройки 202
19.3. Действие текущих и общих настроек 202
19.4. Получение лога в Windows 203
19.5. Список протоколируемых событий 203
19.5.1. Список ошибок протокола ISAKMP 215
19.5.2. Список выполняемых действий по протоколу ISAKMP 216
19.6. Ошибки криптографической подсистемы 223
20. Мониторинг 224
20.1. Выдача статистики 224
20.2. Трап-сообщения 236
21. Требования к внешним мерам безопасности 239
21.1. Физические меры безопасности 239
21.2. Процедурные меры безопасности 239
21.3. Технические меры безопасности 240

22. Приложение 241

22.1. Утилита make_inst.exe 242

22.2. Сообщения об ошибках утилиты make_inst.exe 248

22.3. Установка СКЗИ "КриптоПро CSP 3.6/3.6R2" 251

22.4. Настройка СКЗИ "КриптоПро CSP" 251

22.4.1. Локальный ключевой считыватель 251

22.4.2. Внешний ключевой считыватель и носитель информации 251

22.5. Подключение внешних ключевых считывателей 252

22.6. Создание сертификата пользователя в “КриптоПро CSP 3.6/3.6R2”253

22.6.1. Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2" 253

22.6.2. Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6/3.6R2" 258

22.6.3. Настройка ДСЧ 260

22.6.4. Установка и настройка Удостоверяющего Центра. Создание CA сертификата 262

22.6.5. Экспортирование CA сертификата в файл 274

22.6.6. Создание ключевой пары и формирование запроса на сертификат пользователя 278

22.6.7. Экспортирование сертификата пользователя в файл 289

 Copyright © S-Terra CSP 2003 - 2015

Лицензионное Соглашение

о праве пользования «Программным комплексом CSP VPN Client» производства ООО «С-Терра СиЭсПи»

© 2003 – 2015 ООО "С-Терра СиЭсПи". Все права защищены

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного «Программного комплекса CSP VPN Client» (далее – Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Изделия, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных средств, носителей информации, кода программных комплексов, документации в печатной и электронной формах), включенных в Спецификацию Комплекта Изделия.

Изделие может использоваться только в качестве персонального Агента защиты (устанавливаться на персональный компьютер пользователя) и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Российской Федерации об авторском и имущественном праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 433 ГК РФ имеет силу договора между Конечным Пользователем и Производителем Изделия (ООО «С-Терра СиЭсПи»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный Продукт (комплекс) в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только один экземпляр Изделия и не имеет права устанавливать и использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ООО «С-Терра СиЭсПи») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Российской Федерации и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.gnu.org/licenses/licenses.html).

MS-DOS, Windows, Windows XP/2003/2008/Vista/7 являются торговыми марками компании Microsoft Corporation в США и в других странах.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

Cisco, Cisco PIX Firewall, Cisco IOS Router, CiscoWorks, CiscoWorks VPN/Security Management Solution, CiscoWorks Management Center for VPN Routers, CiscoWorks Management Center for PIX Firewall являются торговыми марками компании Cisco Systems в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young. eay@cryptsoft.com)

Другие названия компаний и Продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, Продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Российской Федерации

Общество с ограниченной ответственностью «С-Терра СиЭсПи»

124498, г. Москва, Зеленоград, Георгиевский проспект, дом 5, помещение I, комната 33

Телефон: +7 (499) 940 9061

Факс: +7 (499) 940 9061

Эл.почта: *information@s-terra.com*

http://www.s-terra.com

1. Комплект поставки

В комплект поставки CSP VPN Client входят:

Компакт-диск, на котором записаны:

- Каталог Client_AdminTool_CP
  - Дистрибутив CSP VPN Client 3.11
- Каталог Documentation:
  - Руководство администратора на Программный комплекс CSP VPN Client – CSP_VPN_Client_Admin_Guide_cp.pdf.
  - Руководство пользователя на Программный комплекс CSP VPN Client – CSP_VPN_Client_User_Guide_cp.pdf.
  - Руководство администратора на Программный продукт «С-Терра КП» – S-Terra_KP_AdminGuide.pdf.
  - Правила пользования – Rules.pdf.
  - Формуляр. (ФСТЭК России)
  - Формуляр. (ФСБ России)
  - Копии сертификатов соответствия ФСБ России.
  - Копия сертификата соответствия ФСТЭК России.
- Каталог S-Terra_KP
  - Дистрибутив «С-Терра КП».

В бумажном виде поставляются:

- Голографический специальный защитный знак ФСТЭК России.
- Лицензия на использование программного продукта CSP VPN Client версии 3.11.
- Лицензия на использование программного продукта КриптоПро CSP Driver версии 3.6/3.6R2

Получить дистрибутив продукта СКЗИ «КриптоПро CSP 3.6/3.6R2» уровня КС1/КС2 можно с сайта компании «Крипто-Про» http://cryptopro.ru/cryptopro/products/csp/default.htm, зарегистрировавшись и введя данные полученной лицензии на этот продукт.

Внимание !

Перед началом работы с Продуктом ознакомьтесь с Правилами пользования.

 Copyright © S-Terra CSP 2003 - 2015

2. Назначение и функции Продукта

Программный комплекс CSP VPN Client. Версия 3.11, функционирующий на аппаратных платформах в архитектуре Intel x86 под управлением операционных систем: Microsoft Windows XP (в том числе Embedded) SP3x86, Microsoft Windows Server 2003 (R2) SP2 x86, Microsoft Windows Server 2008 (R2) SP1 x86, Microsoft Windows Vista SP2 x86 и Microsoft Windows 7 SP1 x86, устанавливается на компьютер и функционирует в интересах одного пользователя.

Программный комплекс (далее Продукт CSP VPN Client, Продукт, CSP VPN Client) предназначен для создания защищенных соединений между клиентом VPN и другими взаимодействующими с ним доверенными шлюзами VPN и клиентами VPN, а также может выполнять роль межсетевого экрана.

Продукт CSP VPN Client выполняет следующие функции:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней
- аутентификацию пользователя и аутентификацию узла сети
- событийное протоколирование
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика.

CSP VPN Client осуществляет защиту трафика протоколов семейства TCP/IP в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Продукт CSP VPN Client использует в качестве внешней криптографической библиотеки средство криптографической защиты информации (СКЗИ) "КриптоПро CSP 3.6/3.6R2", разработанное компанией "Крипто-Про".

СКЗИ "КриптоПро CSP" реализует российские криптографические алгоритмы:

- ГОСТ 28147-89 – шифрование/расшифрование данных
- ГОСТ Р 34.11-94 – алгоритм хэширования
- ГОСТ Р 34.10-2001 – формирование и проверка электронно-цифровой подписи (ЭЦП)
- VKO ГОСТ Р 34.10-2001 – поддержка схемы открытого распределения ключей Диффи-Хеллмана [RFC4357]
- генерация случайных чисел.

 Copyright © S-Terra CSP 2003 - 2015

CSP VPN Client является продуктом для корпоративного использования в том смысле, что политику безопасности и настройки режимов этого Продукта осуществляет системный администратор или администратор безопасности предприятия.

Продукт CSP VPN Client для всех интерфейсов задает одинаковую политику безопасности.

Настройка CSP VPN Client может осуществляться с использованием продукта «С-Терра КП» версии 3.11, предназначенного для централизованного удаленного управления всей линии продуктов, производимых компанией «С-Терра СиЭсПи».

 Copyright © S-Terra CSP 2003 - 2015

3. Требования на базовые платформы и совместимость

Продукт CSP VPN Client выпущен для следующих базовых платформ:

- Microsoft Windows 7 SP1 x86
- MS Windows Vista SP2 x86
- MS Windows Server 2008 (R2) SP1 x86
- MS Windows Server 2003 (R2) SP2 x86
- MS Windows XP SP3x86 (в том числе Embedded).

Продукт совместим с криптографической библиотекой "КриптоПро CSP 3.6/3.6R2", разработанной компанией "Крипто-Про".

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4.

В части удаленного мониторинга и сбора статистики управления Продукт совместим с CiscoWorks Monitoring Center for Performance 2.0.2, входящим в состав CiscoWorks VMS 2.3.

Продукт совместим с eToken PRO32k, eToken PRO64k, eToken NG-FLASH, eToken NG-OTP, eToken PRO (Java) производства компании Aladdin.

 Copyright © S-Terra CSP 2003 - 2015

4. Процесс подготовки персонального инсталляционного пакета пользователя

Продукт CSP VPN Client предназначен для виртуальных корпоративных сетей. Полагаем, что в таких сетях пользователь не имеет права на изменение политики безопасности корпоративной сети. Поэтому, Продукт CSP VPN Client разработан таким образом, что администратор безопасности корпоративной сети формирует персонализованный инсталляционный пакет для каждого пользователя, при этом настройки для пользователя согласуются с его должностными обязанностями.

Процесс подготовки персонализованного инсталляционного пакета пользователя производится следующим образом.

Администратор безопасности получает административный пакет в виде отдельного Продукта, размещенного в каталоге Client_AdminTool_CP поставляемого диска. Администратор устанавливает на своем компьютере административный пакет, с помощью которого готовит для пользователя инсталляционный пакет.

Используя предустановленные ключи либо сертификаты открытых ключей пользователя, корневой сертификат удостоверяющего центра и локальную политику безопасности, предписанную для данного пользователя, администратор готовит инсталляционный пакет пользователя.

Создание инсталляционного пакета пользователя осуществляется двумя способами:

- использование графического интерфейса
- использование утилиты командной строки `make_inst.exe`.

Использование графического интерфейса для задания локальной политики безопасности, персональных настроек и создание инсталляционного пакета пользователя с использованием сертификатов открытых ключей либо предустановленных ключей (Preshared Keys) описано в главе "Подготовка инсталляционного пакета с помощью графического интерфейса".

Для создания инсталляционного пакета пользователя используется технология One Click Installation, которая реализуется с помощью утилиты командной строки `make_inst.exe`. Эта утилита описана в Приложении "Утилита make_inst.exe".

Технологические процессы формирования персональных инсталляционных пакетов пользователей с использованием сертификатов открытых ключей или предустановленных (разделяемых) ключей (Preshared Keys) и утилиты `make_inst.exe` описаны в главах "Подготовка инсталляционного пакета с предустановленными ключами (Preshared Keys) с помощью утилиты make_inst" и "Два сценария подготовки инсталляционного пакета с открытыми ключами (сертификатами) с помощью утилиты make_inst", соответственно.

Перед использованием утилиты `make_inst.exe` должна быть создана и записана в файл в текстовом формате локальная политика безопасности. Создание конфигурационного файла описано в главе "Создание локальной политики безопасности. Конфигурационный файл".

Пользователь, используя подготовленный для него администратором персонализованный инсталляционный пакет, производит установку Продукта CSP VPN Client на своем компьютере.

Настройка CSP VPN Client может осуществляться с использованием продукта «С-Терра КП». Дистрибутив «С-Терра КП» находится на компакт-диске в каталоге S-Terra_KP, документация на «С-Терра КП» – в каталоге Documentation.(S-Terra_KP_AdminGuide.pdf).

Далее перейдите к подготовке рабочего места администратора безопасности.

 Copyright © S-Terra CSP 2003 - 2015

5. Подготовка рабочего места администратора безопасности

Подготовка рабочего места осуществляется администратором безопасности в несколько этапов:

- инсталляция на свой компьютер СКЗИ "КриптоПро CSP 3.6/3.6R2". Установка этого Продукта описана в Приложении "Установка СКЗИ "КриптоПро CSP 3.6/3.6R2"
- инсталляция административного пакета. Описана в разделе "Инсталляция административного пакета".

Перед инсталляцией административного пакета можете убедиться в целостности его дистрибутива, размещенного в каталоге Client_AdminTool_CP поставляемого диска. Такая проверка целостности описана в разделе "Контроль целостности дистрибутива"

5.1. Контроль целостности дистрибутива

Проверка целостности дистрибутива административного пакета осуществляется с использованием утилиты `cpverify`, разработанной компанией "Крипто-Про". Утилита `cpverify` размещена в каталоге установленного продукта КриптоПро CSP. Для вычисления хэш-суммы по каждому файлу дистрибутива, например, `setup.exe`, и выдачи результата на экран выполните команду (указав пути к файлам):

```
cpverify -mk setup.exe
```

Полученное значение сравните со эталонным значением хэш-суммы, записанным в файл `hashes` из состава дистрибутива, который содержит строки вида `<hash> <file_name>`,

где

`<hash>` – эталонное значение хэш-суммы

`<file_name>` – имя файла, для которого подсчитана хэш-сумма.

Для вычисления хэш-суммы для файла дистрибутива и автоматического сравнения с эталонным значением, например, для файла `setup.exe`, выполните команду (указав пути к файлам):

```
cpverify setup.exe hash_from_file,
```

где

`hash_from_file` – эталонное значение хэш-суммы для файла `setup.exe`, скопированное из файла `hashes` (вставить в командную строку можно при помощи нажатия правой кнопки мыши и выбора предложения "Вставить").

Если проверка прошла успешно, то на экран будет выдано сообщение:
`File <product_file_full_path> has been verified.`

При обнаружении ошибки выдается сообщение:
`File <product_file_full_path> was corrupted,`

где

`product_file_full_path` – полный путь к файлу дистрибутива, на котором произошла ошибка.

 Copyright © S-Terra CSP 2003 - 2015

5.2. Инсталляция административного пакета

Администратор безопасности получает административный пакет в виде отдельного Продукта CSP VPN Client AdminTool, размещенного в каталоге Client_AdminTool_CP поставляемого диска. В состав дистрибутива этого Продукта входит:

- `hashes` – файл с эталонными значениями хэш-сумм для каждого файла дистрибутива
- `setup.exe` – утилита запуска Windows Installer
- `setup.ini` – настроечный файл, необходимый для setup.exe
- `sysdlls.cab` – хранилище системных DLL, необходимых для клиента
- `version.txt` – текстовый файл, содержащий версию Продукта
- `VPN_CLIENT_ADMIN.msi` – MSI-база инсталлятора (MSI – MicroSoft Installer)
- `VPN_CLIENT_ADMIN.cab` – хранилище файлов клиента.

Администратор должен установить административный пакет на своем компьютере.

Запуск инсталляции производится командой setup.exe из административного пакета, появляется окно визарда с приглашением к инсталляции:

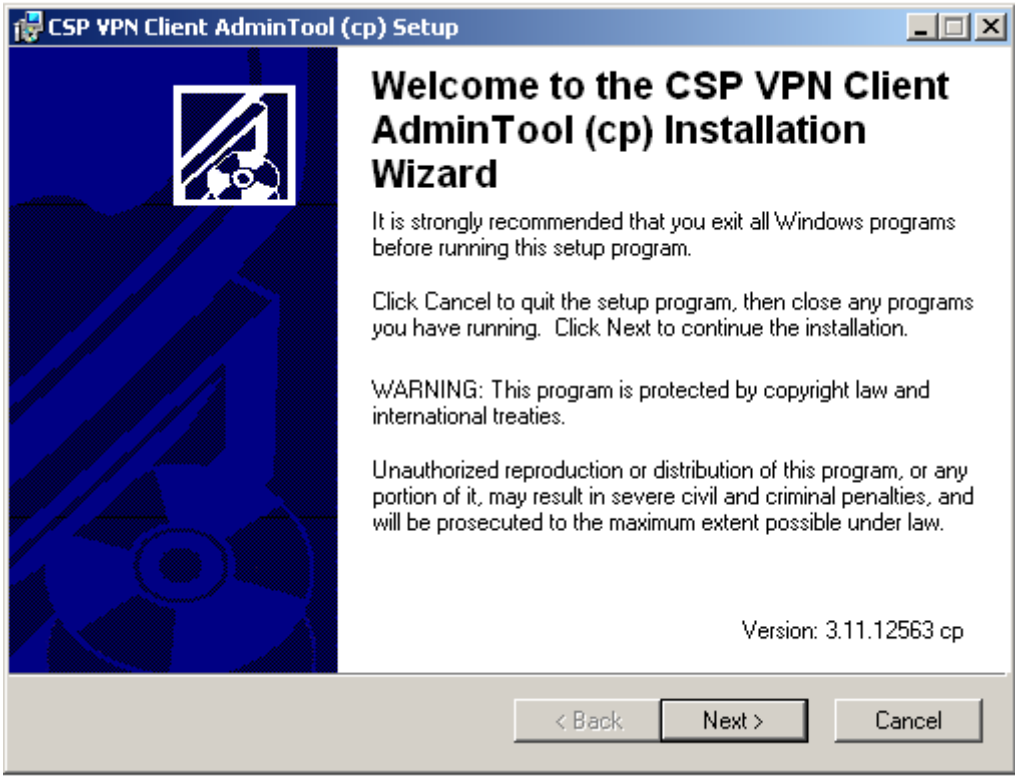


Рисунок 1

 Copyright © S-Terra CSP 2003 - 2015

В окне с текстом Лицензионного Соглашения после установки переключателя в положение "I accept the license agreement" кнопка Next становится доступной:

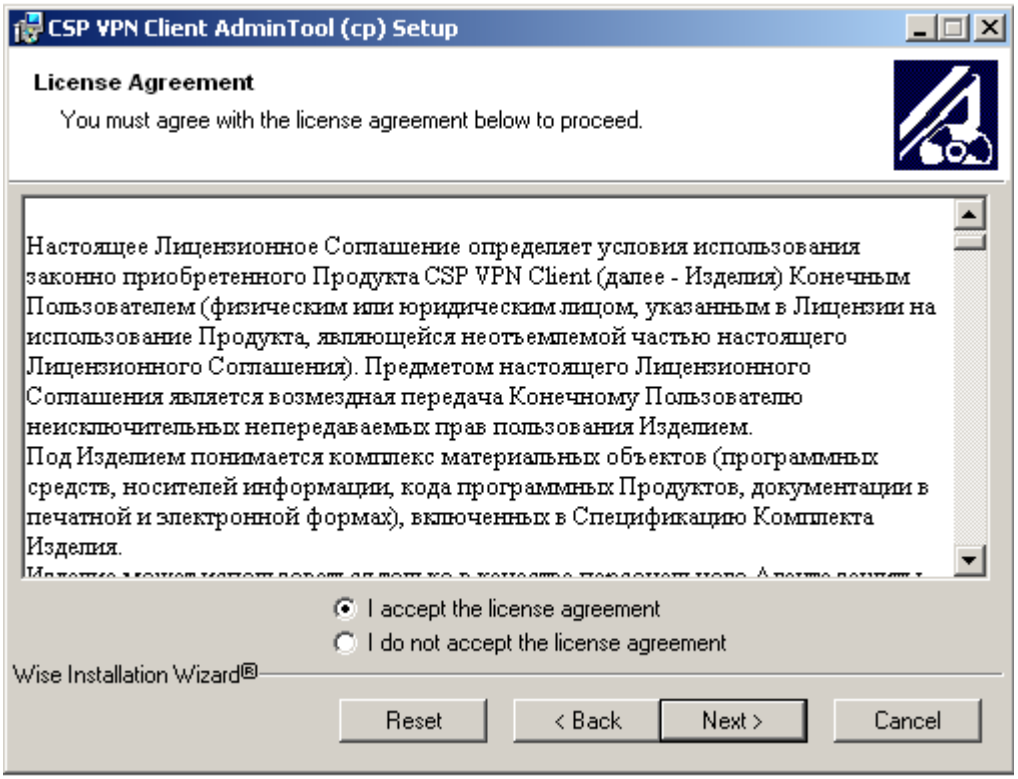


Рисунок 2

Выбрать папку, в которую будет установлен административный пакет, нажав на клавишу Browse:

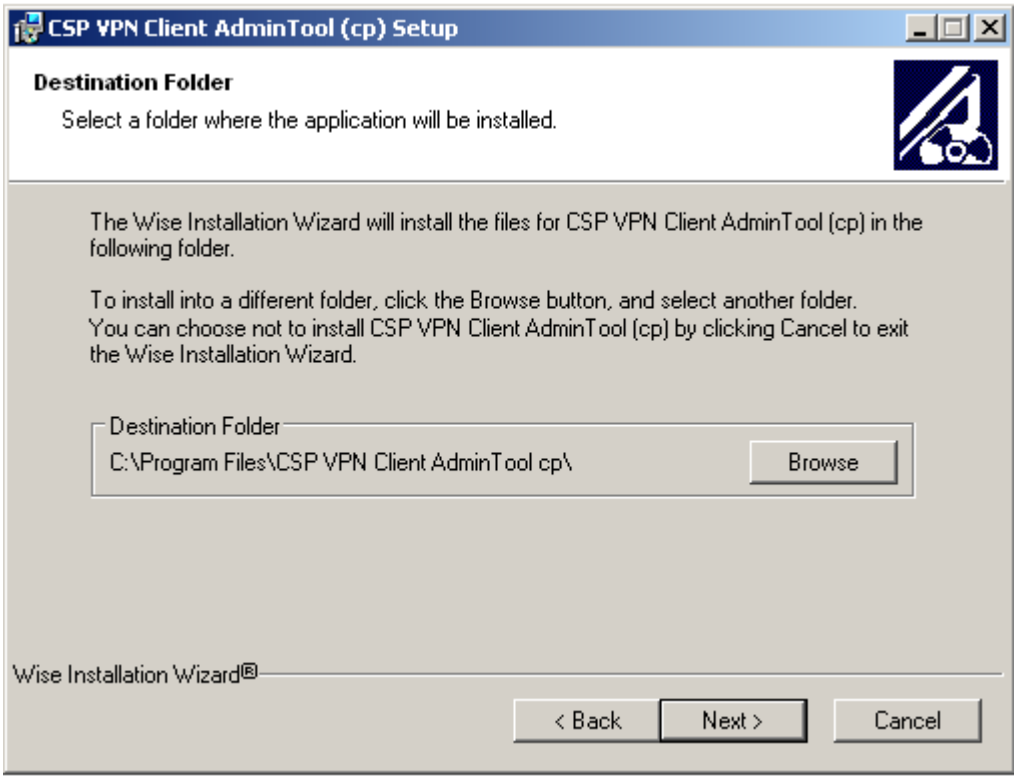


Рисунок 3

Copyright © S-Terra CSP 2003 - 2015

Для начала процесса инсталляции нажать клавишу Next:

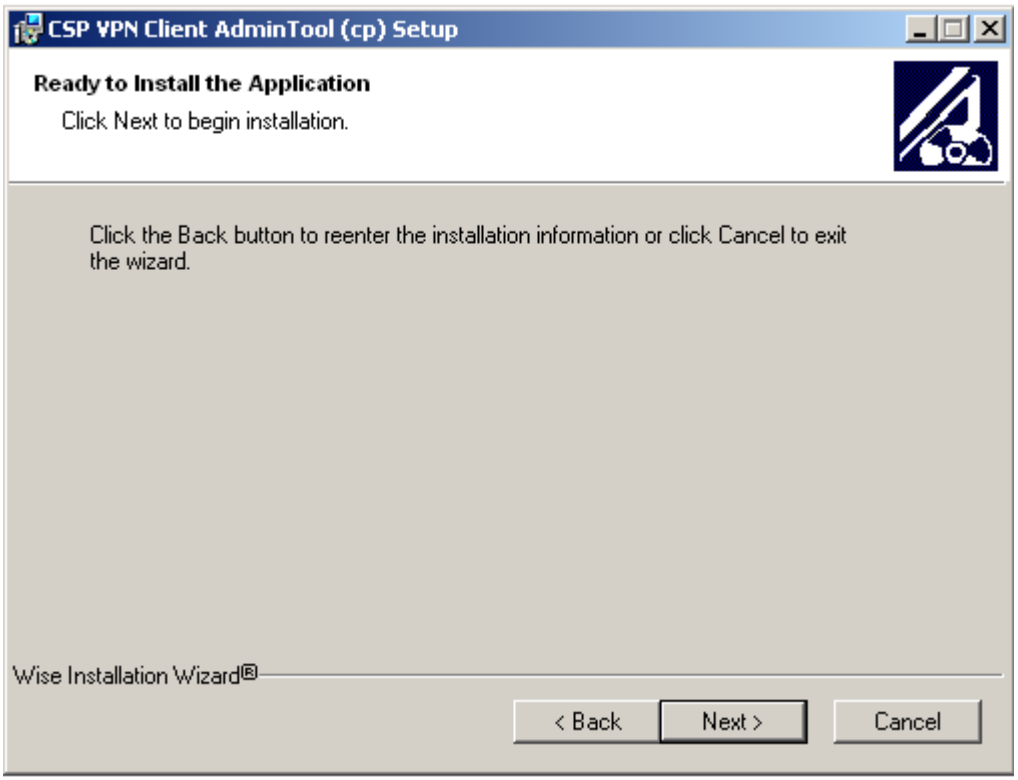


Рисунок 4

Индикатор процесса инсталляции:

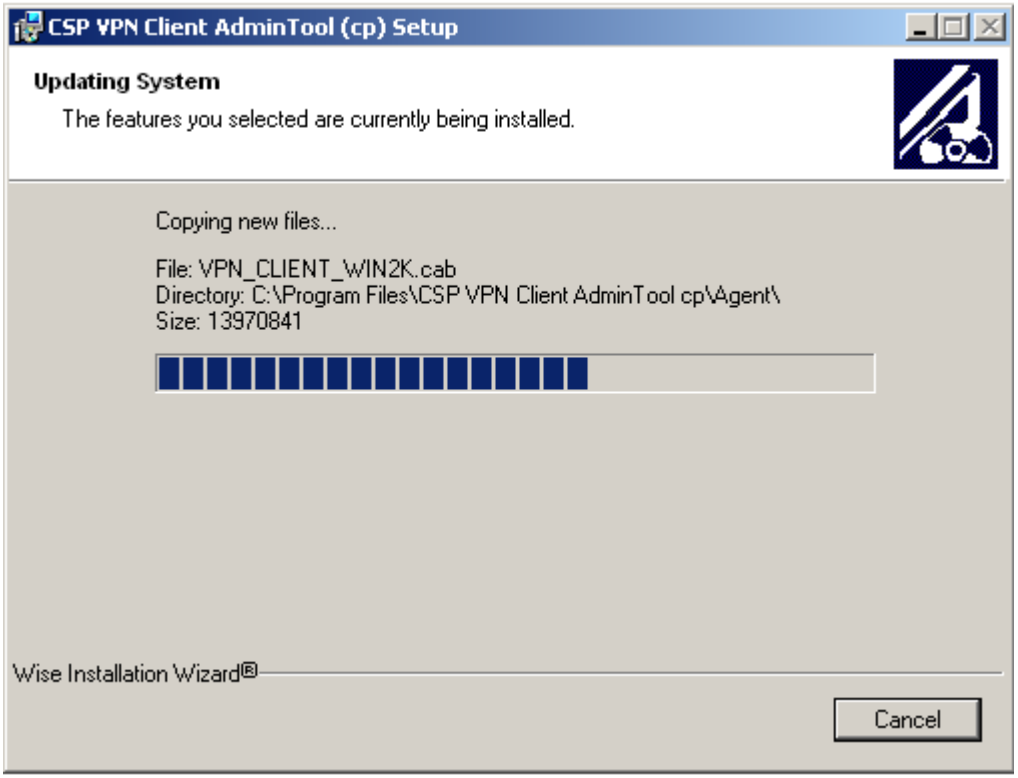


Рисунок 5

 Copyright © S-Terra CSP 2003 - 2015

Инсталляция завершена, нажать клавишу Finish:

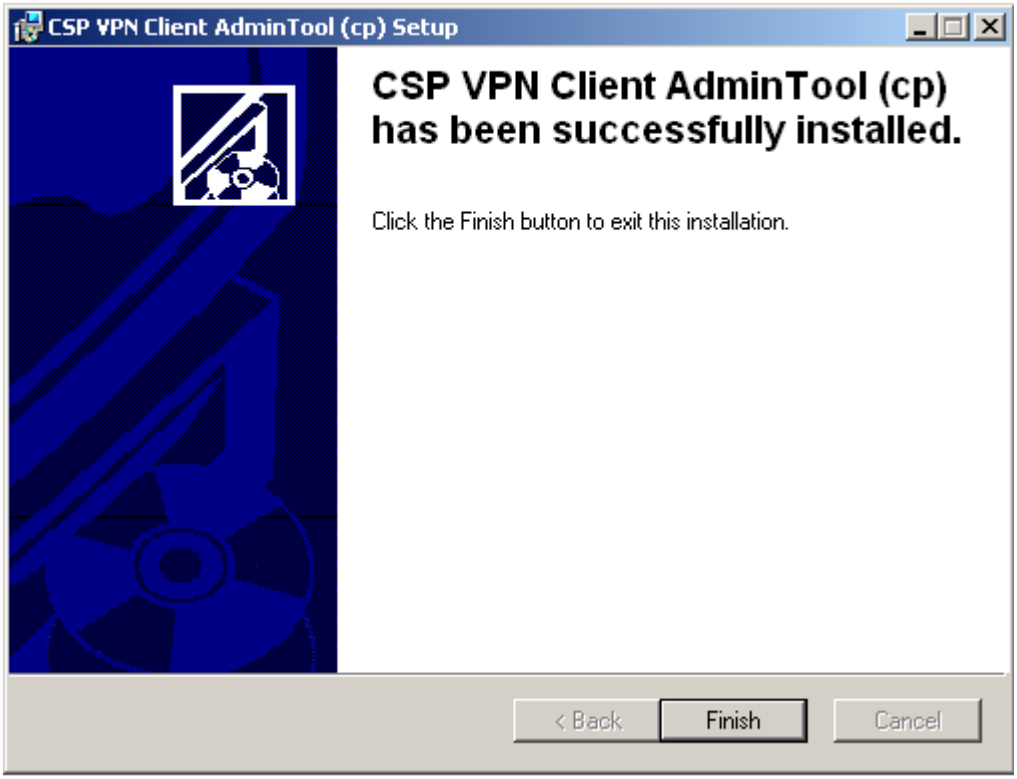


Рисунок 6

Установленный административный пакет состоит из следующих папок и файлов:

Корневая папка:

- `make_inst.exe` – утилита командной строки для создания инсталляционного файла пользователя
- `pkg_maker.exe` – утилита графического интерфейса для создания локальной политики, локальных настроек и инсталляционного файла пользователя, которая вызывает утилиту make_inst.exe
- `version.txt` – текстовый файл, содержащий версию Продукта
- `pkg_maker.chm` – файл, содержащий Help
- вспомогательные файлы (`dll, ini`) для обеспечения работы утилит.

Папка Agent содержит основные файлы инсталлятора:

- `VPN_CLIENT_WIN2K.msi` – MSI-база инсталлятора (MSI – MicroSoft Installer)
- `VPN_CLIENT_WIN2K.cab` – хранилище файлов клиента
- `sysdlls.cab` – хранилище системных DLL, необходимых для клиента

Папка SFX содержит:

- служебные файлы, необходимые для сборки SFX-архива.

 Copyright © S-Terra CSP 2003 - 2015

6. Атрибуты аутентификации

Технология IPsec обеспечивает аутентификацию, шифрование и целостность данных на уровне передаваемых IP-пакетов. Для реализации этих функций технологии IPsec необходима дополнительная информация, которая поставляется протоколом IKE: ключевой материал и согласованная политика защиты.

Для аутентификации взаимодействующих сторон протоколу IKE также необходима некоторая аутентификационная информация.

Такой аутентификационной информацией может быть:

- предустановленный (разделяемый) ключ (Preshared Key)
- сертификат стандарта X.509.

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате будут присутствовать другие расширения, не указанные в таблице и заданные как критичные, то такой сертификат не может быть использован. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, и сертификат используется.

Name	OID value
Subject Key Identifier	2.5.29.14
Key Usage	2.5.29.15
Subject Alternative Name	2.5.29.17
Issuer Alternative Name	2.5.29.18
Basic Constraints	2.5.29.19
Name Constraints	2.5.29.30
CRL Distribution Points	2.5.29.31
Authority Key Identifier	2.5.29.35

В следующей таблице приведен список критичных расширений сертификата, которые распознаются и игнорируются Продуктом.

Name	OID value
SubjectDirectoryAttributesr	2.5.29.9
CertificatePolicies	2.5.29.32
QcStatements	1.3.6.1.5.5.7.1.3
HcRole	1.0.21091.2.0.5

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (http://tools.ietf.org/html/rfc5280#section-4.2).

 Copyright © S-Terra CSP 2003 - 2015

7. Подготовка инсталляционного пакета с предустановленными ключами (Preshared Keys) с помощью утилиты make_inst

Ключ – произвольная последовательность байтов. Ключ может быть записан в файл.

Создать предустановленный (разделяемый) ключ (Preshared Key) можно разными способами. Самый простой – записать в файл любую произвольную последовательность символов.

Имя ключа – идентификатор, состоящий из латинских букв, цифр, символов `"_"` и `"-"` , и начинающийся с латинской буквы или символа `"_"`. Например, key1.

Примечание: Если предустановленный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами `0x0D 0x0A` (символ возврата и перевода каретки) и тогда при подготовке предустановленного ключа для партнера должны быть использованы эти символы.

Имя предустановленного ключа используется:

- при подготовке инсталляционного пакета пользователя
- при создании локальной политики безопасности (LSP) – в структуре AuthMethodPreshared в атрибуте SharedIKESecret.

Создание инсталляционного пакета пользователя осуществляется в несколько этапов:

- администратор безопасности или пользователь создает предустановленный ключ
- администратор безопасности определяет для пользователя локальную политику безопасности и записывает ее в файл (см. главу "Создание локальной политики безопасности. Конфигурационный файл" или "Подготовка инсталляционного пакета с помощью графического интерфейса")
- администратор безопасности на своем рабочем месте запускает команду `make_inst.exe` из каталога административного пакета. В противном случае будет выдано сообщение об ошибке. В опциях этой команды обязательно указывается имя инсталляционного файла, имя файла с LSP, имя предустановленного ключа, ключ или файл, в котором он размещен. Команда `make_inst.exe` в этом случае имеет следующие опции (подробно описана в Приложении "Утилита make_inst.exe"):

  make_inst.exe `-o SFX_file_path -l LSP_file_path -kn <Preshared_key_name> {-kv <Preshared_key_val> | -kvf <file_path_Preshared_key_val>}`

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, персональные настройки, локальную политику безопасности. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из одного инсталляционного файла.

 Copyright © S-Terra CSP 2003 - 2015

8. Два сценария подготовки инсталляционного пакета с открытыми ключами (сертификатами) с помощью утилиты make_inst

Опишем два сценария подготовки инсталляционного пакета пользователя с аутентификацией сторон на открытых ключах (сертификатах).

Секретный ключ пользователя, соответствующий открытому ключу сертификата, находится в контейнере. Контейнер имеет сложную структуру, где кроме секретного ключа содержится служебная информация, необходимая для обеспечения защиты и целостности ключа. Этот контейнер не является каталогом файловой системы. Контейнер может находиться на локальном ключевом носителе (Реестре) или на каком-либо внешнем ключевом носителе, например, дискете, электронном ключе eToken и др. Контейнер с секретным ключом должен быть уровня компьютера.

Сценарии отличаются тем, кто создает ключевую пару для локального сертификата пользователя и на каком ключевом носителе размещен контейнер с секретным ключом пользователя, возможна или нет проверка соответствия сертификата пользователя и секретного ключа, копируется или нет контейнер с секретным ключом во время инсталляции на компьютере пользователя.

 Copyright © S-Terra CSP 2003 - 2015

8.1. Первый сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя производятся администратором CA. При этом контейнер с секретным ключом записывают на внешний ключевой носитель, например, дискету или eToken. Инсталляция считывателя описана в разделе "Инсталляция внешнего считывателя и ключевого носителя в “КриптоПро CSP 3.6/3.6R2".

В этом сценарии возможна проверка соответствия сертификата пользователя и секретного ключа во время создания инсталляционного файла, а также копирование контейнера с одного носителя на другой, например, в Реестр во время установки инсталляционного файла на компьютере пользователя.

Опишем действия администратора безопасности по этому сценарию:

- администратор безопасности получает от администратора CA локальный сертификат пользователя и корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), экспортированные в файлы. Ему передается и контейнер с секретным ключом на на внешнем носителе
- администратор безопасности задает для пользователя локальную политику безопасности (LSP) и записывает ее в файл (см. главу "Создание локальной политики безопасности. Конфигурационный файл")
- администратор безопасности на своем рабочем месте запускает команду `make_inst.exe`. В опциях этой команды указывается имя инсталляционного файла, путь к локальному сертификату и CA сертификату, путь к файлу с LSP, имя контейнера с секретным ключом на компьютере пользователя, , локальные настройки и др. :
  - если при подготовке инсталляционного файла не задавать проверку соответствия сертификата и секретного ключа пользователя, но задать копирование контейнера, то вызов команды `make_inst.exe` будет следующим (подробно утилита описана в Приложении "Утилита make_inst.exe"):

    make_inst.exe `-o SFX_file_path -l LSP_file_path`
    ```
    -c CA_file_path
    -u USER_cert_file_path
    -uc USER_cert_container_name
    {[-up USER_cert_container_password] |
    [-ufp file_path_USER_cert_container_password]}
    -cs Source_USER_cert_container_name
    ```
  - если при подготовке инсталляционного файла задавать проверку соответствия сертификата и секретного ключа пользователя, то в команде make_inst.exe дополнительно к указанным добавляются еще опции:

    ```
    -chksecret on
    -uac USER_cert_container_name_ADMIN
    {[-uap USER_cert_container_password_ADMIN]|
    [-uafp file_path_USER_cert_container_password_ADMIN]}
    ```
  - существуют другие дополнительные опции, например, для протоколирования событий в файл `file_log.txt` при инсталляции CSP VPN Client указывается опция:

    ```
    -a /l* file_log.txt /i
    ```

 Copyright © S-Terra CSP 2003 - 2015

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, персональные настройки, локальную политику безопасности, локальный сертификат со ссылкой местоположения контейнера с секретным ключом пользователя и CA сертификат. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из инсталляционного файла и контейнера с секретным ключом пользователя на внешнем ключевом носителе, например, eToken. Контейнер должен быть передан пользователю по заслуживающему доверия каналу связи.

Все сообщения, выдаваемые программной утилитой `make_inst` в процессе ее работы, выводятся в файл `make_inst_log.txt` (при каждом создании инсталляционного файла `make_inst_log.txt` переписывается).

 Copyright © S-Terra CSP 2003 - 2015

8.2. Второй сценарий

Создание ключевой пары и формирование запроса на локальный сертификат пользователя производятся администратором безопасности или пользователем на компьютере пользователя. При этом контейнер с секретным ключом размещается на локальном ключевом носителе компьютера пользователя. В этом сценарии невозможна проверка соответствия сертификата пользователя и секретного ключа, копирование контейнера из Реестра в этом случае не производится.

Действия администратора безопасности по этому сценарию следующие:

- администратор безопасности или пользователь на компьютере пользователя создает ключевую пару и формирует запрос на локальный сертификат пользователя. Созданный запрос посылается на сервер Удостоверяющего Центра сертификатов. При этом контейнер с секретным ключом пользователя размещается на локальном ключевом носителе (Реестре) на компьютере пользователя. Подробно этот пункт описан в Приложении "Создание ключевой пары и формирование запроса на сертификат пользователя".
- администратор CA на сервере Удостоверяющего Центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности задает для пользователя локальную политику безопасности и записывает ее в файл (см. главу "Создание локальной политики безопасности. Конфигурационный файл")
- администратор безопасности на своем рабочем месте запускает команду make_inst.exe. В опциях этой команды указывается имя инсталляционного файла, путь к локальному сертификату и CA сертификату, путь к файлу с LSP, имя контейнера с секретным ключом на компьютере пользователя, локальные настройки и др. В команде `make_inst.exe` указываются опции (подробно утилита описана в Приложении "Утилита make_inst.exe"):

  make_inst.exe `-o SFX_file_path -l LSP_file_path`
  `-c CA_file_path`
  `-u USER_cert_file_path`
  `-uc USER_cert_container_name`
  `[-skt {exchange | signature}]`
  `{[-up USER_cert_container_password] |`
  `[-ufp file_path_USER_cert_container_password]}`

  существуют другие дополнительные опции, например, для протоколирования событий в файл `file_log.txt` при инсталляции CSP VPN Client указывается опция:

  `-a /l* file_log.txt /i`

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, персональные настройки, локальную политику безопасности, CA сертификат и локальный сертификат со ссылкой местоположения контейнера с секретным ключом пользователя. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из одного инсталляционного файла.

Все сообщения, выдаваемые программной утилитой `make_inst` в процессе ее работы, выводятся в файл `make_inst_log.txt` (при каждом создании инсталляционного файла `make_inst_log.txt` переписывается).

 Copyright © S-Terra CSP 2003 - 2015

9. Создание нескольких инсталляционных пакетов одновременно

Для создания инсталляционных пакетов для большого числа пользователей одновременно предлагается использовать BAT-файлы, вызывающие в цикле утилиту make_inst.exe. Далее описаны несколько BAT-файлов типичных сценариев. На компьютере администратора должна быть создана специальная папка для файлов пользователей. В этой папке создаются подпапки, которые называются по имени пользователей. Например, папка c:\vpn_client, в ней подпапки c:\vpn_client\alice и c:\vpn_client\bob (важно, чтобы не было посторонних подпапок). В этих подпапках лежит файл localcert.crt, а также для некоторых сценариев могут лежать файлы ca.crt, lsp.txt и pwd.txt (пароль на контейнер).

Сценарий 1. В этом сценарии контейнеры с секретными ключами пользователей имеют пустой пароль. Получаемые SFX-файлы кладутся в папки пользователей под именем vpnclient.exe. В папках пользователей лежат локальные сертификаты. Используется один CA сертификат и одна LSP для всех пользователей:

```
@echo off


SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\CSP VPN Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\\container
SET LSP_PATH=c:\vpn_client\lsp.txt
SET CA_PATH=c:\vpn_client\ca.crt


for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o
%%i\vpnclient.exe -c %CA_PATH% -u %%i\localcert.crt -uc
%CONTAINER_NAME% -l %LSP_PATH%) & (if errorlevel 1 goto err)


goto :end


:err


echo An error occured
exit


:end


echo Make installations complete
```

Используются следующие настройки:

TEMPLATE_DIR – папка, в которой лежат подпапки пользователей. Путь должен быть без пробелов.

MAKE_INST_PATH – путь к утилите make_inst.exe.

CONTAINER_NAME – имя контейнера.

 Copyright © S-Terra CSP 2003 - 2015

LSP_PATH – путь к общей LSP.

CA_PATH – путь к общему CA сертификату.

Здесь и далее фраза в конце "Make installations complete" обозначает успешное завершение, а " An error occured" – что произошла ошибка.

Сценарий 2. Используется общий пароль для всех контейнеров с секретными ключами всех пользователей. Получаемые SFX-файлы кладутся в папки пользователей под именем vpnclient.exe. Каждый пользователь имеет свой CA сертификат и свою LSP:

```
@echo off


SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\CSP VPN Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\\container
SET CONTAINER_PASSWORD=somepwd


for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o
%%i\vpnclient.exe -c %%i\ca.crt -u %%i\localcert.crt -uc
%CONTAINER_NAME% -up %CONTAINER_PASSWORD% -l %%i\lsp.txt) & (if
errorlevel 1 goto err)


goto :end


:err


echo An error occured
exit


:end


echo Make installations complete
```

Новые настройки:

CONTAINER_PASSWORD – общий пароль.

Сценарий 3. Все условия аналогичны сценарию 2, но получаемые файлы кладутся в одну папку с именами username.exe (где username совпадает с именем пользовательской подпапки, например alice.exe или bob.exe):

```
@echo off


SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\CSP VPN Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\\container
SET CONTAINER_PASSWORD=somepwd
SET SFX_DIR=c:\sfx


cd %TEMPLATE_DIR%
```

```
for /d %%i in (*) do (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c
%%~fi\ca.crt -u %%~fi\localcert.crt -uc %CONTAINER_NAME% -up
%CONTAINER_PASSWORD% -l %%~fi\lsp.txt) & (if errorlevel 1 goto
err)


goto :end


:err


echo An error occured
exit


:end


echo Make installations complete
```

Здесь SFX_DIR – папка, в которую кладутся получаемые файлы.

Сценарий 4. Выполняется при тех же условиях, что и в сценарии 2, но в каждой папке пользователя дополнительно лежит файл pwd.txt, содержащий пароль контейнера для данного пользователя. Кроме того, когда каждый пользователь будет устанавливать Продукт CSP VPN Client из подготовленного для него инсталляционного файла, то он будет ставиться не в папку по умолчанию, а в папку c:\my vpn (с пробелом):

```
@echo off


SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\CSP VPN Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\\container
SET SFX_DIR=c:\sfx


cd %TEMPLATE_DIR%
for /d %%i in (*) do  (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c
%%~fi\ca.crt -u %%~fi\localcert.crt -uc %CONTAINER_NAME% -ufp
%%~fi\pwd.txt -l %%~fi\lsp.txt -a "INSTALLDIR=\"c:\my vpn\"") &
(if errorlevel 1 goto err)


goto :end


:err


echo An error occured
exit
:end
echo Make installations complete
```

10. Подготовка инсталляционного пакета с помощью графического интерфейса

Утилита `pkg_maker.exe` предоставляет администратору безопасности удобный графический интерфейс для создания локальной политики безопасности, задания настроек Продукта CSP VPN Client и создания инсталляционного пакета для пользователя.

При подготовке инсталляционного пакета пользователя с аутентификацией сторон на Preshared Keys графический интерфейс предоставляет возможность считывать созданный ключ из файла либо ввести его с клавиатуры.

Секретный ключ пользователя, соответствующий открытому ключу сертификата, находится в контейнере. Контейнер имеет сложную структуру, где кроме секретного ключа содержится служебная информация, необходимая для обеспечения защиты и целостности ключа. Этот контейнер не является каталогом файловой системы. Контейнер может находиться в Реестре или на каком-либо внешнем ключевом носителе, например, дискете, электронном ключе eToken и др. Контейнер с секретным ключом должен быть уровня компьютера.

Сценарии отличаются тем, кто создает ключевую пару для локального сертификата пользователя и на каком ключевом носителе размещен контейнер с секретным ключом пользователя, возможна или нет проверка соответствия сертификата пользователя и секретного ключа, копируется или нет контейнер с секретным ключом с одного ключевого носителя на другой во время инсталляции на компьютере пользователя.

 Copyright © S-Terra CSP 2003 - 2015

10.1. Первый сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя производятся администратором CA. При этом контейнер с секретным ключом размещается на внешнем ключевом носителе, например, eToken, дискете. Администратор безопасности получает контейнер с секретным ключом пользователя на внешнем носителе, поэтому в данном сценарии возможно провести проверку соответствия сертификата и секретного ключа на компьютере администратора, а также скопировать контейнер с секретным ключом с одного носителя на другой, например, в Реестре во время инсталляции CSP VPN Client.

Опишем действия администратора безопасности по этому сценарию:

- администратор безопасности получает от администратора CA локальный сертификат пользователя и корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), экспортированные в файлы. Ему передается и контейнер с секретным ключом на внешнем носителе
- администратор безопасности запускает утилиту графического интерфейса: Пуск – Программы – CSP VPN Client AdminTool cp –Package Maker
- с помощью графического интерфейса администратор безопасности задает для пользователя локальную политику безопасности, указывает имя инсталляционного файла, путь к локальному и CA сертификату, имя контейнера с секретным ключом на компьютере пользователя, локальные настройки и др. Администратор безопасности может выполнить настройки для проведения проверки соответствия сертификата и секретного ключа, а также для копирования контейнера. Заполнив все вкладки графического интерфейса, администратор создает инсталляционный файл. Работа с графическим интерфейсом описана в разделе "Графический интерфейс"
- созданный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, локальную политику безопасности, локальный сертификат пользователя и CA сертификат, персональные настройки. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из инсталляционного файла и контейнера с секретным ключом пользователя на внешнем ключевом носителе.

 Copyright © S-Terra CSP 2003 - 2015

10.2. Второй сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах

Создание ключевой пары и формирование запроса на локальный сертификат пользователя производятся администратором безопасности или пользователем на компьютере пользователя. При этом контейнер с секретным ключом размещается в Реестре на компьютере пользователя. В этом сценарии невозможна проверка соответствия сертификата пользователя и секретного ключа на компьютере администратора, также не проводится копирование контейнера из Реестра на другой ключевой носитель.

Действия администратора безопасности по этому сценарию:

- администратор безопасности или пользователь на компьютере пользователя создает ключевую пару и формирует запрос на создание локального сертификата пользователя. Созданный запрос посылается на сервер Удостоверяющего Центра сертификатов. При этом контейнер с секретным ключом пользователя размещается в Реестре на компьютере пользователя. Подробно этот пункт описан в Приложении в разделах "Создание ключевой пары и формирование запроса на сертификат пользователя"
- администратор CA на сервере Удостоверяющего Центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности на своем компьютере запускает утилиту графического интерфейса:
  `Start – Programs – CSP VPN Client AdminTool cp –Package Maker`
- с помощью графического интерфейса администратор безопасности задает для пользователя локальную политику безопасности, указывает имя инсталляционного файла, путь к локальному и CA сертификату, имя контейнера с секретным ключом на компьютере пользователя, локальные настройки и др. Заполнив все вкладки графического интерфейса, администратор создает инсталляционный файл. Работа с графическим интерфейсом описана в разделе "Графический интерфейс"
- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Client, локальную политику безопасности, локальный сертификат пользователя и CA сертификат, персональные настройки, Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из одного инсталляционного файла.

 Copyright © S-Terra CSP 2003 - 2015

10.3. Графический интерфейс

При запуске утилиты `pkg_maker.exe ( Пуск – Программы – CSP VPN Client AdminTool cp - Package Maker )` открывается окно главной формы.

Главная форма представляет собой диалоговое окно со вкладками, в котором можно создавать LSP, делать локальные настройки и создавать инсталляционный файл.

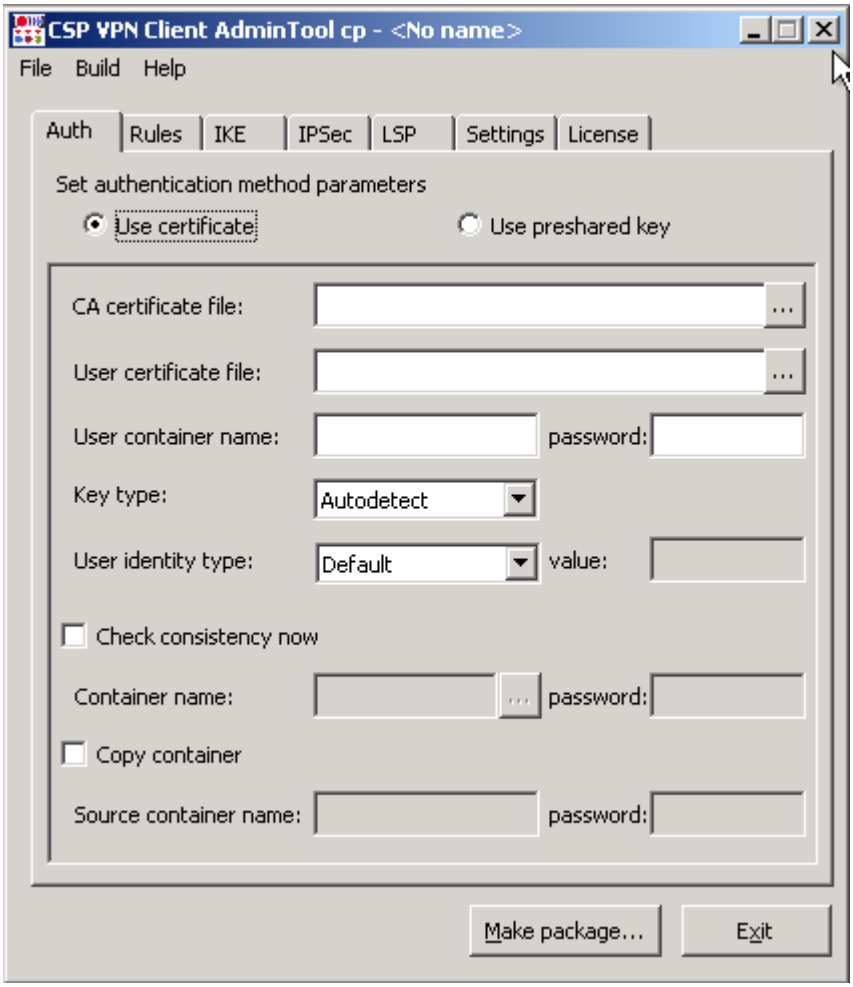


Рисунок 7

Кроме того, главная форма содержит Меню и две функциональные кнопки.

Вкладки главной формы предназначены:

- Auth – для задания способа аутентификации сторон
- Rules – для задания правил сетевой обработки трафика
- IKE – задание параметров IKE соединений
- IPSec – задание параметров IPsec соединений
- LSP – просмотр и редактирование локальной политики безопасности
- Settings – задание параметров протоколирования событий и политики по умолчанию
- License –задание параметров Лицензии.

 Copyright © S-Terra CSP 2003 - 2015

Меню содержит три раздела:

- Раздел `File` имеет следующие предложения:
  - New Project – открывает новый проект. Проект – это файл в текстовом формате с расширением dsc, в котором будет записана LSP с установленными параметрами во вкладках и локальными настройками
  - Open Project… – открывает существующий (ранее созданный) проект
  - Save Project – сохраняет текущее состояние проекта
  - Save Project As… – сохраняет текущее состояние проекта в указанный файл
  - Advanced Project Settings – вызывает окно, в котором можно указать дополнительные настройки проекта. Этот пункт меню активен, если во вкладке Auth выбран метод аутентификации сторон при помощи сертификатов
  - Exit – выход из GUI.
- Раздел `Build` имеет одно предложение:
  - Make package… – создание инсталляционного файла Продукта CSP VPN Client (аналогично кнопке "Make package...").
- Раздел `Help` имеет три предложения:
  - Contents – вызывает окно Help-системы с активной вкладкой Содержание
  - Index – вызывает окно Help-системы с активной вкладкой Указатель
  - About… – открывает окно, содержащее название Продукта, версию, номер сборки, копирайт и логотип компании.

Функциональные кнопки:

- Make package – кнопка для создания инсталляционного файла пользователя
- Exit – выход из GUI.

10.3.1. Формат заполняемых полей

Все поля графического интерфейса, в которые вводится имя папки и файла, могут содержать парные кавычки, пробелы в начале и в конце строки. Все эти символы игнорируются.

Для всех других полей любой введенный символ является значимым.

10.4. Вкладка Authentication

Вкладка Auth предназначена для выбора метода аутентификации и ввода идентификационных данных пользователя. Поддерживаются два метода аутентификации – при помощи GOST сертификата стандарта X.509 или предустановленного (разделяемого) ключа (Preshared Key).

10.4.1. Аутентификация при помощи сертификатов

При аутентификации сторон при помощи сертификатов открытых ключей поставить переключатель в положение Use certificate:

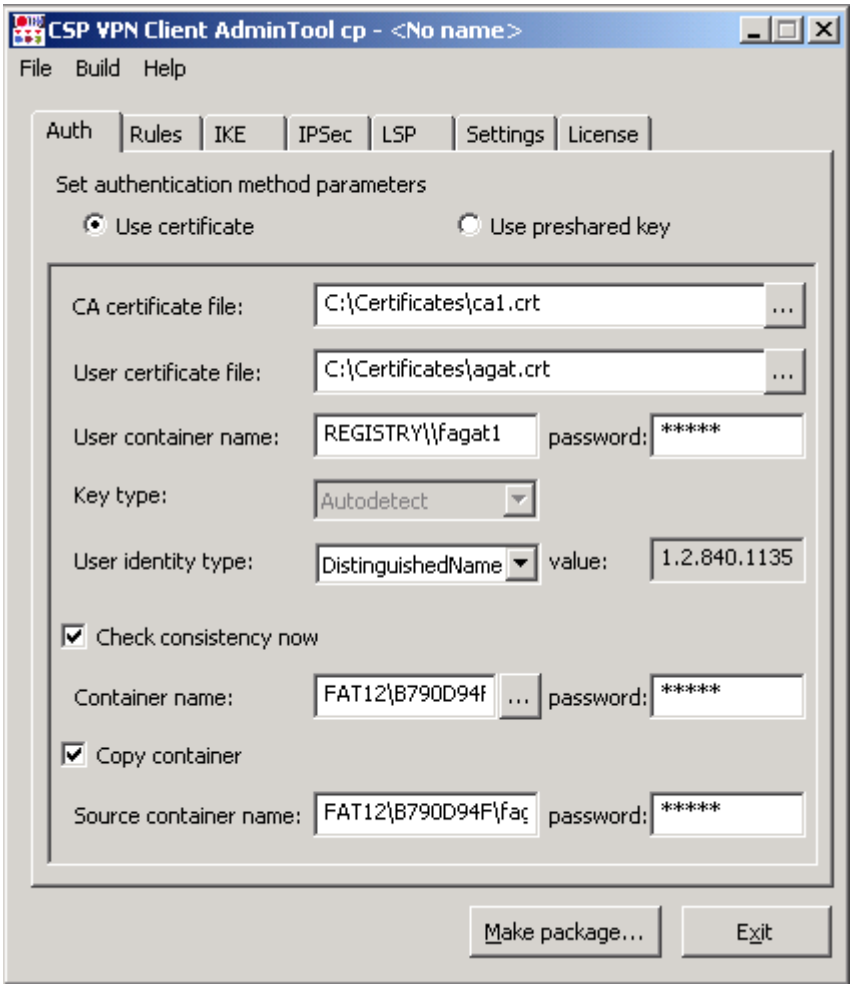


Рисунок 8

При этом становятся доступными для заполнения следующие поля:

- **CA certificate file** – поле для ввода имени файла с корневым сертификатом Удостоверяющего Центра (Trusted CA Certificate), размещенного на компьютере администратора. Имя файла включает в себя и путь к этому файлу. Обязательный параметр. Нажатие кнопки `[...]` открывает окно, в котором можно выбрать файл с сертификатом. Смотрите формат таких полей в разделе "Формат заполняемых полей".
- **User certificate file** – имя файла с локальным GOST сертификатом пользователя, размещенного на компьютере администратора. Обязательный параметр.

 Copyright © S-Terra CSP 2003 - 2015

- **User container name** – уникальное имя контейнера, размещенного на компьютере пользователя, на который будет установлен CSP VPN Client. Контейнер содержит служебную информацию и секретный ключ сертификата пользователя. Уникальное имя контейнера включает имя считывателя, имя ключевого носителя и имя контейнера. Должен быть указан тот считыватель и ключевой носитель, на котором будет расположен контейнер на компьютере пользователя. Обязательный параметр, если используется сертификат.

  Если контейнер `cont_1` находится в Реестре, то уникальное имя контейнера имеет формат:

  ```
  \\.\REGISTRY\cont_1  или  REGISTRY\\cont_1
  ```

  Если контейнер `cont_1` находится на дискете, то уникальное имя контейнера имеет формат:

  ```
  FAT12\BCD0CB6A\a12.000\C59B
  ```

  Если контейнер находится на eToken PRO32, то уникальное имя контейнера имеет, например, формат:

  ```
  SCARD\ETOKEN_PRO32_4f22aa14\CC03\BE25
  ```

  Если контейнер находится на внешнем ключевом носителе, то для указания уникального имени контейнера подключите этот носитель к компьютеру администратора и инсталлируйте его (дискету инсталлировать не нужно). Далее см. **Примечание1**.

- **User container password** – пароль к контейнеру. При использовании eToken в этом поле нужно указать PIN-код к токену
- **Key type** – тип секретного ключа, хранящегося в контейнере. Этот переключатель имеет три положения:
  - Autodetect – тип ключа будет определяться автоматически при первом обращении к контейнеру секретного ключа. Определение типа ключа основано на проверке соответствия открытого ключа сертификата пользователя и секретного ключа в контейнере. Значение по умолчанию.
  - Signature – для подписи
  - Exchange – для обмена

  В этом поле нужно выбрать тип ключа, когда не выставлен флажок Check consistency now. Если создание ключевой пары и создание запроса на сертификат пользователя производились средствами MS CA (см. Приложение) и был выбран тип ключа `both` или `exchange`, то здесь нужно выбрать тип ключа – `exchange`, а если был выбран тип `signature`, то и здесь нужно выбрать `signature`. Если администратору тип ключа неизвестен, то рекомендуется выбирать значение Autodetect
- **User identity typ**e – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
  - Default – в качестве идентификатора партнеру будет высылаться действительный IP-адрес хоста, на котором будет установлен CSP VPN Client
  - Distinguished Name – в качестве идентификатора партнеру будет высылаться значение Subject из сертификата пользователя, показываемое в поле User identity value, если оно там задано
  - Email – в качестве идентификатора партнеру будет высылаться значение поля E-mail расширения сертификата пользователя , показываемое в поле User identity value, если оно там задано

- FQDN – в качестве идентификатора партнеру будет высылаться значение доменного имени хоста, считываемое из поля DNS расширения сертификата и показываемое в поле User identity value, если оно там задано.
- IPV4Addr – в качестве идентификатора партнеру будет высылаться первый IP-адрес, указанный в расширении сертификата, и показываемый в поле User identity value, если он там задан.

- **User identity value** – идентификационная информация, пересылаемая партнеру. Поле доступно только для чтения и заполняется автоматически соответствующим типу идентификатора значением, считываемым из сертификата пользователя. Заполнение происходит в момент выбора типа идентификатора или изменения имени файла с сертификатом пользователя. Параметр обязательный.
- **Check consistency now** – установка этого флажка означает, что будет производиться проверка соответствия сертификата пользователя и секретного ключа. Такая проверка будет проведена на компьютере администратора во время создания инсталляционного файла. Для этого контейнер с секретным ключом нужно разместить на компьютере администратора.
- **Container name** – имя контейнера на компьютере администратора для проведения проверки. При нажатии кнопки […] появляется окно Container list (Рисунок 9) со списком контейнеров на всех ключевых носителях, подключенных к компьютеру администратора и инсталлированных (подключение и инсталляцию ключевых считывателей смотрите в Приложении в разделах "Подключение внешних ключевых считывателей", "Инсталляция внешнего считывателя и ключевого носителя в "КриптоПро CSP 3.6/3.6R2". В списке указывается уникальное имя контейнера, включающее считыватель, ключевой носитель и имя контейнера в hex-цифрах. Из этого списка нужно выбрать контейнер для проверки и нажать ОК. В поле Container name появится уникальное имя этого контейнера.

  Примечание 1: для указания уникального имени контейнера в поле User container name или в утилите make_inst.exe установите флажок Check consistency now и рядом с полем Container name нажмите на кнопку […] . Появится окно Container list (Рисунок 9) со списком доступных контейнеров. Скопируйте уникальное имя контейнера из этого поля. После этого флажок Check consistency now можно снять, если проверка не проводится.

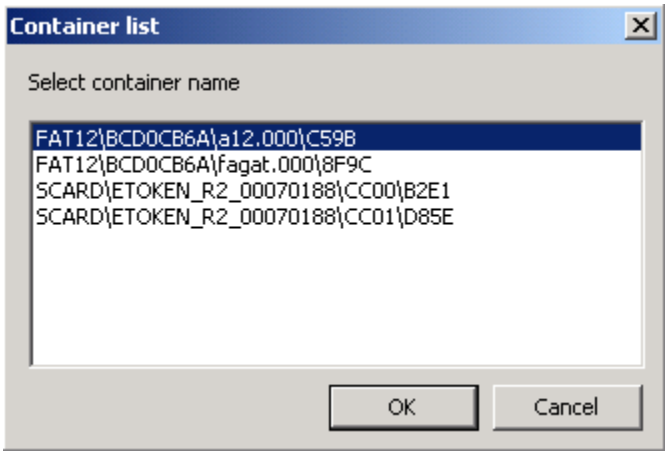


Рисунок 9

- **Container password** – пароль к контейнеру с секретным ключом
- **Copy container** – установка этого флажка означает, что во время инсталляции CSP VPN Client на компьютере пользователя будет произведено копирование контейнера с именем, указанным в поле Source container name, в контейнер с именем, указанным в поле User container name

- **Source container name** – имя контейнера на компьютере пользователя, из которого будет произведено копирование.

На Рисунок 8 вкладка заполнена для контейнера с секретным ключом с именем fagat, размещенного на дискете, и при создании инсталляционного файла будет происходить проверка соответствия сертификата пользователя и секретного ключа. А при инсталляции CSP VPN Client на компьютере пользователя контейнер с дискеты будет скопирован в Реестр с именем `fagat1`.

10.4.2. Аутентификация при помощи Preshared Key

При аутентификации сторон при помощи предустановленного ключа поставить переключатель в положение Use preshared key:

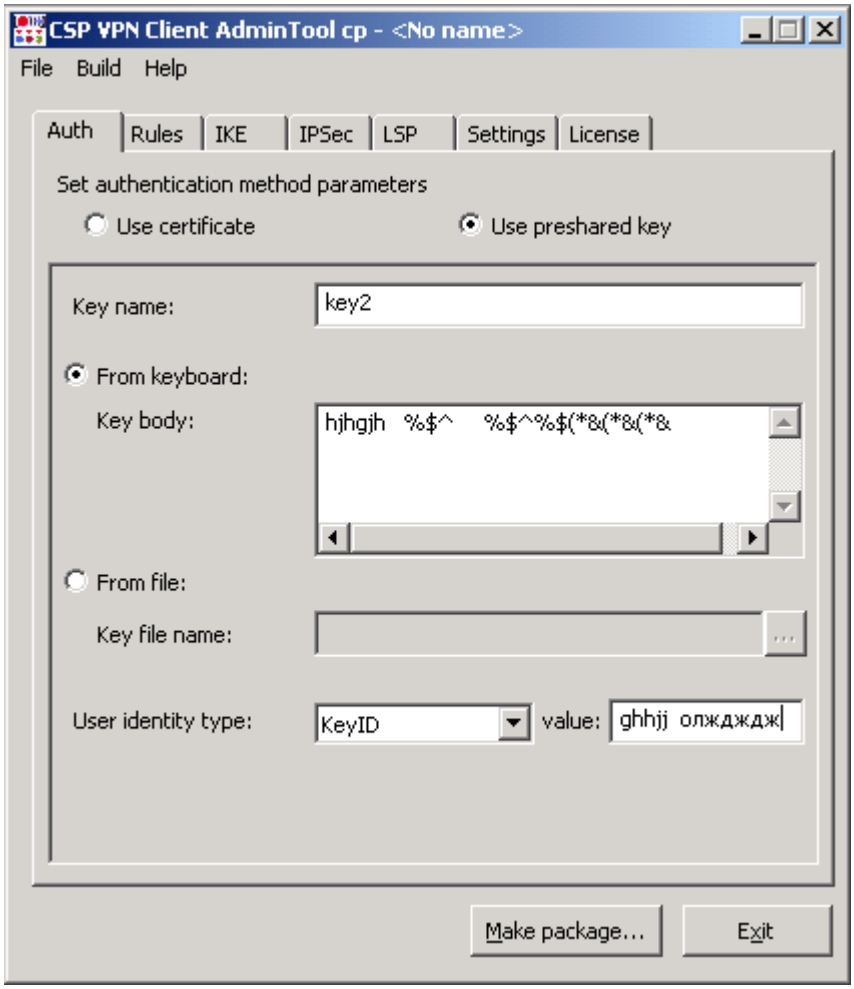


Рисунок 10

Следующие поля становятся доступными для заполнения:

- **Key name** –имя предустановленного ключа. Обязательный параметр.

Для ввода предустановленного ключа имеется переключатель с двумя положениями:

- **From keyboard** – предустановленный ключ нужно ввести с клавиатуры. Примечание: Если предустановленный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами 0x0D 0x0A (символ возврата и перевода каретки) и тогда при подготовке предустановленного ключа для партнера должны быть использованы эти символы.
- **From file** – предустановленный ключ считывается из файла с именем, указанным в поле **Key file name**
- **User identity type** – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
  - Default – в качестве идентификатора партнеру будет высылаться действительный IP-адрес компьютера, на котором будет установлен CSP VPN Client

 Copyright © S-Terra CSP 2003 - 2015

- IPV4Addr – в качестве идентификатора партнеру будет высылаться IP-адрес, который нужно задать в поле "User identity value"
- KeyID – в поле "User identity value" нужно ввести любую последовательность символов, которая может включать в себя пробелы и русские буквы. Во вкладке LSP атрибуту KeyID будет присвоено шестнадцатеричное представление заданной последовательности символов, которое и будет высылаться партнеру в качестве идентификатора.
- User identity value – значение идентификатора, вводимого вручную. Параметр обязательный.

 Copyright © S-Terra CSP 2003 - 2015

10.5. Вкладка Rules

Во вкладке Rules можно создавать, редактировать, удалять правила фильтрации и защиты трафика.

Правила нужно располагать в списке в порядке убывания приоритета. В списке должно находиться хотя бы одно правило.

При получении TCP/IP пакета правила будут просматриваться в порядке убывания приоритета и сравниваться параметры заголовка пакета, относящиеся к IP-адресам, с этими же параметрами в правиле до нахождения первого подходящего правила. Если правило не найдено – пакет уничтожается.

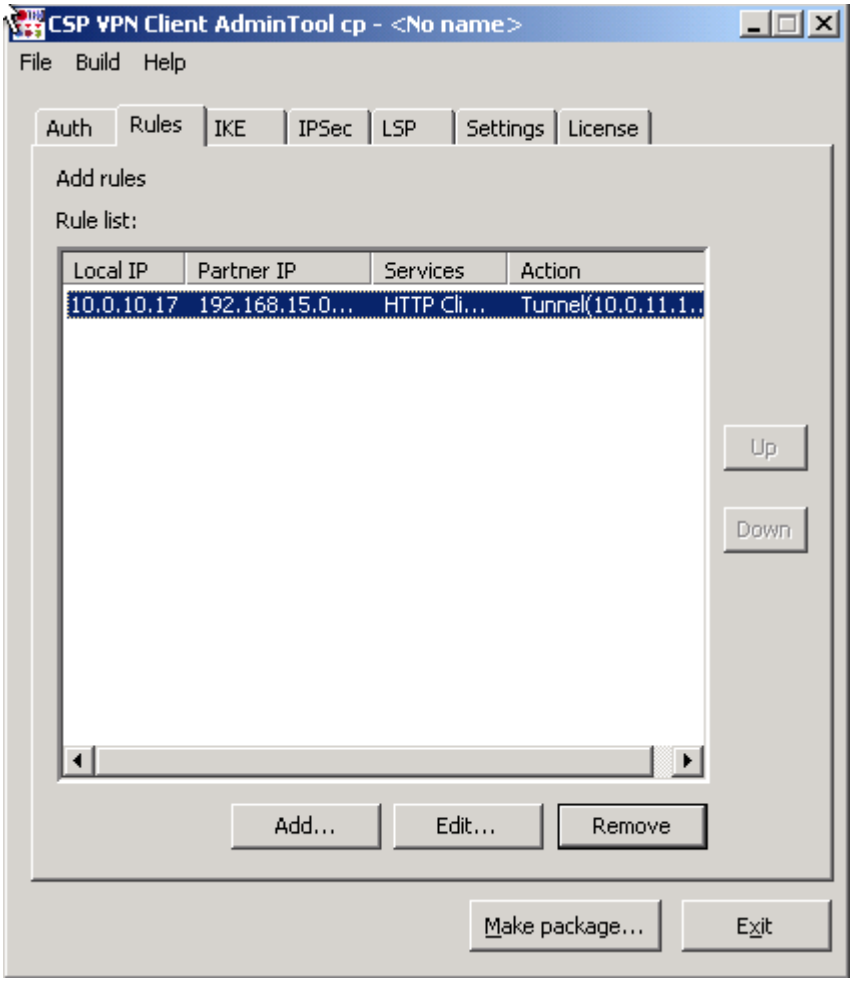


Рисунок 11

Кнопки управления:

- **Add** – вызывает окно, в котором производится создание нового правила
- **Edit** – вызывает окно для редактирования выделенного правила
- **Remove** – удаление выделенного правила с требованием подтверждения операции удаления. Если в списке содержится только одно правило, то при попытке удалить его будет выдано сообщение о невозможности такого удаления (правило не удаляется)
- **Up** – при нажатии этой кнопки выделенное правило в списке перемещается на одну строчку вверх, увеличивая свой приоритет
- **Down** – при нажатии этой кнопки выделенное правило в списке перемещается на одну строчку вниз, уменьшая свой приоритет.

 Copyright © S-Terra CSP 2003 - 2015

10.5.1. Создание и редактирование правила

Создание и редактирование правила производится в окне Add/Edit Rule, которое вызывается кнопкой Add или Edit во вкладке Rules:

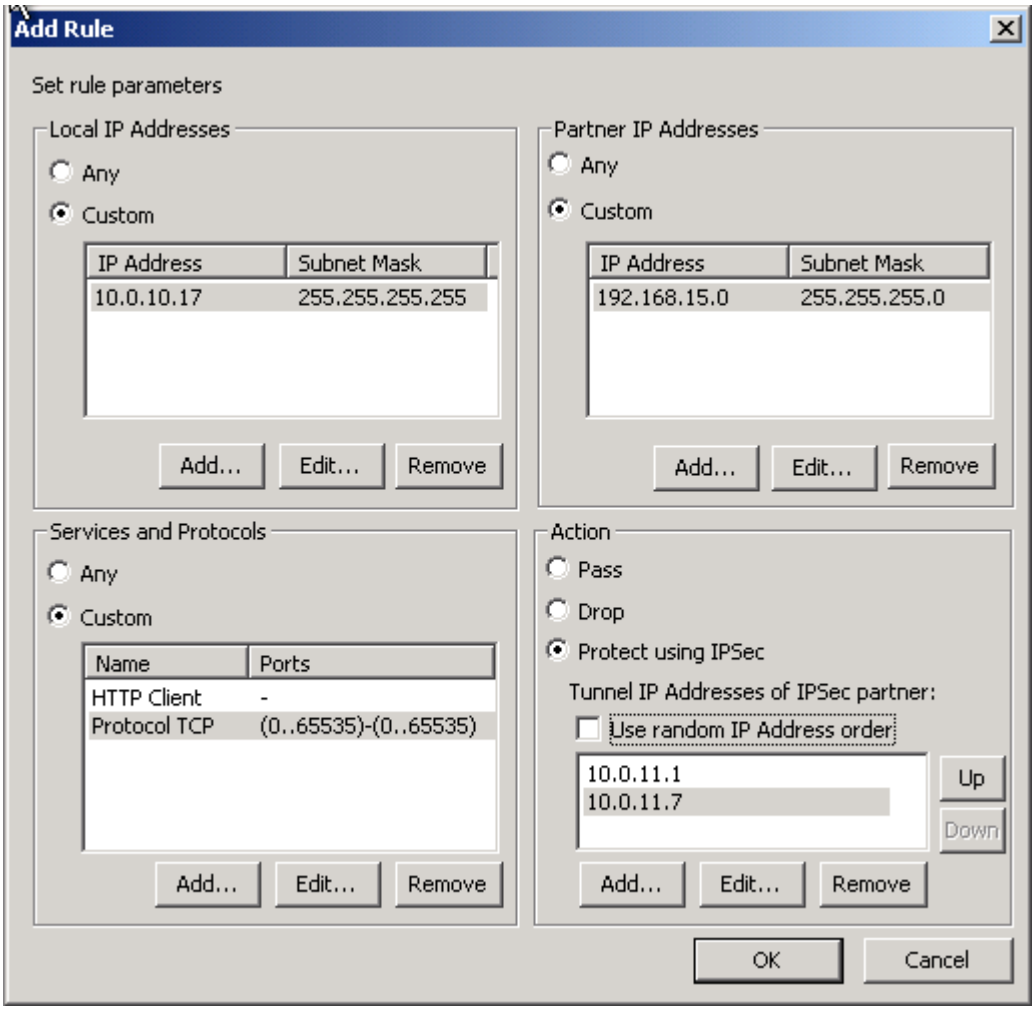


Рисунок 12

Диалоговое окно Rule имеет 4 области для задания правила:

- **Local IP Addresses** – в этой области задаются IP-адреса локального VPN устройства или подсети, на которые будет распространяться правило. Область имеет переключатель с двумя положениями:
  - Any – используется любой IP-адрес
  - Custom – становится доступным окно для ввода IP-адреса и маски подсети
- **Partner IP Addresse**s – в этой области задаются IP-адреса или подсети партнеров, на которые распространяется правило
- **Services and Protocols** – область для задания сетевых сервисов и протоколов, на которые распространяется правило
- **Action** – в этой области задаются действия, применяемые к сетевому трафику этого правила.
- Кнопки управления:
  - **Add** – вызывает окно IP address для ввода IP-адреса и маски хоста или подсети
  - **Edit** – вызывает окно для редактирования выделенной записи

 Copyright © S-Terra CSP 2003 - 2015

- **Remove** – удаление выделенной записи с требованием подтверждения операции удаления
- **Up**, **Down** – кнопки для изменения приоритета выделенного туннельного адреса партнера.

Задание IP-адреса и маски подсети в правиле

Для создания/редактирования IP-адреса хоста (подсети) и маски подсети в правиле в областях Local IP Addresses и Partner IP Addresses установить переключатель в положение Custom и кнопкой Add или Edit вызвать окно Add/Edit IP Address (Рисунок 13). Если сетевая маска равна 255.255.255.255, то задается IP-адрес хоста. Адрес не может быть нулевым.

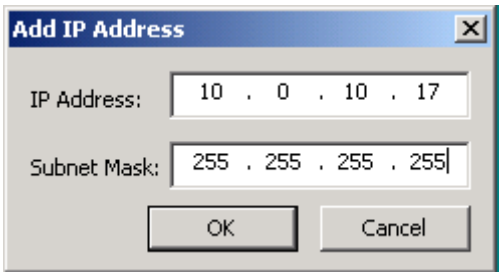


Рисунок 13

Создание сетевого сервиса или протокола в правиле

В области Services and Protocols установить переключатель в положение Custom и кнопкой Add вызвать окно Add Service (Рисунок 14):

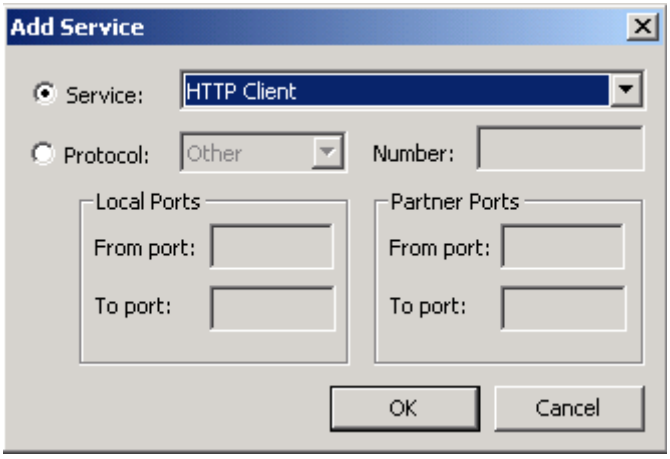


Рисунок 14

В окне Add Service имеется переключатель с двумя положениями:

- **Service** – при установке переключателя в это положение доступным становится только поле Service, которое содержит выпадающий предопределенный не редактируемый список сервисов. Из этого списка выбрать значение и нажать кнопку OK

 Copyright © S-Terra CSP 2003 - 2015

- **Protocol** – при установке переключателя в это положение доступными становятся все поля, кроме поля Service (Рисунок 15). Сетевой протокол выбирается из выпадающего списка, а в поле Number будет автоматически выводиться номер выбранного протокола. Задать протокол можно и по номеру из зарезервированного пространства (0-255). При указании протокола так же возможно указание диапазона портов (в тех протоколах, в которых это возможно). Область Local Ports предназначена для задания портов на локальном компьютере, а область Partner Ports - для задания портов на компьютере партнера. В полях From port и To port задается порт или диапазон портов из зарезервированного пространства (0-65535). Значение в поле From port должно быть меньше или равно значению в поле To port.

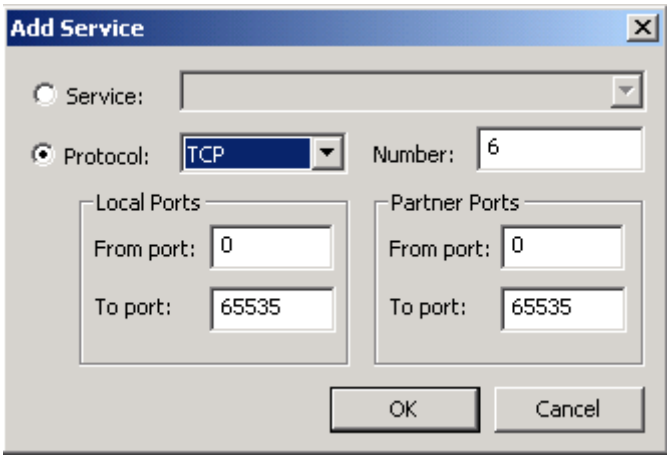


Рисунок 15

Список предлагаемых сетевых сервисов:

- DHCP Client – все пакеты протокола UDP, идущие на порт 67 компьютера партнера и все пакеты протокола UDP, идущие на порт 68 локального компьютера
- DHCP Server – все пакеты протокола UDP, идущие на порт 68 компьютера партнера и все пакеты протокола UDP, идущие на порт 67 локального компьютера
- HTTP Client – все пакеты протокола TCP, идущие на(с) порт(порта) 80 компьютера партнера
- HTTP Server – все пакеты протокола TCP, идущие на(с) порт(порта) 80 локального компьютера
- LDAP Client – все пакеты протокола TCP, идущие на(с) порт(порта) 389 компьютера партнера
- LDAP Server – все пакеты протокола TCP, идущие на(с) порт(порта) 389 локального компьютера
- LDAPS Client – все пакеты протокола TCP, идущие на(с) порт(порта) 636 компьютера партнера
- LDAPS Server – все пакеты протокола TCP, идущие на(с) порт(порта) 636 локального компьютера
- RTELNET Client – все пакеты протокола TCP, идущие на(с) порт(порта) 107 компьютера партнера
- RTELNET Server – все пакеты протокола TCP, идущие на(с) порт(порта) 107 локального компьютера
- SMTP Client – все пакеты протокола TCP, идущие на(с) порт(порта) 25 компьютера партнера

 Copyright © S-Terra CSP 2003 - 2015

- SMTP Server – все пакеты протокола TCP, идущие на(с) порт(порта) 25 локального компьютера
- SNMP – все пакеты протокола UDP, идущие на(с) порт(порта) 161 локального компьютера
- SNMP Trap – все пакеты протокола UDP, идущие на(с) порт(порта) 162 компьютера партнера
- SSH Client – все пакеты протоколов TCP и UDP, идущие на(с) порт(порта) 22 компьютера партнера
- SSH Server – все пакеты протоколов TCP и UDP, идущие на(с) порт(порта) 22 локального компьютера
- TELNET Client – все пакеты протокола TCP, идущие на(с) порт(порта) 23 компьютера партнера
- TELNET Server – все пакеты протокола TCP, идущие на(с) порт(порта) 23 локального компьютера.

Список предлагаемых сетевых протоколов:

EGP, GGP, HMP, ICMP, PUP, RDP, RVD, TCP, UDP, XNS-IDP.

Редактирование выделенного сервиса или протокола производится в окне Edit Service, совпадающем с окном Add Service.

Задание действия в правиле

Задание действия в правиле, распространяющегося на пакет, в области Action (Рисунок 12) производится при помощи переключателя с тремя положениями:

- **Pass** – пропускать сетевой трафик без шифрования
- **Drop** – не пропускать сетевой трафик
- **Protect using IPSec** – защищать сетевой трафик (шифровать). Сетевой трафик защищается между клиентом и указанным туннельным адресом партнера (это может быть адрес интерфейса шлюза безопасности, защищающего подсеть, в которой находится клиент либо адрес интерфейса клиента). В результате этого строится туннель. При установке переключателя в это положение нажмите кнопку Add и в открывшемся окне Add IP Address (Рисунок 16) укажите IP-адрес интерфейса, до которого будет построен туннель для партнера. Адрес не может быть нулевым.

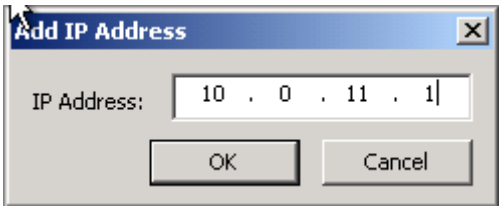


Рисунок 16

Можно указать список IP-адресов, до которых возможно построить туннель. Адреса в списке можно расположить в порядке убывания приоритета – первый в списке имеет самый высокий приоритет. Если не удалось построить туннель до интерфейса с первым указанным адресом в списке, то производится попытка построить туннель со вторым туннельным адресом и т.д. Кнопки Up и Down предназначены для изменения приоритета адресов в списке.

Используя кнопки **Add**, **Edit** и **Delete**, адреса в список можно добавлять, редактировать и удалять из списка.

Use random IP Address order – при установке этого флажка туннельный адрес партнера будет выбираться из списка случайным образом. При неудачной попытке построить туннель с этим адресом, следующий туннельный адрес будет выбираться также случайным образом.

 Copyright © S-Terra CSP 2003 - 2015

10.6. Вкладка IKE

В этой вкладке определены наборы политик IKE, которые предлагаются партнеру при создании ISAKMP SA.

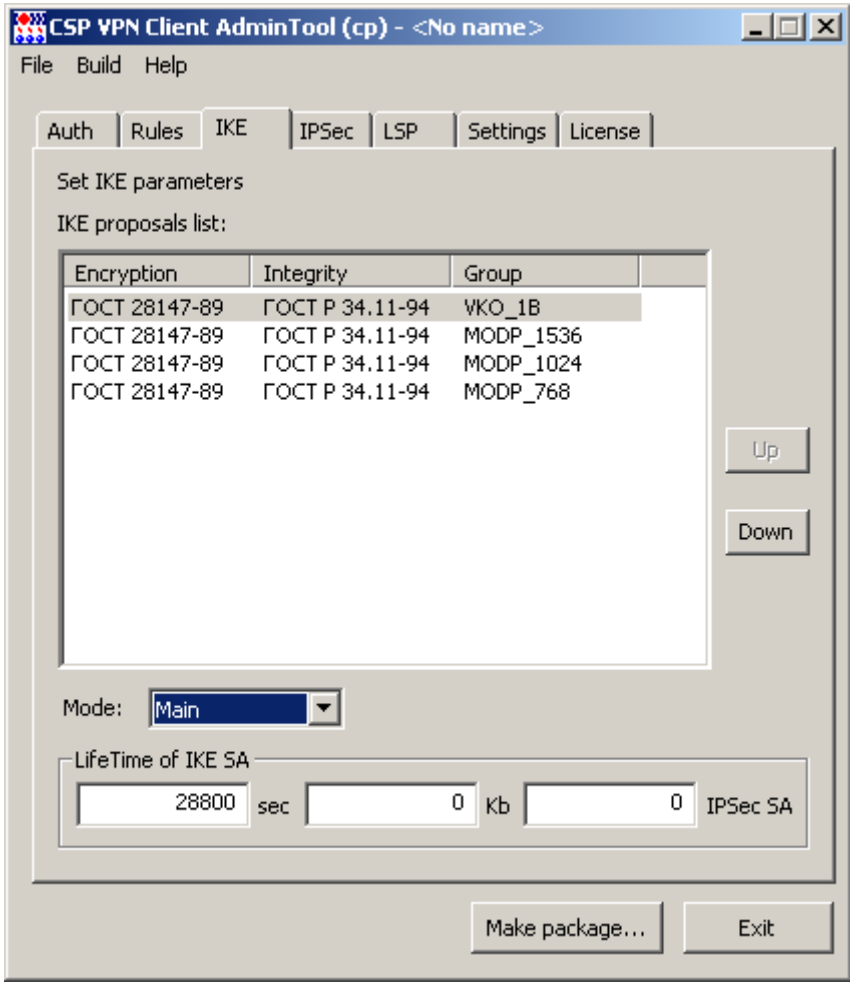


Рисунок 17

IKE proposals list – упорядоченный список IKE предложений по приоритету. В верхней строчке находится предложение с наивысшим приоритетом.

Encryption – предлагаемые алгоритмы шифрования пакетов: Предлагается только один российский криптографический алгоритм:

- ГОСТ 28147-89 – российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как G2814789CPRO1-K256-CBC-65534.

Integrity – предлагаемые алгоритмы проверки целостности. Предлагается только один российский криптографический алгоритм:

- ГОСТ Р 34.11-94 – российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-65534.

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла `admintool.ini`, размещенного в папке Продукта CSP VPN Client AdminTool cp. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе "Формат задания имен алгоритмов в файле admintool.ini", и перезапустить графический интерфейс.

 Copyright © S-Terra CSP 2003 - 2015

Group – параметры выработки ключевого материала:

- VKO_1B – используется алгоритм VKO ГОСТ Р 34.10-2001 [RFC4357]
- MODP_768 – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)
- MODP_1024 – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)
- MODP_1536 – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

Mode – режим обмена информацией о параметрах защиты и установления IKE SA. Имеет два значения:

- Main – в этом режиме партнеру высылаются все IKE политики для выбора и согласования.
- Aggresssive – в этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет. При выборе этого режима выдается об этом предупреждение. Если для аутентификации используется предустановленный ключ и выбран тип идентификатора KeyID, то должен использоваться только режим Aggressive.

LifeTime of IKE SA (sec) – время в секундах, в течение которого ISAKMP SA будет существовать. Возможное значение – целое число из диапазона 0 .. 4 294 967 295. Рекомендуемое значение – 28800, которое выставлено при открытии нового проекта. Значение 0 означает, что время действия SA не ограничено. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

LifeTime of IKE SA (Kb) – указывает объем данных в килобайтах, который могут передать стороны во всех IPsec SA, созданных в рамках одного ISAKMP SA. Возможное значение – целое число из диапазона 0 .. 4 294 967 295. Рекомендуемое значение – 0, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

IPSec SA – количество IPsec SA, созданных в рамках одного ISAKMP SA. Значение 0 означает, что количество IPsec SA не ограничено.

Кнопки **Up** и **Down** предназначены для упорядочивания списка предложений по приоритету.

10.7. Вкладка IPSec

В данной вкладке задаются политики защиты IPsec в виде набора преобразований, каждый из которых есть комбинация AH преобразования и ESP преобразования. Партнеру направляется список наборов преобразований и по протоколу IKE происходит согласование и выбор конкретного набора преобразований, который будет использоваться для защиты трафика для одного SA.

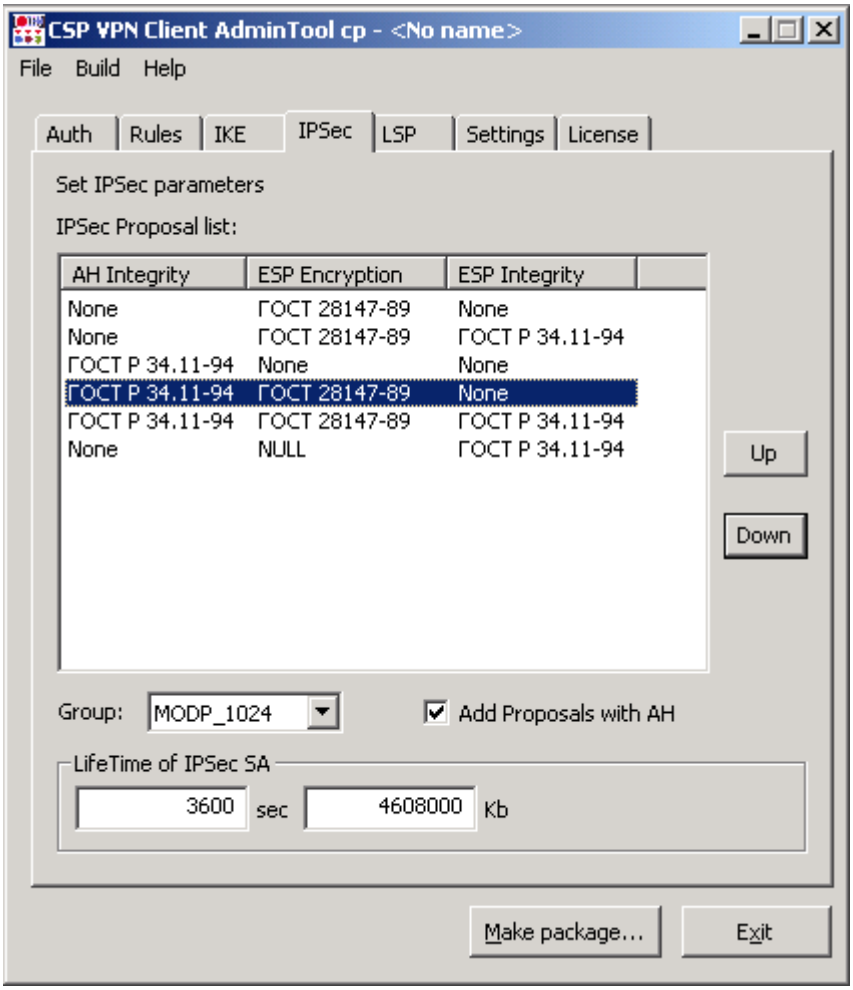


Рисунок 18

IPSec Proposal list – упорядоченный список наборов преобразований, высылаемых партнеру для согласования. При помощи кнопок Up и Down выполняется упорядочивание списка по приоритету. В верхней строчке находится набор преобразований с наивысшим приоритетом.

AH Integrity – предлагаемые алгоритмы проверки целостности по протоколу AH. Имеется два значения:

- None – алгоритм проверки целостности не применяется
- ГОСТ Р 34.11-94 – российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-H96-HMAC-254.

ESP Integrity – предлагаемые алгоритмы проверки целостности по протоколу ESP. Имеется два значения:

- None – алгоритм проверки целостности не применяется
- ГОСТ Р 34.11-94 – российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-H96-HMAC-65534.

 Copyright © S-Terra CSP 2003 - 2015

ESP Encryption – предлагаемые алгоритмы шифрования пакетов по протоколу ESP:

- None – алгоритм шифрования ESP не применяется
- Null – алгоритм применять, но не шифровать
- ГОСТ 28147-89 – российский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как G2814789CPRO1-K256-CBC-254
- ESP_GOST-4M-IMIT – российский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как G2814789CPRO1-K288-CNTMAC-253. Криптографический алгоритм ESP_GOST-4M-IMIT самостоятельно обеспечивает как защиту конфиденциальности (шифрование), так и контроль целостности данных (имитозащиту).

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла `admintool.ini`, размещенного в папке Продукта CSP VPN Client AdminTool ср. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе "Формат задания имен алгоритмов в файле admintool.ini", и перезапустить графический интерфейс.

Add Proposals with AH – при установке этого флажка выводится сообщение:

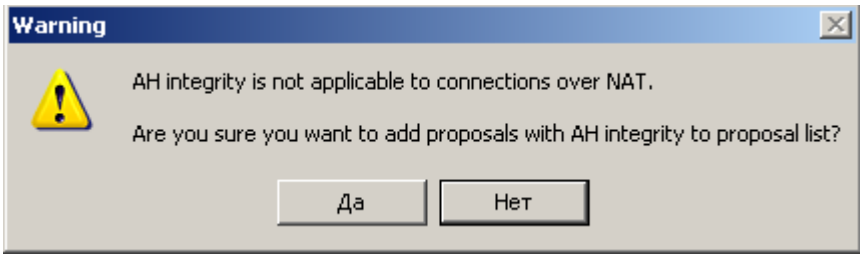


Рисунок 19

Оно означает, что протокол AH несовместим со средствами NAT, так как NAT изменяют IP-адрес в заголовке TCP/IP пакета. Протокол AH обеспечивает проверку аутентичности и целостности пакетов, а NAT нарушает данные аутентификации. После нажатия кнопки «Да» добавляется российский криптографический алгоритм ГОСТ Р 34.11-94.

Group – параметры выработки ключевого материала, высылаемые партнеру для согласования:

- No PFS – опция PFS не включена и при согласовании новой SA новый обмен по алгоритму Диффи-Хеллмана или VKO не выполняется. Ключевой материал заимствуется из первой фазы IKE.
- Выбранный параметр означает, что при согласовании новой SA выполняется новый обмен ключами по алгоритму Диффи-Хеллмана или VKO_1B в рамках IPsec. Может использоваться один из параметров:
  - VKO_1B – используется алгоритм VKO ГОСТ Р 34.10-2001 [RFC4357]
  - MODP_768 – группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)
  - MODP_1024 – группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)
  - MODP_1536 – группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

LifeTime of IPSec SA (sec) – время в секундах, в течение которого IPsec SA будет существовать. Возможное значение – целое число из диапазона 1..4 294 967 295. Рекомендуемое значение – 3600, которое выставлено при открытии нового проекта. Пустая строка и значение 0, которое означает неограниченное время жизни IPsec SA, – недопустимы, при создании инсталляционного файла будет выдано сообщение об ошибке.

 Copyright © S-Terra CSP 2003 - 2015

LifeTime of IPSec SA (Kb) – указывает объем данных в килобайтах, который могут передать стороны в рамках одной IPsec SA. Возможное значение – целое число из диапазона 0..4294967295. Рекомендуемое значение – 4608000, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

Кнопки **Up** и **Down** предназначены для упорядочивания списка предложений по приоритету.

 Copyright © S-Terra CSP 2003 - 2015

10.8. Локальная политика безопасности

Во вкладке LSP просматривается и редактируется локальная политика безопасности для пользователя, определенная в предыдущих вкладках.

Существует два режима работы с LSP:

- режим автоматического формирования LSP
- режим ручного задания LSP.

10.8.1. Режим автоматического формирования LSP

В режиме автоматического формирования (флажок "Use custom LSP" не установлен) локальная политика безопасности формируется на основе данных вкладок Auth, Rules, IKE, IPSec и расширенных параметров, задаваемых в диалоговом окне, вызываемом кнопкой Advanced.

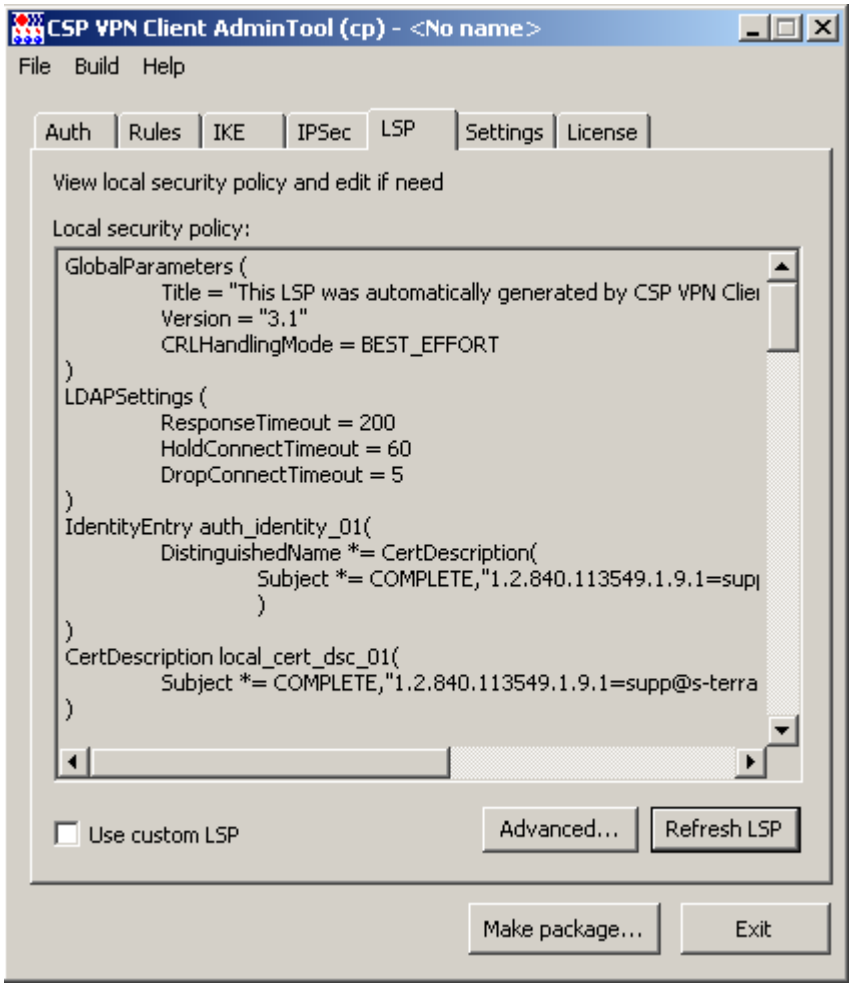


Рисунок 20

Local security policy – поле с LSP в текстовом формате

Use custom LSP – установка этого флажка переключает в режим ручного формирования LSP.

Refresh LSP – кнопка для обновления LSP в окне Local security policy для отображения текущей конфигурации с изменениями.

Advanced – кнопка вызова окна Advanced LSP Settings для настройки расширенного списка параметров LSP.

Copyright © S-Terra CSP 2003 - 2015

Advanced LSP Settings

Это окно отображает расширенный список переменных LSP и их текущие значения, которые можно отредактировать и установить значения по умолчанию. Переменные объединены в пять групп.

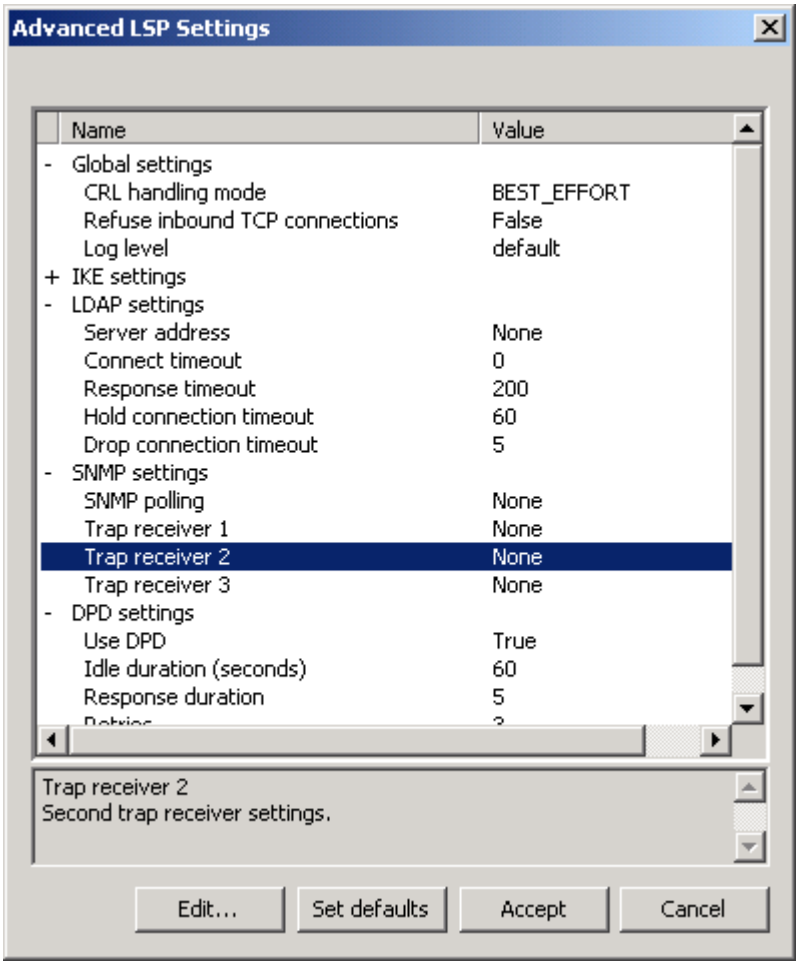


Рисунок 21

Окно содержит 4 функциональные кнопки:

- **Edit** – кнопка вызова окна для редактирования выделенной переменной. Окно редактирования открывается также при двойном клике левой кнопки "мыши" на выделенной строке.
- **Set defaults** – кнопка для установки значений по умолчанию для всех переменных.
- **Accept** – кнопка для закрытия окна с сохранением отредактированных значений переменных.
- **Cancel** – кнопка для закрытия окна без сохранения отредактированных значений переменных.

 Copyright © S-Terra CSP 2003 - 2015

Global settings

CRL handling mode

Переменная задает режим использования списков отозванных сертификатов (CRL). При нажатии кнопки Edit появляется окно для выбора значений из выпадающего списка:

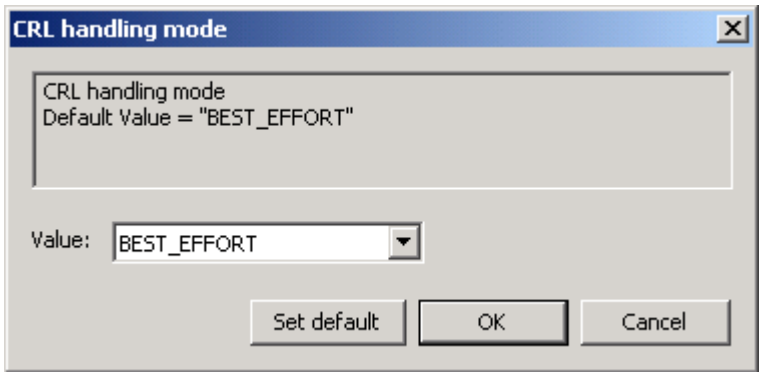


Рисунок 22

Возможные значения:

- DISABLE – при проверке сертификата список отозванных сертификатов не обрабатывается
- OPTIONAL – список отозванных сертификатов используется только в случае, если он был предустановлен или получен (и обработан) в процессе IKE обмена и является действующим
- BEST_EFFORT – список отозванных сертификатов используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима OPTIONAL тем, что CRL может быть получен посредством протокола LDAP (если он настроен). Это значение используется по умолчанию.
- ENABLE – для успешной проверки сертификата обрабатывается список отозванных сертификатов.

Значение по умолчанию – BEST_EFFORT.

Все окна для редактирования переменных имеют три функциональные кнопки:

- Set default – кнопка для установления значения по умолчанию данной переменной
- OK – кнопка для закрытия окна с сохранением выбранного значения переменной.
- Cancel – кнопка для закрытия окна без сохранения выбранного значения переменной.

Refuse inbound TCP connections

Задает блокировку входящих TCP-соединений. Используется как дополнительное ограничение к действию. При редактировании появляется окно:

 Copyright © S-Terra CSP 2003 - 2015

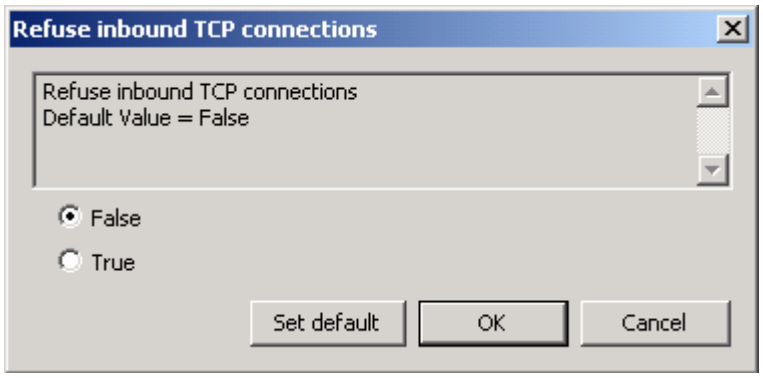


Рисунок 23

Переключатель имеет два положения:

- TRUE – уничтожается первый входящий TCP-пакет соединения, если он входящий. В результате отвергаются все TCP-соединения, инициированные извне.
- FALSE – не производится никаких дополнительных действий. Значение по умолчанию.

Значение по умолчанию – FALSE.

Log level

Задает текущий уровень лога для разных событий, связанных с доступом к LDAP серверу, с применением LSP, получением, обработкой сертификатов и их сохранением в базе Продукта, системными событиями. При редактировании появляется окно:

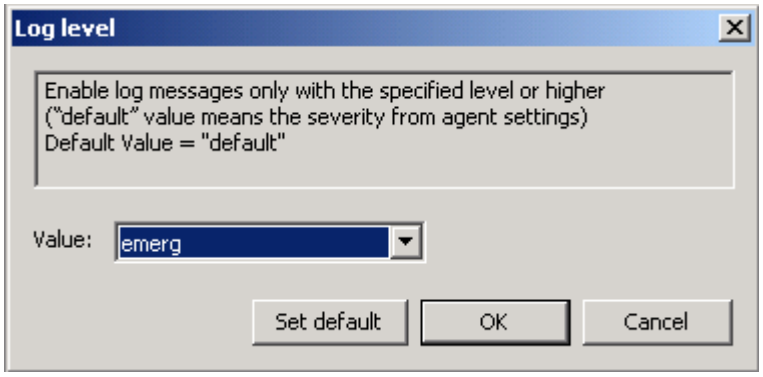


Рисунок 24

Значение по умолчанию – default, которое берется из общего уровня протоколирования событий, установленных во вкладке Settings в поле Severity.

IKE settings

Default port

Порт для протокола IKE, который будет использован по умолчанию. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 500.

Окно для выбора значения порта:

 Copyright © S-Terra CSP 2003 - 2015

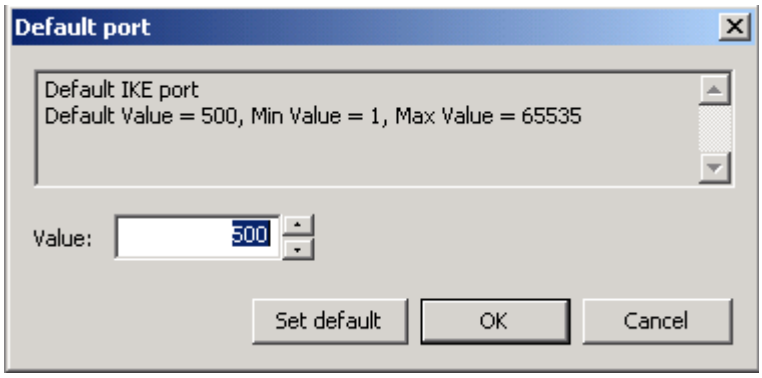


Рисунок 25

Send packet retries

Количество попыток посылки IKE-пакетов партнеру. Возможное значение – целое число из диапазона 1..30. Значение по умолчанию – 5.

Окно для установки значения:

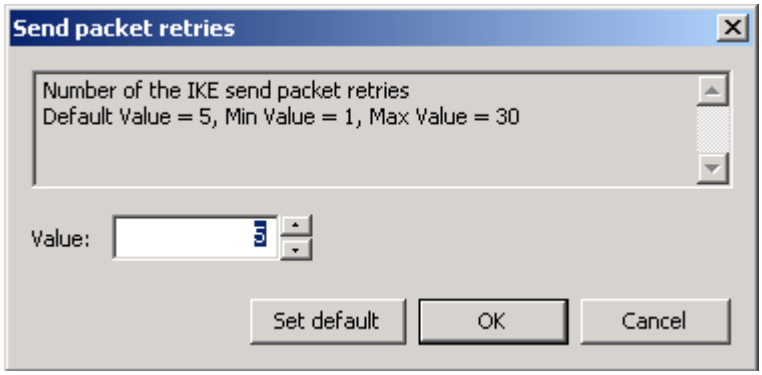


Рисунок 26

Initial retry time (seconds)

Начальный интервал времени между повторными попытками посылки IKE-пакетов партнеру (в секундах). Если ответ не получен в течение начального интервала, то запрос посылается повторно и интервал между повторными попытками увеличивается в два раза. Этот интервал увеличивается в два раза до тех пор, пока:

- не будет получен ответ или
- значение интервала Initial retry time не достигнет значения Max retry time, (повторные попытки будут продолжаться с интервалом Max retry time) и количество попыток не достигнет значения Send packet retries.

Возможное значение – целое число из диапазона 1..5. Значение по умолчанию – 1.

Окно для установки начального интервала времени:

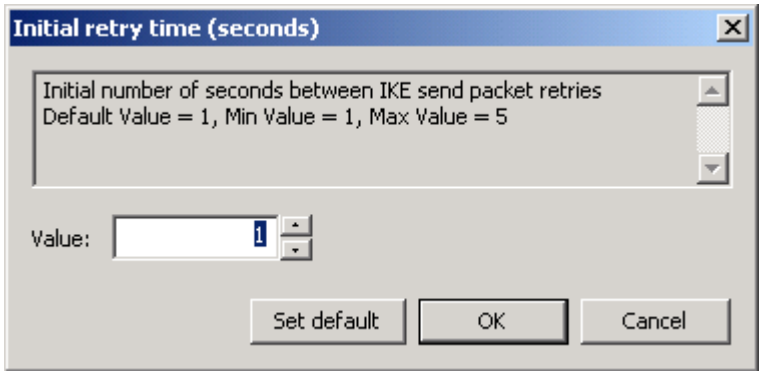


Рисунок 27

 Copyright © S-Terra CSP 2003 - 2015

Max retry time (seconds)

Максимальный интервал времени между повторными попытками посылки IKE-пакетов партнеру (в секундах). Если выставленное значение Max retry time меньше, чем значение Initial retry time, то при загрузке конфигурации Max retry time присваивается значение Initial retry time. Возможное значение – целое число из диапазона 1..60. Значение по умолчанию – 30.

Окно для установки максимального интервала времени:

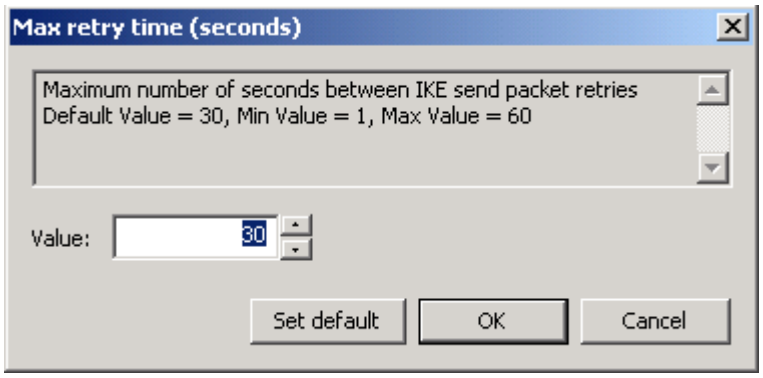


Рисунок 28

Max session duration (seconds)

Максимальный интервал времени на каждую сессию IKE (в секундах). Возможное значение – целое число из диапазона 10..300. Значение по умолчанию – 60. Окно для выбора значения:

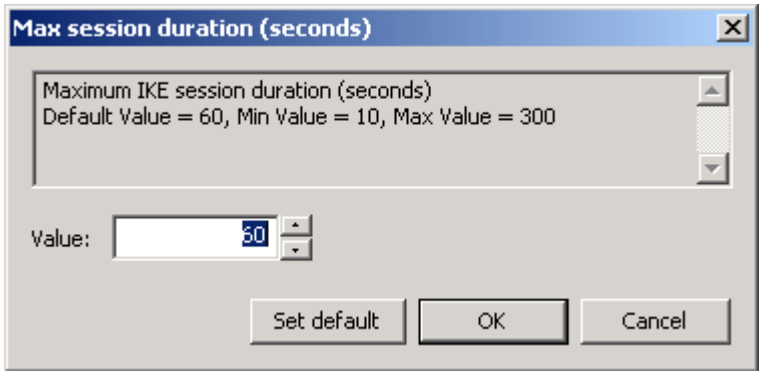


Рисунок 29

Max sessions initiated at once

Максимальное количество одновременно инициируемых IKE-сессий для всех партнёров. Возможное значение – целое число из диапазона 1..10000. Значение по умолчанию – 30. Окно для выбора значения:

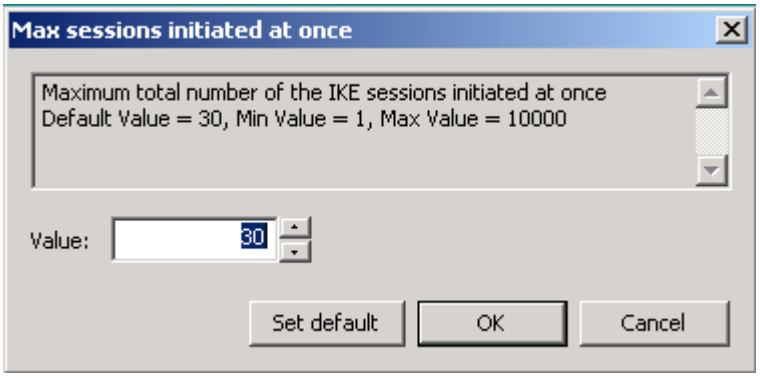


Рисунок 30

Copyright © S-Terra CSP 2003 - 2015

Max responder sessions with a partner

Максимально допустимое количество одновременных обменов, проводимых VPN-устройством с одним неаутентифицированным партнером, в качестве ответчика. С таким партнером нет ни одного ISAKMP SA. Как только создается хотя бы один ISAKMP SA, данный атрибут перестает действовать.

Возможное значение – целое число из диапазона 1..20. Значение по умолчанию – 20. Окно для установки значения:

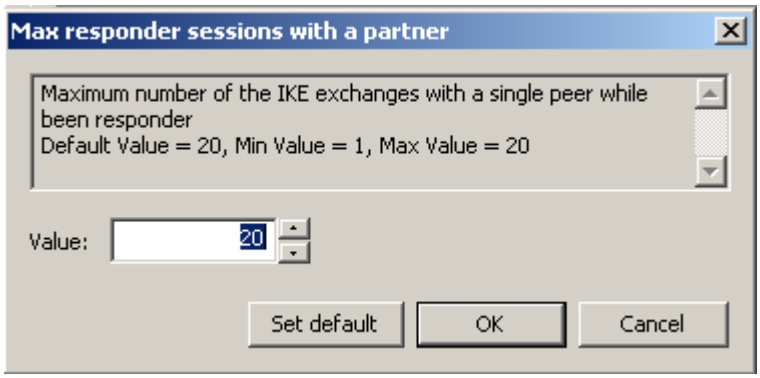


Рисунок 31

Max blacklog sessions

"Черный список" предназначен для защиты от DoS-атак (Denial of Service –отказ от обслуживания). "Черный список" минимизирует обработку IKE-пакетов от партнеров, находящихся в "черном списке". В случае первой неуспешной IKE-сессии, инициированной со стороны партнера, партнер сразу же заносится в "черный список". Max blacklog sessions устанавливает число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, только что попавшим в "черный список". При каждом следующем неудачном завершении IKE обмена число разрешенных одновременных IKE обменов для данного партнера снижается вдвое с округлением в меньшую сторону, вплоть до полного запрещения IKE трафика с данным партнером.

Примечание: как только партнер заносится в "черный список", для него текущее значение разрешенных одновременно проводимых IKE обменов не только начинает уменьшаться в два раза после каждого неуспешного завершения обмена, но и увеличиваться на единицу по истечении каждого интервала времени Blacklog relax time (описанного далее).

Возможное значение - целое число из диапазона – 0..4294967295.

Если значение равно 0, то "черный список" не используется.[1]

Если значение Max blacklog sessions больше или равно значению Max responder sessions with a partner, то Max blacklog sessions присваивается значение Max responder sessions with a partner `-1`.

Значение по умолчанию – 16.

[1] При загрузке конфигурации с отключенным "черным списком" вся статистическая информация о "плохих" партнерах сбрасывается. Если же "черный список" включен, то к уже имеющейся накопленной статистике применяются новые параметры настроек "черного списка".

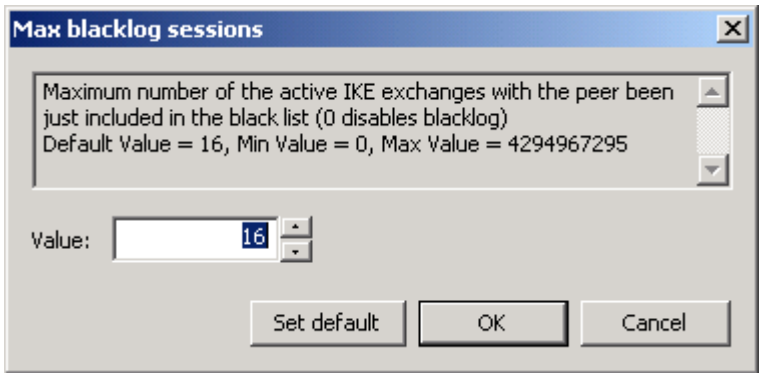


Рисунок 32

Min blacklog sessions

Минимальное число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, находящимся в "черном списке".

Возможное значение – целое число из диапазона – 0..4294967295.

Если значение Min blacklog sessions больше, чем Max blacklog sessions, то Min blacklog sessions присваивается значение Max blacklog sessions.

Значение по умолчанию – 0 означает, что нет ограничения снизу на активные обмены с партнером, находящимся в "черном списке".

Окно для выбора минимального количества обменов с партнером из "черного списка":

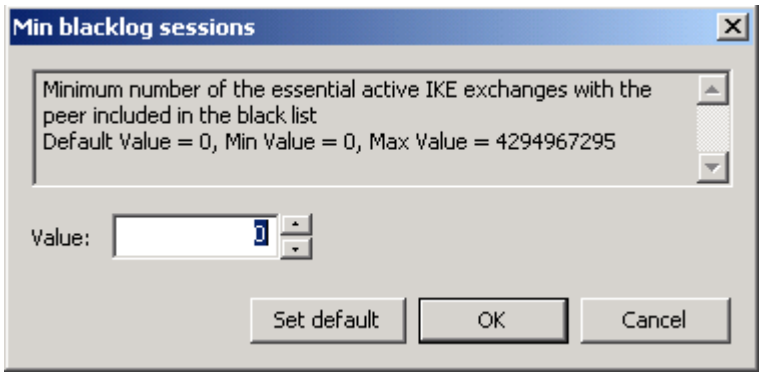


Рисунок 33

Blacklog sessions silent

Число активных обменов, инициированных партнером, находящимся в "черном списке", по достижении которого VPN-устройство перестает информировать партнера о причине отказа в создании IKE–контекста (ISAKMP SA).

Возможное значение - целое число из диапазона – 0..4294967295.

Если значение Blacklog sessions silent больше, чем Max blacklog sessions, то Blacklog sessions silent присваивается значение Max blacklog sessions.

Значение по умолчанию – 4.

Окно для выбора количества обменов:

 Copyright © S-Terra CSP 2003 - 2015

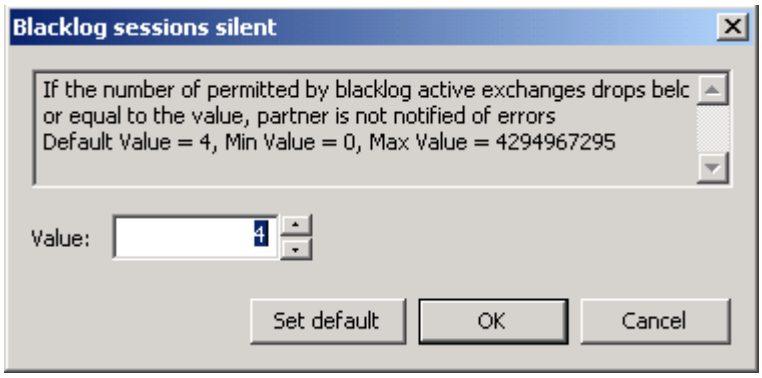


Рисунок 34

Blacklog relax time (seconds)

Устанавливает интервал времени (в секундах) релаксации "черного списка".

За указанный период времени число разрешенных одновременных IKE обменов для каждого партнера, находящегося в "черном списке", увеличивается на единицу. По истечении следующего такого же интервала времени, текущие значения разрешенных одновременно проводимых IKE обменов для каждого партнера опять увеличивается на единицу и т.д. Этот интервал времени отсчитывается с момента последней загрузки конфигурации.

Как только текущее значение разрешенных одновременно проводимых партнером IKE обменов начинает превышать значение Max blacklog sessions, такой партнер исключается из "черного списка".

Возможное значение – целое число из диапазона 0..4294967295. Значение 0 означает бесконечное время релаксации "черного списка" (партнер попадает в "черный список" навсегда). Значение по умолчанию – 120 секунд.

Примечание: помимо механизма релаксации, партнер также может быть иключен из "черного списка" в следующих случаях:

- при перезапуске сервиса
- при загрузке конфигурации с отключенным "черным списком" (Max blacklog sessions = 0)
- при инициации IKE обмена со стороны локального VPN устройства с целью установления ISAKMP (IPsec) соединения[2]
- если партнеру удалось установить ISAKMP (IPsec) соединение с локальным VPN устройством, и тем самым партнер был успешно аутентифицирован.

Окно для выбора интервала времени:

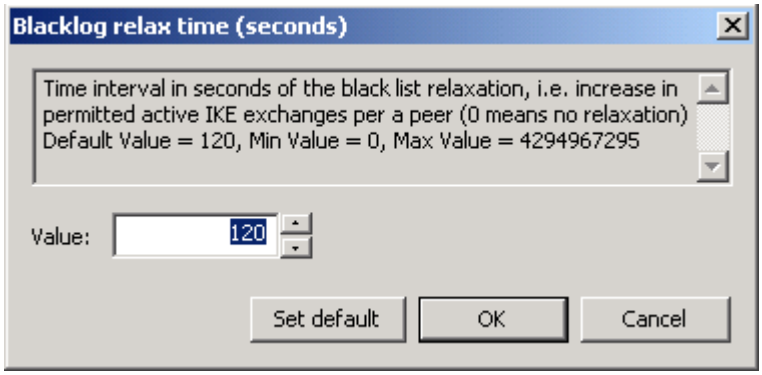


Рисунок 35

[2] В данном случае считается, что локальное VPN устройство потенциально доверяет партнеру, с которым оно хочет установить соединение, и информация, накопленная в "черном списке", для такого партнера сбрасывается.

 Copyright © S-Terra CSP 2003 - 2015

Initiate IKE CFG request

Задает режим работы IKECFG клиента. Возможные значения:

- TRUE – агент является активным IKECFG клиентом, т.е. агент инициирует посылку запроса на получение адреса у партнера сразу после создания IKE SA (если партнер не является IKECFG-сервером – строительство SA продолжается как с обычным партнером)
- FALSE – не производится никаких действий.

Значение по умолчанию – TRUE.

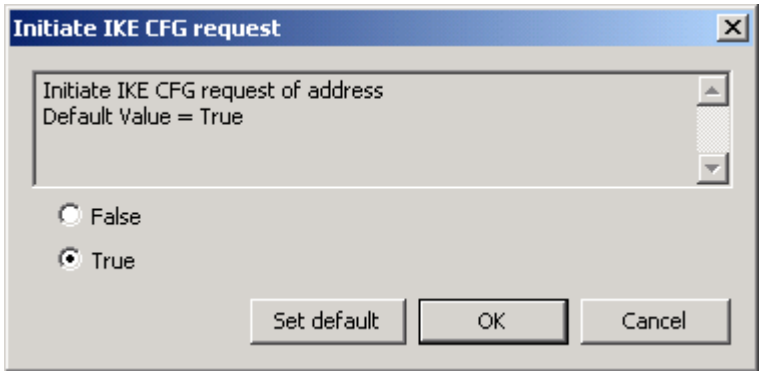


Рисунок 36

Send certificate request mode

Определяет логику отсылки запроса на сертификат партнера. Возможные значения:

- AUTO – запрос высылается, если возможный сертификат партнера отсутствует
- NEVER – запрос не высылается
- ALWAYS – запрос высылается всегда.

Значение по умолчанию – AUTO.

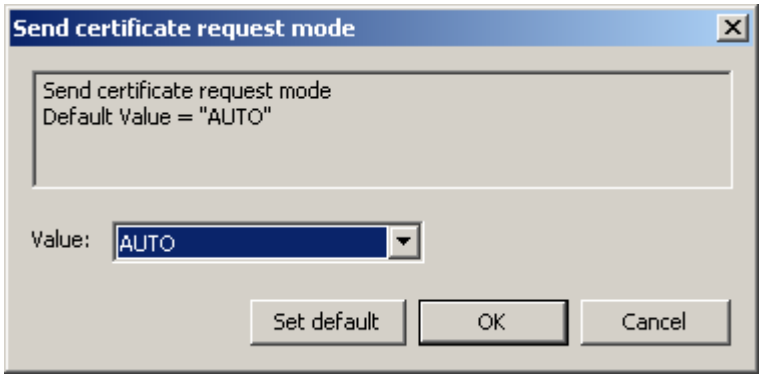


Рисунок 37

Send certificate mode

Определяет логику отсылки локального сертификата в процессе первой фазы IKE на запрос партнера. В своем запросе партнер может указать какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отсылается. Возможные значения:

- AUTO – автоматически определяется, когда необходима отсылка локального сертификата партнеру
- NEVER – сертификат не высылается
- ALWAYS – сертификат высылается всегда

 Copyright © S-Terra CSP 2003 - 2015

- CHAIN – сертификат высылается всегда, причем в составе с цепочкой доверительных CA. Имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

Значение по умолчанию – AUTO.

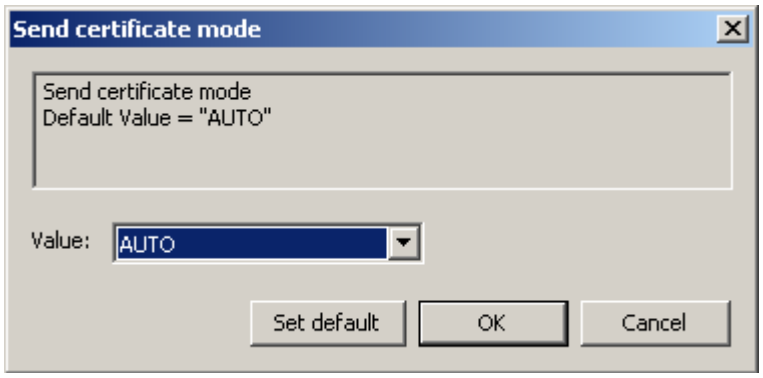


Рисунок 38

Do autopass

Задает режим автоматического пропускания ISAKMP-трафика. Возможные значения:

- TRUE – автоматически пропускать ISAKMP-пакеты по всем фильтрам, по которым защищается трафик.
- FALSE – не пропускать автоматически ISAKMP-пакеты. Правило фильтрации для пропускания ISAKMP-трафика должно быть задано явно (вручную) с действием PASS.

Значение по умолчанию – TRUE.

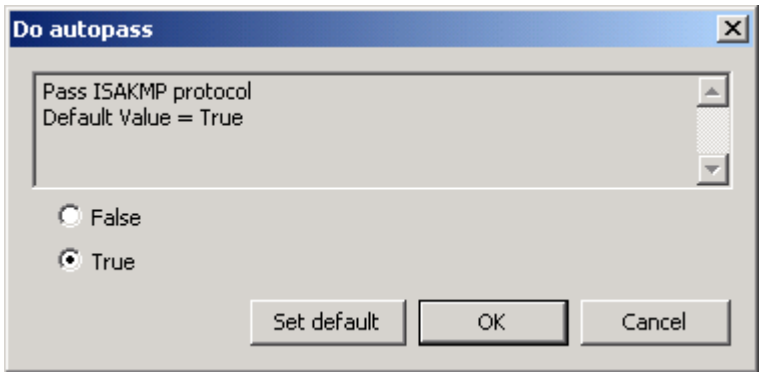


Рисунок 39

LDAP settings

Server address

Задаваемые здесь параметры LDAP-сервера используются тогда, когда сертификат, для которого производится проверка подписи, не содержит расширение CDP (CRL Distribution Point) с адресом LDAP-сервера либо в этом поле прописанный путь к LDAP-серверу является неполным и тогда добавляются данные из этой структуры.

В окне Server address задаются параметры LDAP-сервера. Возможные значения:

- LDAP-сервер не используется, когда флажок Use default LDAP Server не установлен

 Copyright © S-Terra CSP 2003 - 2015

- LDAP-сервер используется, когда флажок Use default LDAP Server установлен. При необходимости будет производиться поиск сертификатов и CRLs на заданном LDAP сервере. При этом нужно заполнить поля:
  - IP Address – сетевой адрес LDAP-сервера.
  - Port – сетевой порт LDAP-сервера, на который будут посылаться LDAP запросы. Значение по умолчанию – 389.
  - Search base – имя (Distinguished Name, DN) корневого X.500-объекта, в поддереве которого производится поиск сертификатов и CRL на LDAP-сервере. Если DN сертификата и DN X.500-объекта не совпадают, и если DN сертификата является частью имени DN X.500-объекта, то заполняется поле Searchbase, чтобы дополнить запрос, созданный на основе имени из сертификата или CRL, для нахождения соответствующего X.500-объекта. Для запроса на основе URL данное имя не используется. См. Пример в структуре LDAPSettings.
- Pass LDAP protocol with the LDAP Server – при установке этого флажка производится автоматическое создание сетевого фильтра для пропускания пакетов между агентом и LDAP-сервером.

Значение по умолчанию – LDAP-сервер не используется.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP_PROTOCOL_ERROR (наиболее вероятная причина – не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

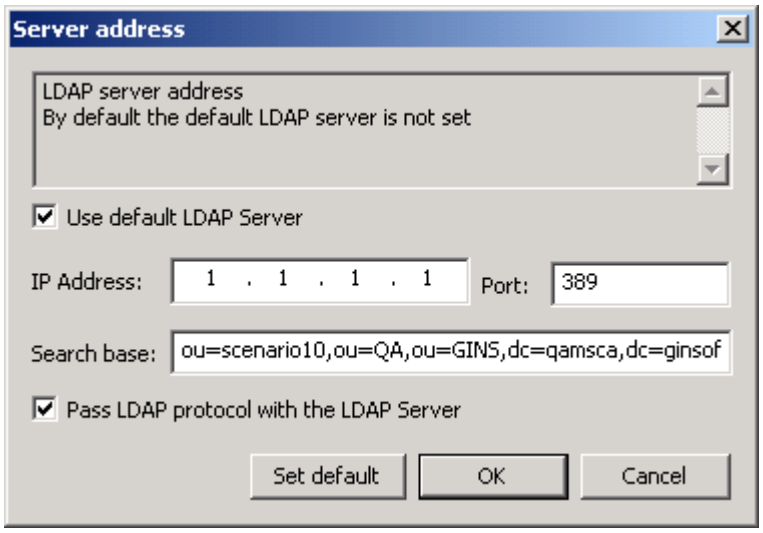


Рисунок 40

Connect timeout

Connect timeout позволяет ограничить время (в секундах) создания TCP-соединения с LDAP-сервером. Возможное значение – целое число из диапазона 1..6000. Значение по умолчанию – 0, которое означает, что время создания TCP-соединения с LDAP-сервером ограничивается установленным для ОС временем создания TCP-соединения.

Примечание: Если в момент обращения к LDAP-серверу устройство, на котором он установлен, недоступно, то процесс создания TCP-соединения может занимать продолжительное время (до 3 минут, зависит от ОС). По этой причине могут наблюдаться внешние признаки зависания агента и это может служить причиной неудачной попытки создания соединения.

 Copyright © S-Terra CSP 2003 - 2015

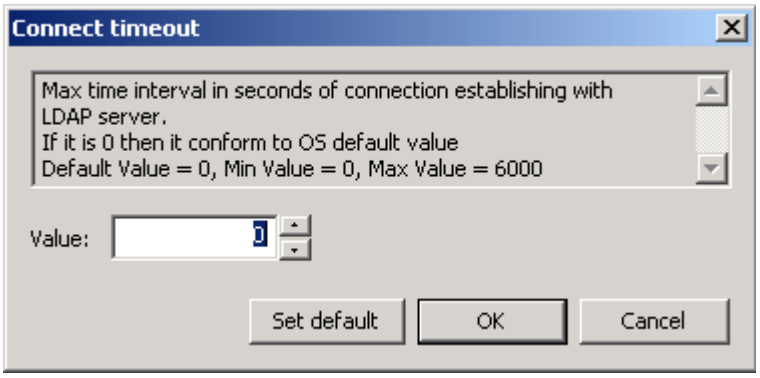


Рисунок 41

Response timeout

Поиск посредством протокола LDAP может занимать достаточно продолжительное время, оно зависит от многих факторов, в том числе от масштаба запроса и характеристик канала передачи данных. Response timeout позволяет ограничить время (в секундах), в течение которого ожидается ответ от LDAP-сервера на единичный запрос. Возможное значение – целое число из диапазона 2..6000. Значение по умолчанию – 200.

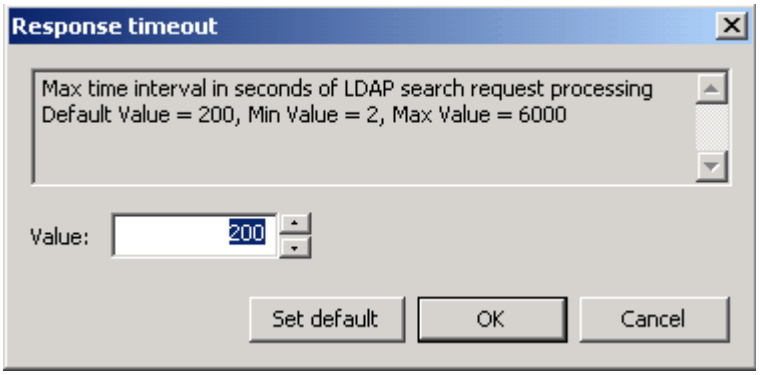


Рисунок 42

Hold connection timeout

Hold connection timeout устанавливает период времени, в течение которого держится установленное соединение к серверу на случай, если придет к нему повторный запрос. Возможное значение – целое число из диапазона 0..6000.

При значении 0 после обмена с LDAP-сервером соединение с ним сразу закрывается.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в 1 секунду, поскольку это может привести в некоторых случаях к немедленному закрытию соединения и к избыточному открытию нового соединения.

Значение по умолчанию – 60.

 Copyright © S-Terra CSP 2003 - 2015

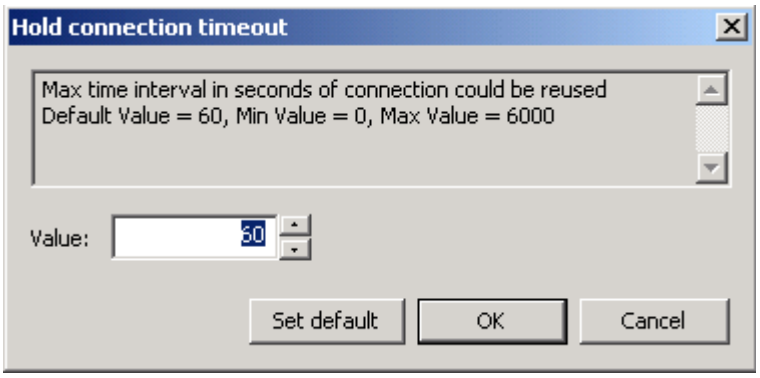


Рисунок 43

Drop connection timeout

Атрибут Drop connection timeout устанавливает период времени, начиная с первой неудачной попытки создания соединения с LDAP-сервером, в течение которого новые попытки создания соединения с ним игнорируются. Возможное значение – целое число из диапазона 0..6000.

При значении 0 в случае неудачной попытки установления соединения с LDAP-сервером новые попытки не игнорируются.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в одну секунду, поскольку это может привести в некоторых случаях к избыточным попыткам создания соединения.

Значение по умолчанию – 5.

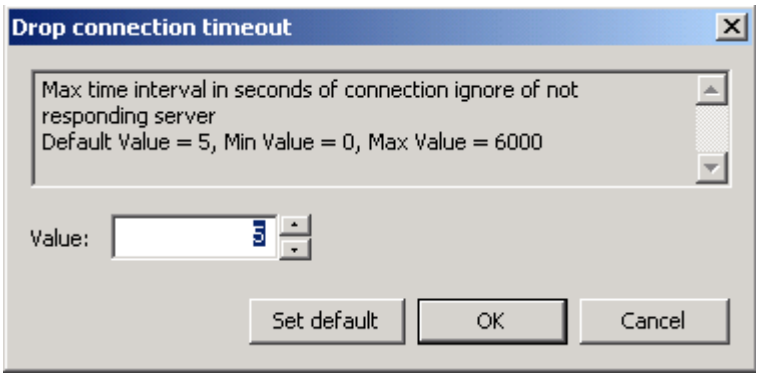


Рисунок 44

SNMP settings

SNMP polling

Задает настройки по выдаче информации по запросу SNMP-менеджера. Возможные значения:

- не принимаются и не обрабатываются запросы на выдачу SNMP статистики
- принимаются и обрабатываются запросы на выдачу SNMP статистики.

Значение по умолчанию – SNMP статистика не выдается.

 Copyright © S-Terra CSP 2003 - 2015

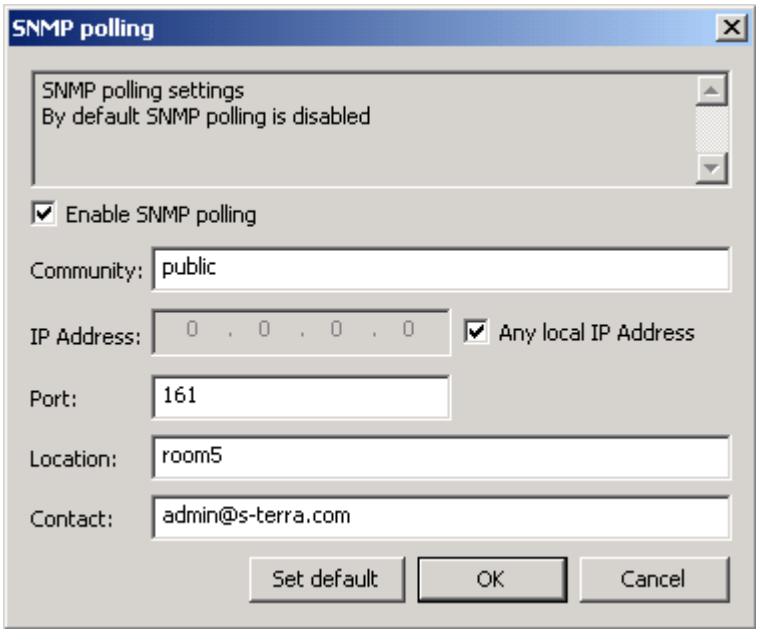


Рисунок 45

Enable SNMP polling – при установке этого флажка задаются настройки для принятия запроса и выдачи статистики.

Community – эта строка действует подобно паролю и разрешает доступ к чтению статистики SNMP-менеджеру.

IP Address – локальный IPv4-адрес, на который можно получать запросы от SNMP-менеджера.

Any local IP Address – установка этого флажка разрешает получение запроса от SNMP-менеджера на любой локальный IP-адрес.

Port – задаёт порт, на который можно получать SNMP-запросы.

Location – информация о физическом расположении SNMP-агента.

Contact – информация о контактном лице, ответственном за работу SNMP-агента.

Trap receiver

Задает настройки получателя SNMP-трапов и дополнительные настройки для трапов, отсылаемых на него. Возможные значения:

- получатель SNMP-трапов не задан
- получатель SNMP-трапов задан.

Значение по умолчанию - получатель SNMP-трапов не задан.

Можно задать до трех получателей SNMP-трапов.

Enable the trap receiver - при установке этого флажка задаются настройки получателя SNMP-трапов.

Community – текстовая строка, играющая роль идентификатора отправителя трап-сообщения.

Receiver's IP Address – IP-адрес получателя SNMP-трапов.

Receiver's Port – UDP-порт, на который менеджеру будут высылаться трап-сообщения.

SNMP Version – версия SNMP, в которой формируются трап-сообщения.

Agent's IP Address – IP-адрес отправителя трап-сообщения. Этот атрибут указывается только для Version = V1.

 Copyright © S-Terra CSP 2003 - 2015

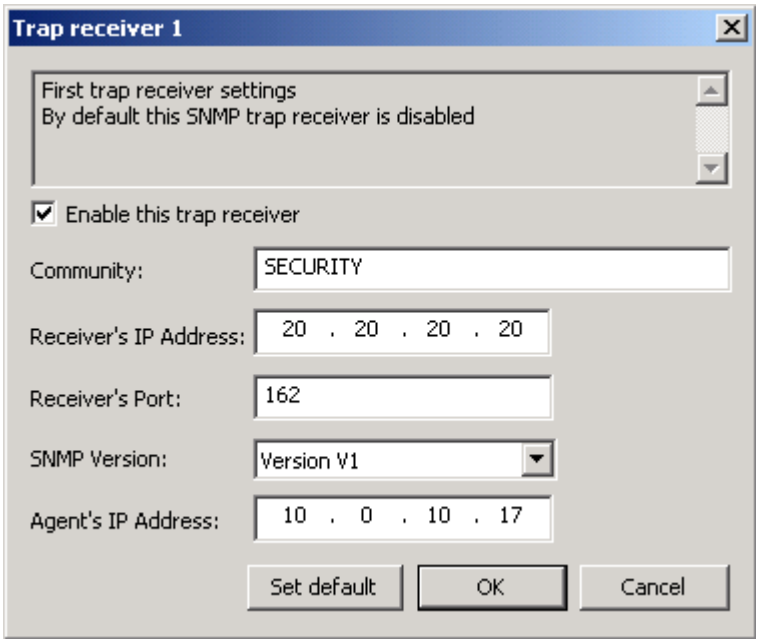


Рисунок 46

DPD settings

Use DPD

Задает режим использования протокола DPD (Dead-Peer-Detection). Возможные значения:

- TRUE – использовать протокол DPD.
- FALSE – не использовать протокол DPD. В этом случае другие переменные этого раздела не появляются.

Значение по умолчанию – TRUE.

Окно для установки переключателя:

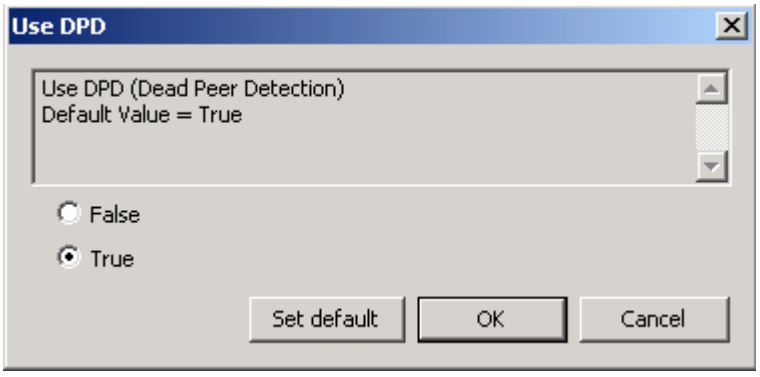


Рисунок 47

Idle duration (seconds)

Интервал времени отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия. Возможные значения – целое число из диапазона 1..32762. Значение по умолчанию – 60. Окно для установки значения:

 Copyright © S-Terra CSP 2003 - 2015

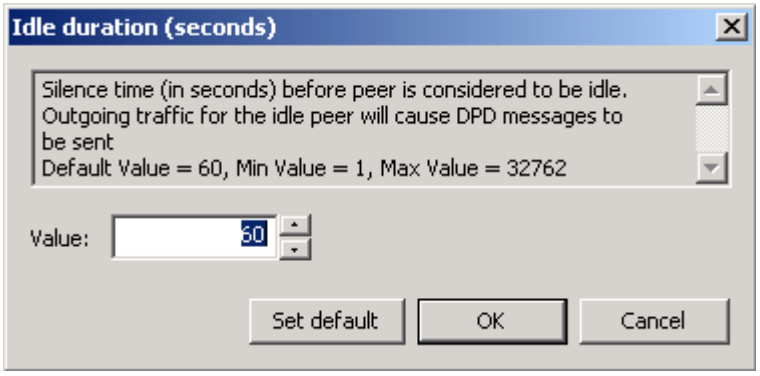


Рисунок 48

Response duration

Время ожидания ответа от партнера на DPD-запрос в секундах. Возможные значения – целое число из диапазона 1..300. Значение по умолчанию – 5. Окно для выбора значения:

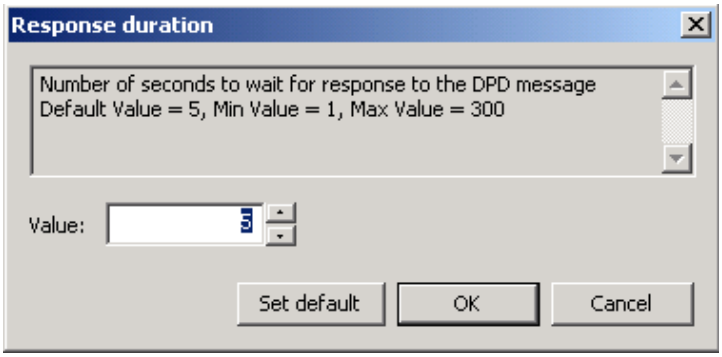


Рисунок 49

Retries

Количество попыток провести DPD-обмен. Если все попытки закончились неудачей, защищенное соединение (IKE-контекст) считается "мертвым", и производится попытка создать его заново. Возможные значения – целое число из диапазона 1..10. Значение по умолчанию – 3. Окно для выбора значения:

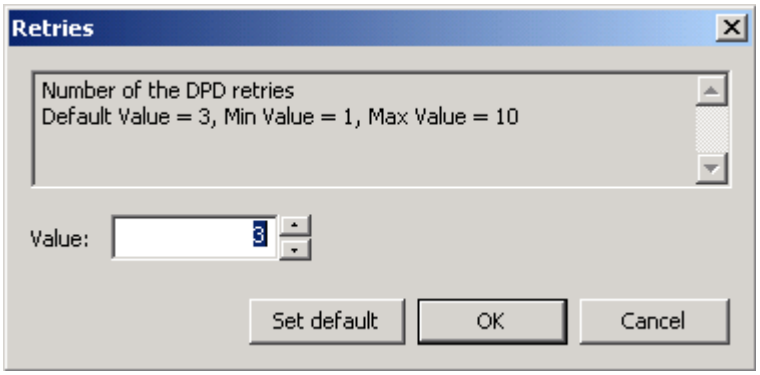


Рисунок 50

Copyright © S-Terra CSP 2003 - 2015

10.8.2. Режим ручного задания LSP

В режиме ручного задания локальная политика безопасности задается администратором (вкладки Rules, IKE и IPSec становятся невидимыми)

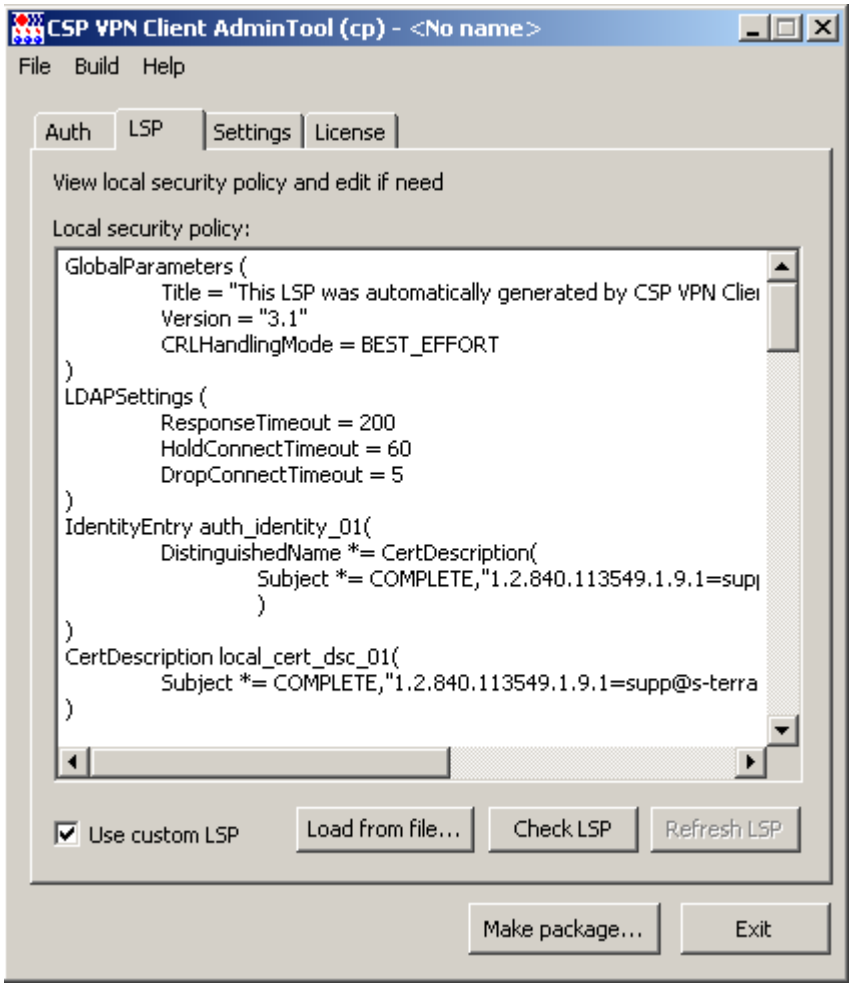


Рисунок 51

Local security policy – поле с текстовым представлением локальной политики безопасности. В этом поле можно создавать и редактировать LSP.

Use custom LSP – снятие этого флажка переводит в режим автоматического формирования LSP

Load from file – при нажатии этой кнопки происходит загрузка LSP из файла в поле Local security policy.

Check LSP – при нажатии этой кнопки происходит проверка заданной LSP по выявлению синтаксических ошибок. При обнаружении ошибки выдается сообщение с описанием ошибки (если строка с ошибочными символами определена, то она выделяется и на эту строку автоматически переводится фокус. Если данная LSP не содержит синтаксических ошибок, то выдается сообщение, что синтаксических ошибок не найдено.

 Copyright © S-Terra CSP 2003 - 2015

10.9. Вкладка Settings

Во вкладке Settings задаются настройки протоколирования событий, политика по умолчанию и дополнительные параметры инсталляции Продукта CSP VPN Client.

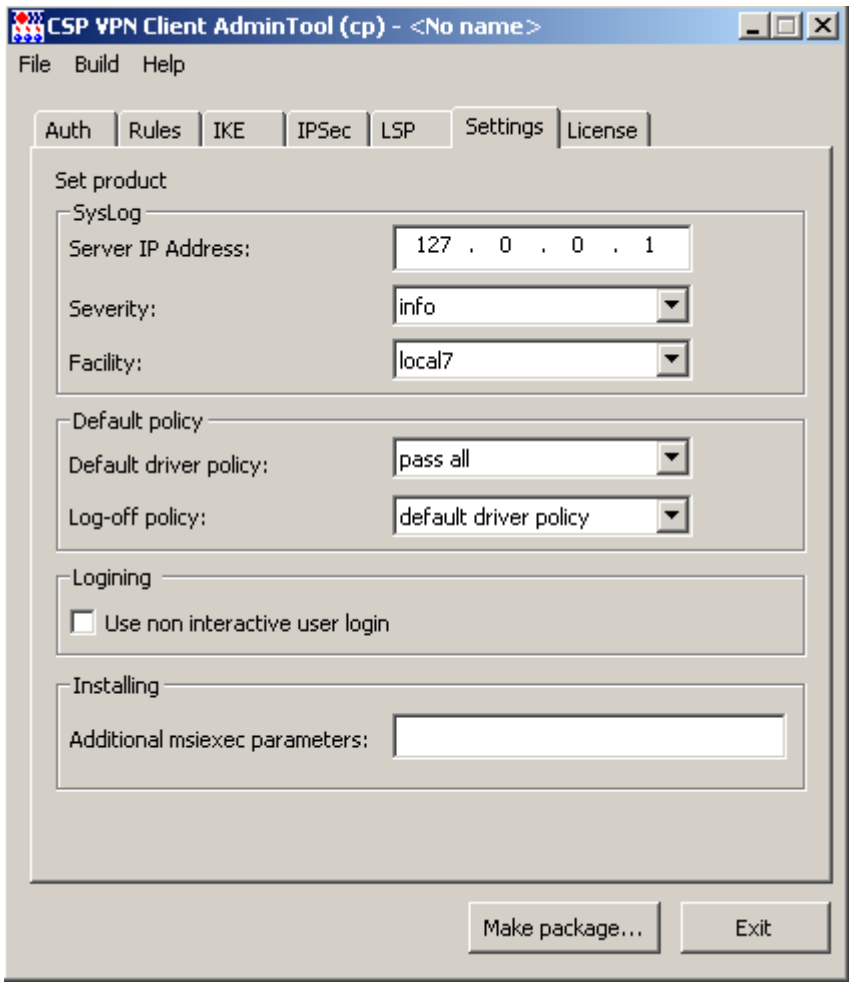


Рисунок 52

Для задания настроек Syslog-клиента заполняются следующие поля:

- **Server IP-Address** – IP-адрес компьютера, на который будут посылаться сообщения о протоколируемых событиях. Значение по умолчанию – 127.0.0.1 означает, что сообщения посылаются на локальный хост.
- **Severity** – задание общего уровня протоколирования. Содержит выпадающий список значений - emerg, alert, crit, err, warning, notice, info, debug. Значение по умолчанию – info. Заданный общий уровень протоколирования используется тогда, когда не задан уровень протоколирования для разных событий во вкладке LSP в окне Advanced LSP Settings переменной Log level.
- **Facility** – задание источника сообщений. Содержит выпадающий список значений – local0, local1, local2, local3, local4, local5, local5, local7. Значение по умолчанию – local7.

Задание политики по умолчанию:

- **Default Driver Policy (DDP)** – политика драйвера по умолчанию. Выпадающий список содержит два значения:
  - правило Passall – пропускать все пакеты. Значение по умолчанию
  - правило PassDHCP – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для конфигурирования TCP/IP стека по протоколу DHCP.

 Copyright © S-Terra CSP 2003 - 2015

Политика DDP, которая задается администратором, загружается в следующих случаях:

- до старта VPN Service
- при остановке VPN Service.

- **Log-off policy** – политика безопасности, которая задается администратором при подготовке инсталляционного пакета, и служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений. Эта политика работает по одному из двух правил:
  - правило Drop All – удалять любой трафик, приходящий на компьютер пользователя
  - правило Default Driver Policy (DDP) – политика драйвера по умолчанию.

Политика Log-off policy загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя
- если при загрузке конфигурации обнаружены ошибки.

Use non interactive user login – при установке этого флажка CSP VPN Client будет использовать неинтерактивный режим логина, а при снятии – интерактивный режим логина:

- неинтерактивный режим – при входе пользователя в систему производится попытка логина с пустым паролем (в качестве пароля используется пустая строка). При таком успешном логине окно с запросом пароля не выводится. При неуспешном логине – Продукт ведет себя как при интерактивном режиме
- интерактивный режим – выдается окно запроса пароля. Этот режим используется по умолчанию.

Additional msiexec parameters – в этом поле можно установить дополнительные параметры запуска WinInstaller.

Например, альтернативный каталог, в который будет установлен Продукт, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

Например, для протоколирования событий в файл C:\Client\install_log_file.txt при инсталляции CSP VPN Client нужно выставить опцию `/l* C:\Client\install_log_file.txt`.

Эту опцию рекомендуется указать, если планируется выбрать режим инсталляции silent.

Для CSP VPN Client можно указать время инициализации VPN сервиса (vpnsvc). В поле дополнительных параметров запуска указывается параметр и его значение, например, `MAX_SERVICE_START_TIMEOUT=45`. Значение по умолчанию для этого параметра равно 30 секундам, максимальное значение – 600 секунд.

 Copyright © S-Terra CSP 2003 - 2015

10.10. Вкладка License

Во вкладке License задаются регистрационные данные Лицензии на Продукт CSP VPN Client:

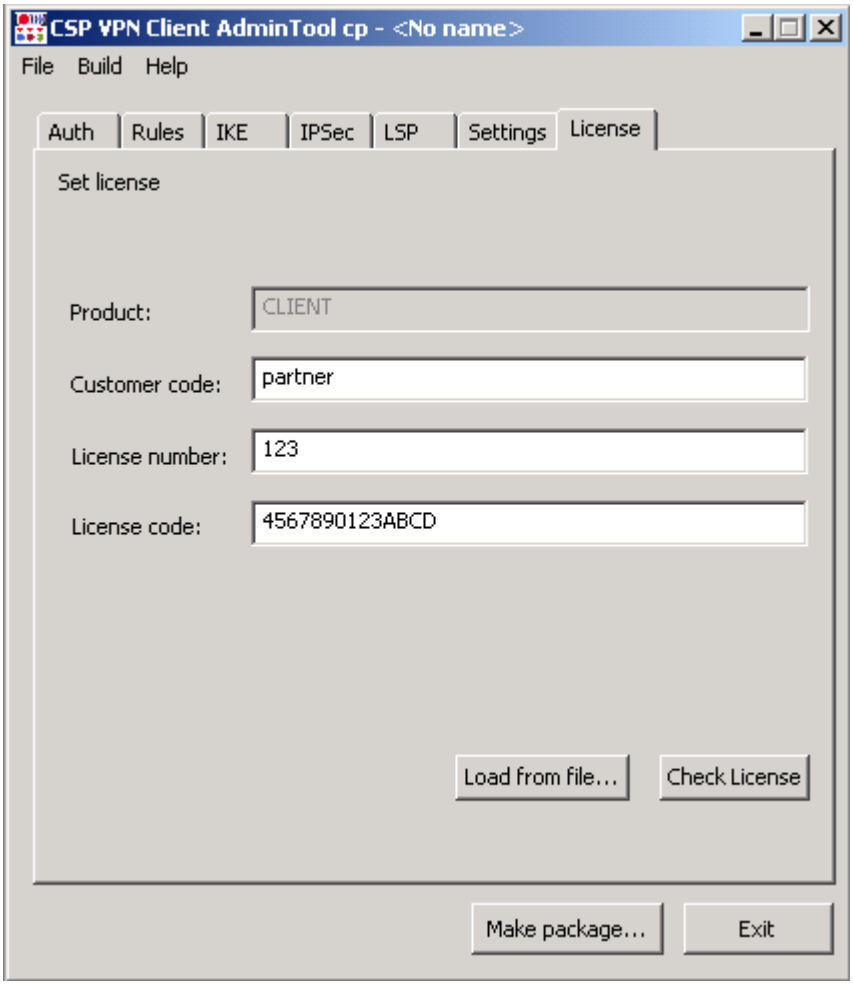


Рисунок 53

Данные Лицензии:

- Product – поле для задания типа Продукта (всегда CLIENT)
- Customer code – код пользователя
- License number – номер лицензии
- License code – код лицензии.

Кнопки управления:

- Load from file – при нажати этой кнопки происходит загрузка данных Лицензии из указанного текстового файла. В файле данные Лицензии должны быть записаны в виде:

```
[license]
CustomerCode=NNNN
ProductCode=CLIENT
LicenseNumber=NNNN
LicenseCode=NNNNNNN
```

- Check License – проверка правильности введенных данных Лицензии.

 Copyright © S-Terra CSP 2003 - 2015

10.11. Advanced project settings

Окно Advanced project settings вызывается через пункт меню File–>Advanced Project Settings. Этот пункт меню активен, если во вкладке Auth выбран метод аутентификации сторон при помощи сертификатов.

Во вкладке Partner certificates можно указать путь к сертификату партнера или промежуточному CA-сертификату, который будет положен в базу локальных настроек продукта при инсталляции. Эту настройку рекомендуется использовать в случаях, когда присутствуют проблемы с передачей сертификатов по протоколу IKE и LDAP.

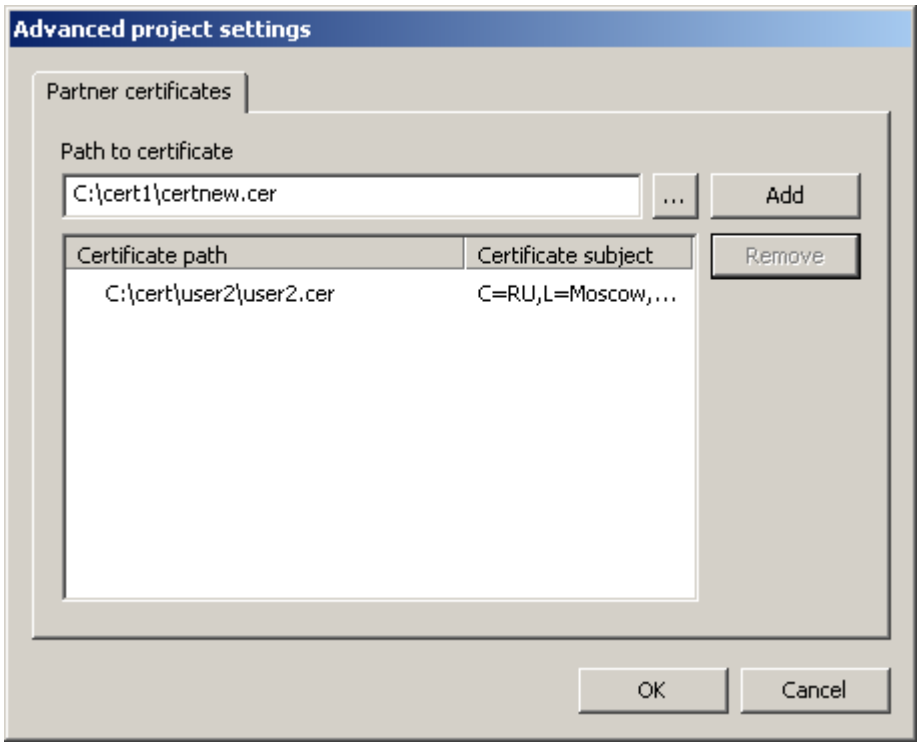


Рисунок 54

Path to certificate – путь к файлу с сертификатом. При нажатии кнопки [...] открывается стандартное диалоговое окно, в котором можно выбрать файл с сертификатом.

Кнопка **Add** – активна, если поле Path to certificate не пустое. При нажатии на кнопку, выбранный сертификат добавляется в список. **Примечание:** из контейнера сертификатов в формате pkcs7 выбирается только первый.

Список сертификатов – содержит сертификаты, которые будут добавлены в инсталляционный пакет. В списке отображается две колонки:

Certificate path – путь к файлу с сертификатом.

Certificate subject – subject сертификата.

Кнопка **Remove** – активна, если в списке есть выделенный сертификат. При нажатии на кнопку, выделенный сертификат удаляется из списка.

 Copyright © S-Terra CSP 2003 - 2015

10.12. Создание инсталляционного файла

Создание инсталляционного файла происходит при нажатии кнопки Make package в главной форме. При этом происходит проверка корректности введенных данных и при обнаружении ошибки выводится сообщение о возможных причинах, и переключение на вкладку с некорректными данными. Если ошибки не обнаружено, то появляется окно Package parameters:

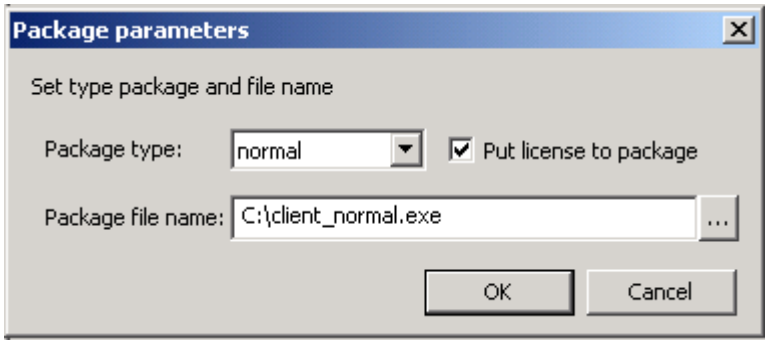


Рисунок 55

В этом окне необходимо задать:

- **Package type** – поле для выбора режима инсталляции. Возможные значения:
  - basic – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию
  - normal – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензионного Соглашения и другими окнами
  - silent – неинтерактивная установка без запросов. Стартует сразу после запуска EXE-файла без дополнительных запросов.
- **Package file name** – поле для ввода имени инсталляционного файла на компьютере администратора.
- **Put license to package** – при установке этого флажка введенные данные Лицензии будут включены в инсталляционный файл. При этом вкладка License должна содержать корректные данные Лицензии.

При нажатии кнопки ОК вызывается утилита make_inst.exe с соответствующими опциями, которая и создает инсталляционный файл. На время работы утилиты появляется окно с просьбой подождать:

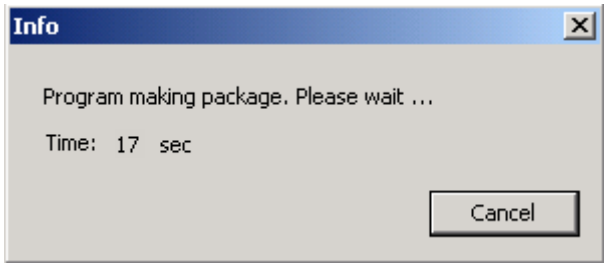


Рисунок 56

В случае выявления ошибки выдается сообщение о коде ошибки.

При нажатии на кнопку Cancel работа утилиты make_inst.exe прерывается (инсталляционный файл не создается). В случае успешного завершения работы утилиты выдается сообщение о создании инсталляционного файла:

 Copyright © S-Terra CSP 2003 - 2015

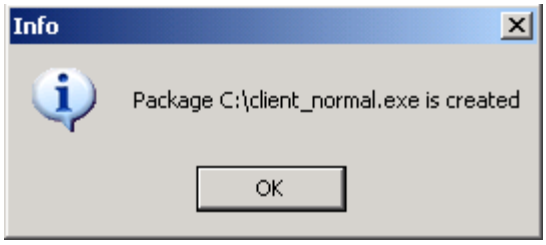


Рисунок 57

Все сообщения, выдаваемые программой утилитой make_inst в процессе ее работы, выводятся в файл make_inst_log.txt (при каждом создании инсталляционного файла make_inst_log.txt переписывается).

 Copyright © S-Terra CSP 2003 - 2015

10.13. Сохранение данных проекта

В процессе сохранения проекта – `Save Project as` (`Save Project`) – сохраняются данные тех вкладок, которые на данный момент являются активными. Данные вкладок, которые являются невидимыми, не сохраняются. Исключение составляет ситуация: при переключении на ручное задание LSP (вкладка LSP, выставлен флажок "Use custom LSP") данные вкладок Rules, IKE и IPSec сохраняются в проекте, не смотря на то, что после переключения эти вкладки являются неактивными и не показываются пользователю. При повторном открытии сохраненного проекта, при переходе к режиму автоматического формирования LSP (снятие флажка "Use custom LSP"), все введенные ранее пользователем данные во вкладках Rules, IKE и IPSec будут доступны для дальнейшего редактирования. Данная особенность реализована для облегчения редактирования LSP при ее автоматическом формировании.

 Copyright © S-Terra CSP 2003 - 2015

10.14. Задание расписания для правил фильтрации

При настройке CSP VPN Client в качестве межсетевого экрана имеется возможность задать расписание работы правил фильтрации. Для этого используются утилиты `uplogin_mgr` и `sfxview`, которые входят в состав дистрибутива административного пакета.

Для настройки расписания правил фильтрации выполните следующие действия:

- файл `sfxview.exe` разместите в каталоге `C:\windows\system32`, а файл `uplogin_mgr.exe` – в каталоге `C:\Program Files\CSP VPN Client`
- создайте инсталляционный файл CSP VPN Client, например, с именем `C:\Configs\policy2.exe`, с правилами фильтрации, которые должны включаться в определенное время
- создайте файл с расширением `.bat` следующего содержания(в данном примере пароль пользователя – 123):

```
mkdir C:\Configs\conf2

sfxview unpack c:\Configs\policy2.exe c:\Configs\conf2

"C:\Program Files\CSP VPN Client\uplogin_mgr.exe" change -p
"123" -n ""

net stop vpnsvc

FOR %%i IN ("C:\Program Files\CSP VPN
Client\db\lsps\000000??") DO copy
"C:\Configs\conf2\OCI\db\lsps\00000001" "%%i"

net start vpnsvc

"C:\Program Files\CSP VPN Client\uplogin_mgr.exe" change -p
"" -n "123"

"C:\Program Files\CSP VPN Client\uplogin_mgr.exe" login -p
"123"

Pause
```

- в случае, если пароль пользователя пустой, скрипт может быть упрощен:

```
mkdir C:\Configs\conf2

sfxview unpack c:\Configs\policy2.exe c:\Configs\conf2

net stop vpnsvc

FOR %%i IN ("C:\Program Files\CSP VPN
Client\db\lsps\000000??") DO copy
"C:\Configs\conf2\OCI\db\lsps\00000001" "%%i"

net start vpnsvc

"C:\Program Files\CSP VPN Client\uplogin_mgr.exe" login -p ""

pause
```

- используйте планировщик заданий Windows для задания момента времени, в который будут включаться правила фильтрации, заданные в конфигурации policy2.exe, и укажите на выполнение созданный `.bat` файл.

Аналогичным образом можно создать неограниченное количество конфигураций с разными правилами фильтрации и задать для них расписание для применения.

Замечание: при заданном пароле пользователя для аутентификации в продукт CSP VPN Client база данных с политикой безопасности, локальными настройками, аутентификационными данными (предопределенными ключами, сертификатами) хранится в зашифрованном виде, при изменении пароля – база данных

перешифровывается. Для замены в базе данных одной политики безопасности на другую (замены одних правил фильтрации на другие) база данных должна быть в незашифрованном виде, а следовательно, пароль пользователя нужно изменить на пустой. После замены одной политики на другую прежний пароль пользователя восстанавливают.

10.15. Формат задания имен алгоритмов в файле admintool.ini

Имена алгоритмов, используемые во вкладках IKE, IPSec и LSP, задаются в файле `admintool.ini` в секции `[algorithm_names]`. Пример приведен ниже. Наименование алгоритма справа от знака равенства остается неизменным, а присваиваемое значение может быть взято из структурах AHTransform, ESPTransform, IKETransform, описанных в разделе «Создание локальной политики безопасности. Конфигурационный файл».

Для большей наглядности разрешается назначать алгоритмам пользовательские псевдонимы (в этом случае во вкладках IKE и IPSec будут отображаться не реальные имена, а назначенные псевдонимы). Для задания псевдонима необходимо дополнить строку имени алгоритма именем псевдонима, заключенного в круглые скобки:

```
[algorithm_names]
ike-hash=GR341194CPRO1-65534 (ГОСТ Р 34.11-94)
ike-cipher=G2814789CPRO1-K256-CBC-65534 (ГОСТ 28147-89)
ah-integrity=GR341194CPRO1-H96-HMAC-254 (ГОСТ Р 34.11-94)
esp-integrity=GR341194CPRO1-H96-HMAC-65534 (ГОСТ Р 34.11-94)
esp-cipher=G2814789CPRO1-K256-CBC-254 (ГОСТ 28147-89)
```

 Copyright © S-Terra CSP 2003 - 2015

11. Подготовка к инсталляции CSP VPN Client

Перед установкой Продукта CSP VPN Client на компьютере пользователя выполните следующие предварительные действия:

1. установите программный продукт СКЗИ "КриптоПро CSP 3.6/3.6R2", если он еще не установлен. Установка описана в Приложении "Установка СКЗИ "КриптоПро CSP 3.6/3.6R2"
2. инсталлируйте ключевой считыватель Реестр для временного контейнера, создаваемого в процессе инсталляции CSP VPN Client, в который будет записано начальное значение ДСЧ. Такая инсталляция описана в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2". Если аутентификация партнеров осуществляется с использованием сертификатов, то временный контейнер для ДСЧ может быть размещен на том же носителе, что и контейнер с секретным ключом, в этом случае перейдите к выполнению следующего действия
3. если аутентификация сторон осуществляется на основе сертификатов и контейнер с секретным ключом сертификата находится не на дискете, а на другом внешнем ключевом носителе, то сначала подключите считыватель этого ключевого носителя как описано в разделе "Подключение внешних ключевых считывателей". Затем инсталлируйте считыватель и ключевой носитель. Такая инсталляция изложена в разделе "Инсталляция внешнего считывателя и ключевого носителя в "КриптоПро CSP 3.6/3.6R2". Если же контейнер с секретным ключом находится в Реестре, то этот считыватель ключевой информации уже инсталлирован.
4. В ОС Windows XP Embedded имеются некоторые особенности в подготовке ОС, которые следует учесть перед инсталляцией CSP VPN Client, описанные в разделе «Подготовка ОС Windows XP Embedded к инсталляции».

 Copyright © S-Terra CSP 2003 - 2015

11.1. Подготовка ОС Windows XP Embedded к инсталляции

Предполагается, что используется некоторый типичный вариант установки Windows XP Embedded для формирования работоспособной клиентской среды, в которой запускаются и работают большинство программ для Windows XP. В этом варианте обязательно должны присутствовать сетевые компоненты, Windows Installer, GUI и т.п.

Далее в таблице перечислены необходимые компоненты ОС, которые могут отсутствовать в типичном варианте установки Windows XP Embedded. Желательно, чтобы данные компоненты были добавлены при сборке образа ОС.

Таблица 1

Необходимый компонент	DLL для обходного решения
Performance Data Helper	pdh.dll, odbcbcp.dll
Quality of Service Traffic Control	traffic.dll

Если данные компоненты не были добавлены, то после инсталляции CSP VPN Client используйте DLL для обходного решения. Данные DLL возьмите из той же версии ОС XP Embedded либо из стандартной ОС Windows XP Professional (каталог `C:\WINDOWS\System32`) и скопируйте указанные DLL в каталог Продукта.

> Выполните копирование вручную после того, как инсталлятор создаст каталог Продукта. Это желательно сделать до запуска сервиса vpnsvc. Если файлы не будут скопированы до попытки старта сервиса, будет выдано сообщение об ошибке 1920 (`"Service 'CSP VPN Service' (vpnsvc) failed to start. Verify that you have sufficient privileges to start system services."`). Скопируйте требуемые DLL и нажмите кнопку Retry.
>
> **Внимание!** Перед копированием убедитесь, что указанные файлы действительно отсутствуют в каталоге `C:WINDOWS\System32`.

В некоторых системах во время инсталляции могут появляться сообщения о нехватке свободного места на диске, несмотря на то, что на системном диске свободного места достаточно. Эта ситуация может быть вызвана тем, что каталог %TEMP% (%TMP%) указывает на маленький RAM-диск.

Для обхода этой проблемы:

- создайте временный каталог на системном диске (например, `C:\TEMP`)
- переопределите переменные окружения TEMP и TMP, указав в них полный путь к данному каталогу:
  - нажмите правой кнопкой на "`My Computer`", далее `Properties -> Advanced -> Environment Variables`; в разделе "`User variables for Administrator`" поменяйте значения TEMP и TMP.

После завершения инсталляции верните данные переменные в исходное значение, а также удалите временный каталог.

Для массовых установок можно написать скрипт или или BAT-файл, выполняющий вышеперечисленные действия.

 Copyright © S-Terra CSP 2003 - 2015

12. Инсталляция CSP VPN Client

Установка программного Продукта CSP VPN Client на компьютере пользователя осуществляется запуском инсталляционного файла, подготовленного и переданного администратором безопасности пользователю.

Инсталляция должна производиться пользователем, имеющим права администратора.

Если контейнер с секретным ключом пользователя находится на дискете, то дискета должна быть вставлена в дисковод.

После запуска файла для установки CSP VPN Client инсталляция происходит в одном из 3 режимов, который был выбран администратором при подготовке инсталляционного файла:

- **режим basic** – основной режим, неинтерактивная установка с запросом на инсталляцию, вариант по умолчанию
- **режим normal** – интерактивная установка
- **режим silent** – неинтерактивная установка без запросов.

Если при подготовке инсталляционного файла администратор включил копирование контейнера с секретным ключом с внешнего ключевого носителя на другой, например, в Реестр, то копирование произойдет в процессе установки CSP VPN Client. Подробное описание копирования размещено в разделе "Копирование контейнера при инсталляции".

Все протоколируемые события при инсталляции CSP VPN Client будут записываться в файл, если администратор задал его при создании инсталляционного файла пользователя.

При возникновении ошибок во время инсталляции или работы Продукта устраните их и попытайтесь повторно провести инсталляцию Продукта. При появлении сбоев во время работы Продукта перезагрузите компьютер, но если перезагрузка не устраняет проблему – обратитесь в службу поддержки по адресу mailto:support@s-terra.com.

При инсталляции CSP VPN Client происходит отключение стандартного сервиса, связанного с IPsec и IKE, и перевод его в состояние Manual. В Windows XP и Windows Server 2003 – это Служба IPSEC, внутреннее название которой PolicyAgent. В Windows Vista, Windows Server 2008 и Windows 7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT).

В ОС Windows Vista, Windows Server 2008 и Windows 7 производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке CSP VPN Client в Windows FireWall добавляется новое правило:

- правило для входящих подключений
- имя – CSP VPN Service – UDP allowed (predefined)
- правило включено
- действие – разрешить подключение
- протокол – UDP (все порты)
- программа – полный путь к установленному файлу vpnsvc.exe
- службы – применятьтолько к службам
- профили – все профили
- остальные параметры – по умолчанию.

 Copyright © S-Terra CSP 2003 - 2015

Эти настройки можно посмотреть следующим образом: Панель управления – Администрирование – Брандмауэр Windows в режиме повышенной безопасности – Правила для входящих подключений.

12.1. Режим basic

В ОС Windows **Vista/Windows Server 2008/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 58). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

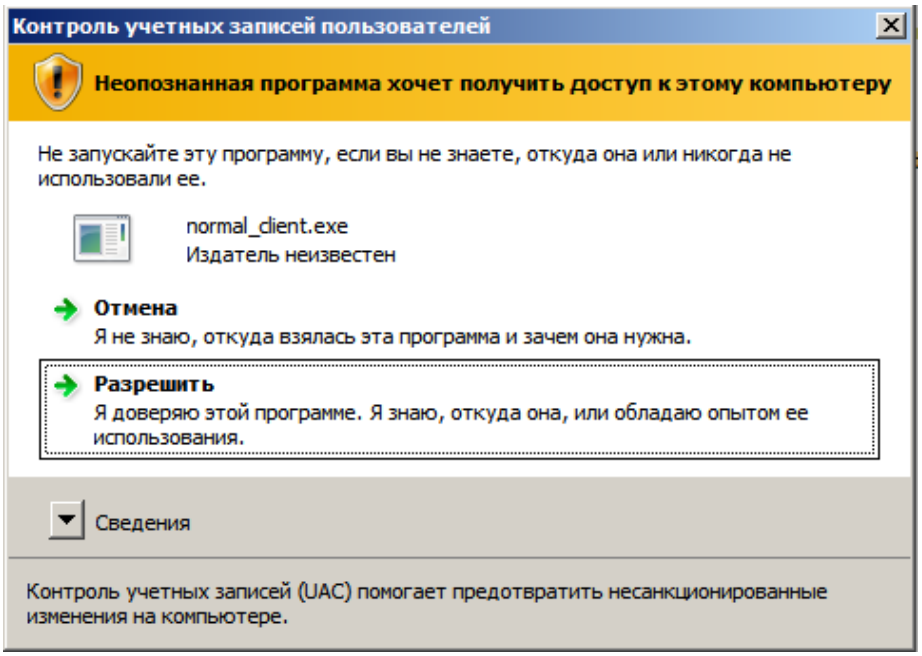


Рисунок 58

Затем выдается запрос на инсталляцию CSP VPN Client (в ОС Windows XP и Windows Server 2003 это окно появляется первым):

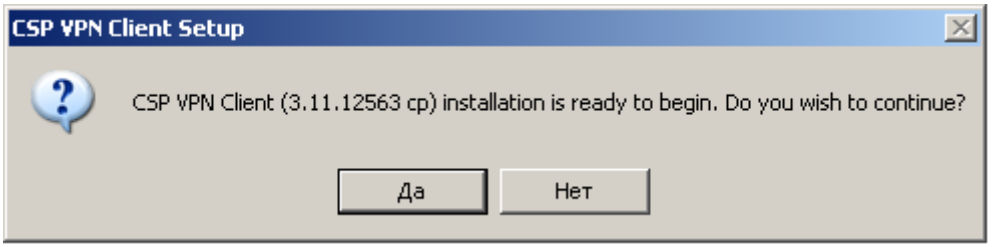


Рисунок 59

После нажатия кнопки Да происходит установка Продукта:



Рисунок 60

 Copyright © S-Terra CSP 2003 - 2015

Появляется окно с индикатором процесса инсталляции:

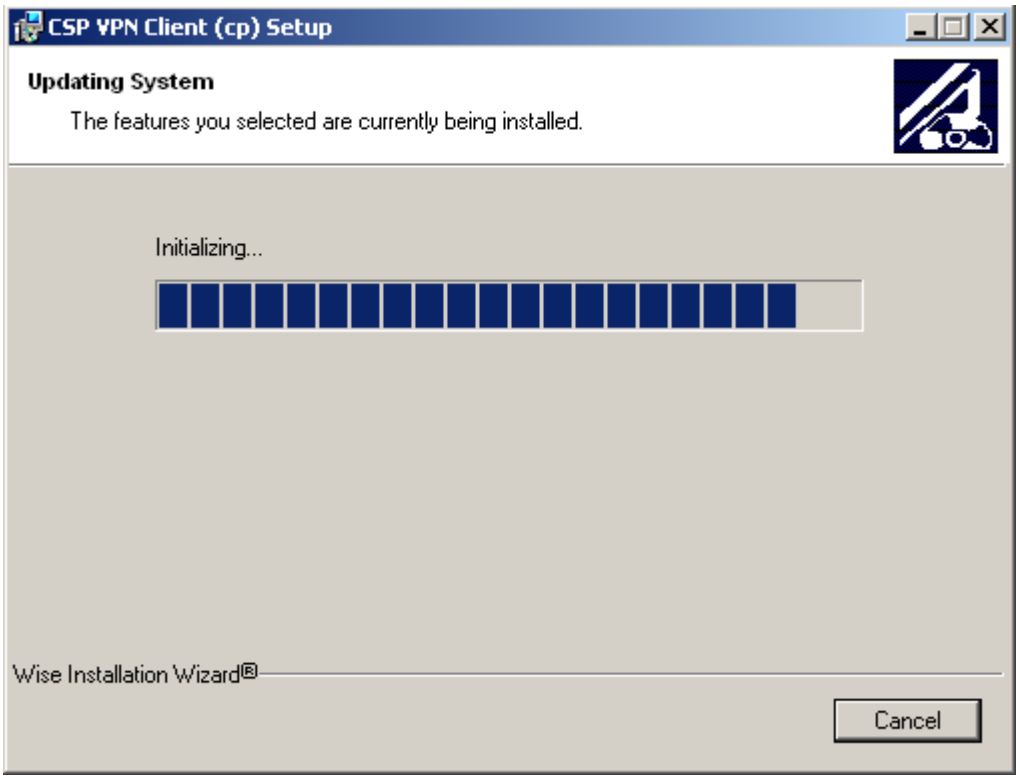


Рисунок 61

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель:

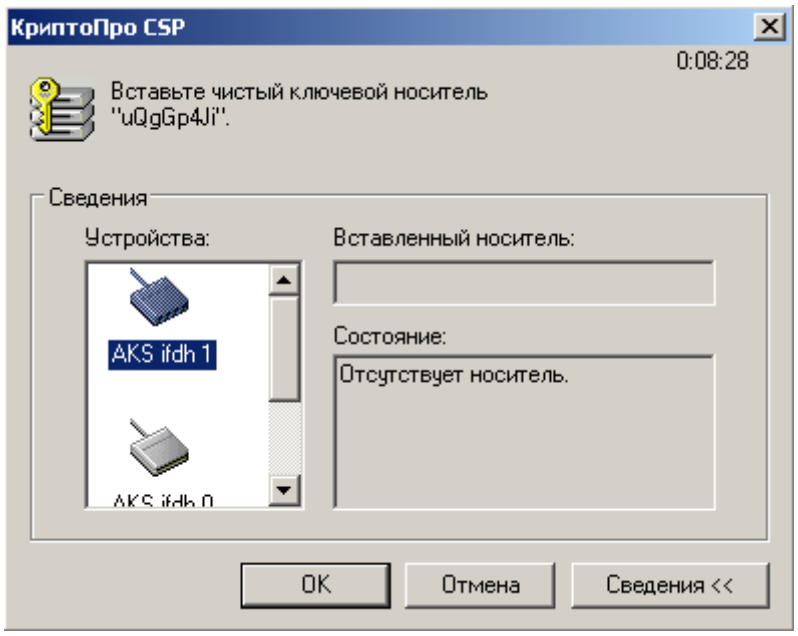


Рисунок 62

 Copyright © S-Terra CSP 2003 - 2015

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

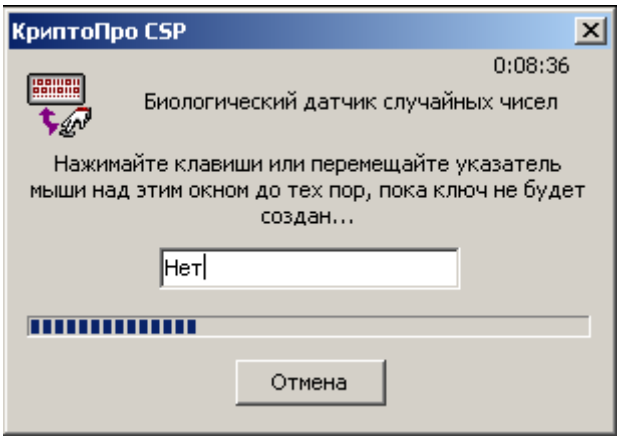


Рисунок 63

При инсталляции в ОС **Windows Vista/Windows Server 2008/Windows 7** появляется окно (Рисунок 64) с запросом на установку драйверов. Выберите предложение – Все равно установить этот драйвер.

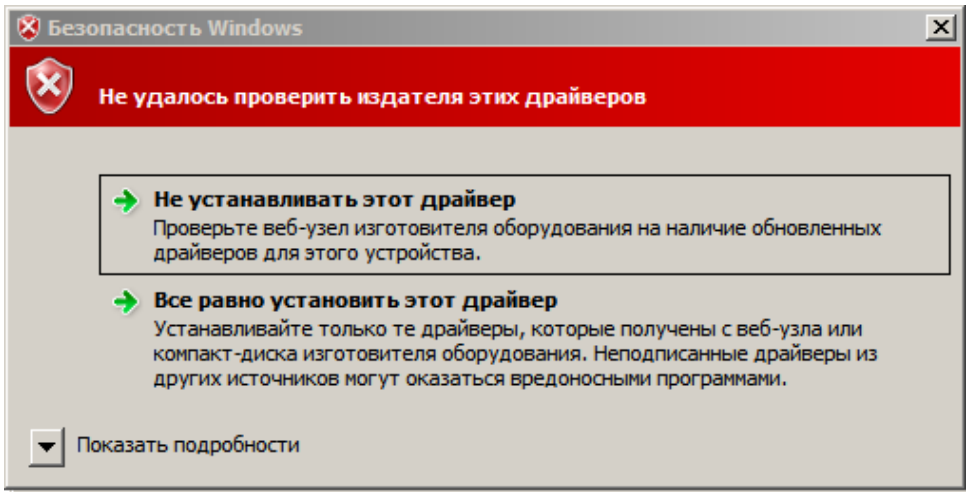


Рисунок 64

 Copyright © S-Terra CSP 2003 - 2015

При инсталляции в ОС **Windows XP/Windows Server 2003** если реакция системы Windows на установку неподписанных драйверов установлена в положение `Предупреждать` (`Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Предупреждать`), то возможно появление окна (Рисунок 65) для подтверждения установки VPN Filter на интерфейс. Таких окон может появиться несколько. Для продолжения процесса инсталляции нажмите кнопку `Все равно продолжить` в каждом из этих окон:

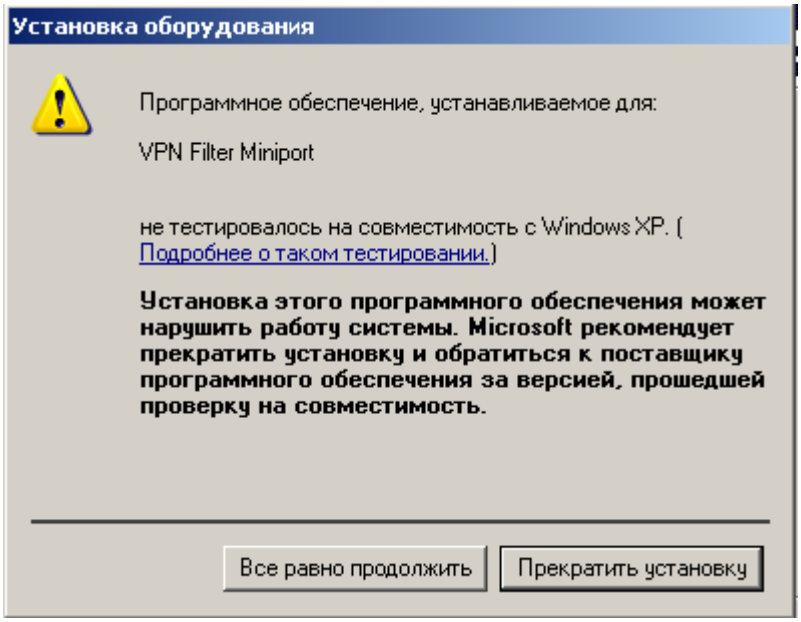


Рисунок 65

Для отключения возможности появления такого окна, установите реакцию системы Windows на установку неподписанных драйверов в положение `Пропускать (Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Пропускать)`.

При инсталляции в ОС **Windows XP Embedded**, при установке драйверов не показывается предупреждение об установке неподписанных драйверов (вне зависимости от соответствующей системной настройки).

При попытке установки драйвера vpndrvr, система может не найти файлы vpndrvr.sys, netvpn_m.inf, которые изначально располагаются в директории Продукта, и выдать окно с запросом на указание пути к одному из этих файлов:

```
The file '<имя_файла>' on VPN Filter Disk is needed.
Type the path where the file is located, and then click OK.
Copy files from:...
```

Укажите директорию Продукта по кнопке `Browse...`

По окончании установки CSP VPN Client выдается окно (Рисунок 84) с предупреждением о необходимости перезагрузки операционной системы.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта.

 Copyright © S-Terra CSP 2003 - 2015

12.2. Режим normal

В ОС **Windows Vista/Windows Server 2008/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 58). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

Этот режим является диалоговым режимом. Открывается стартовое окно визарда с приглашением к инсталляции:



Рисунок 66

После нажатия кнопки Next будет открыто окно визарда с текстом Лицензионного Соглашения. После установки переключателя в положение "`I accept the license agreement`" будет доступна кнопка Next:

 Copyright © S-Terra CSP 2003 - 2015

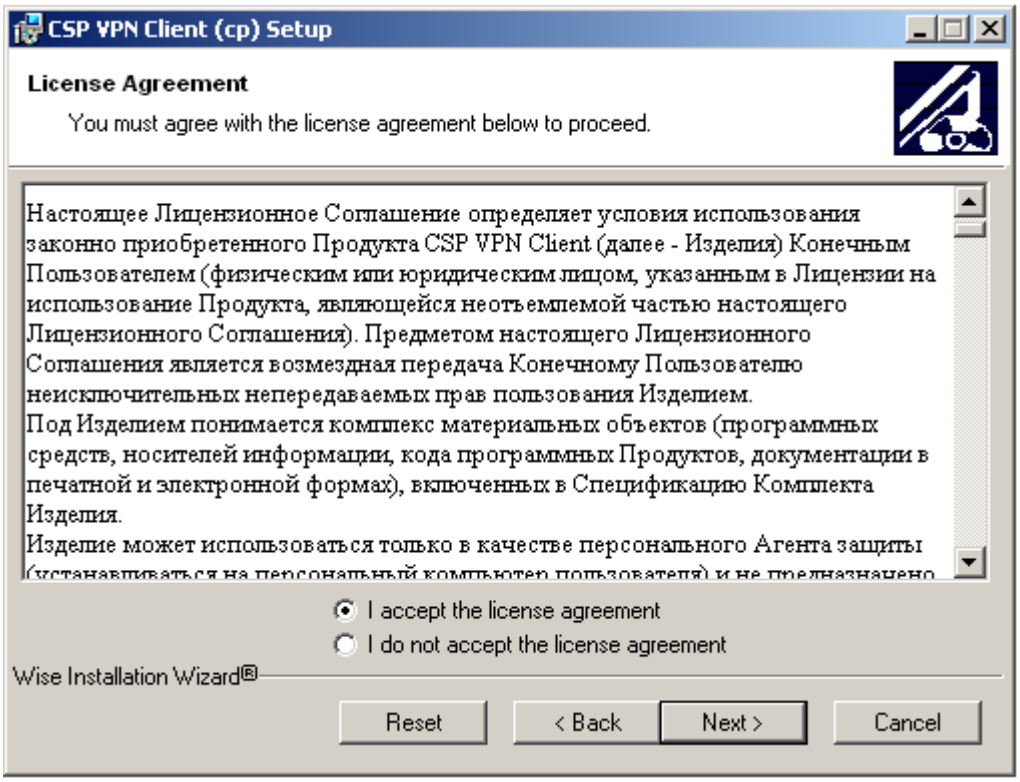


Рисунок 67

Для указания папки, в которую будет установлен Продукт, нажать кнопку Browse и сделать выбор:

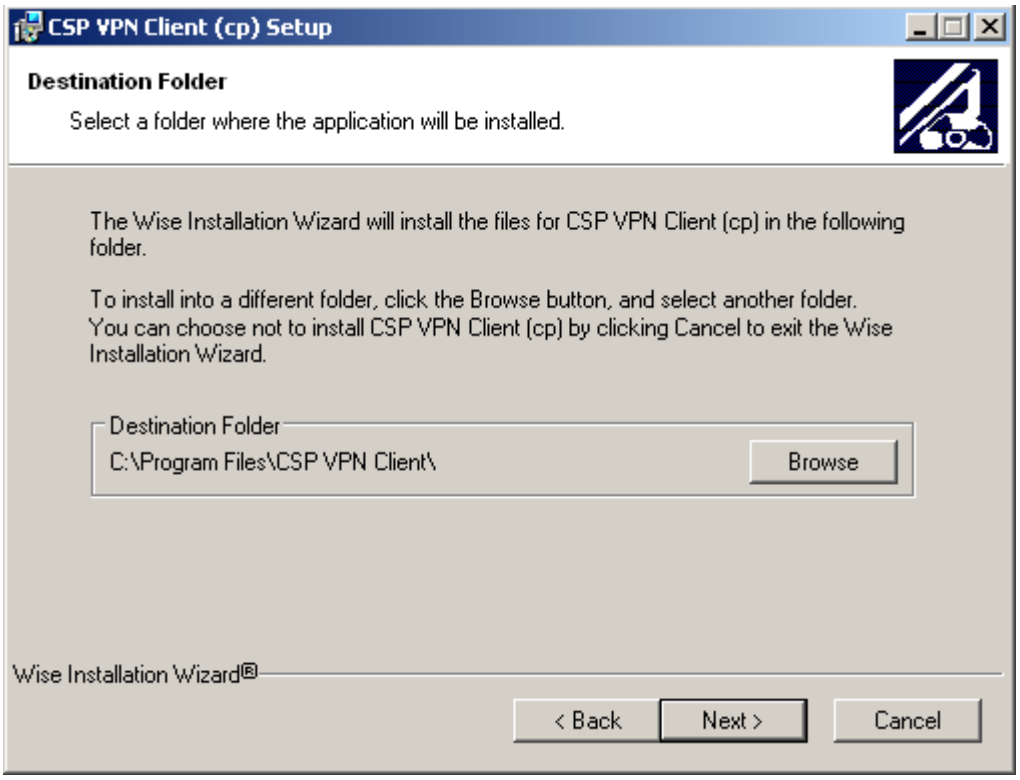


Рисунок 68

Если при создании инсталляционного файла регистрационные данные Лицензии на Продукт CSP VPN Client не были включены в инсталляционный файл, то появится окно для ввода данных Лицензии на Продукт:

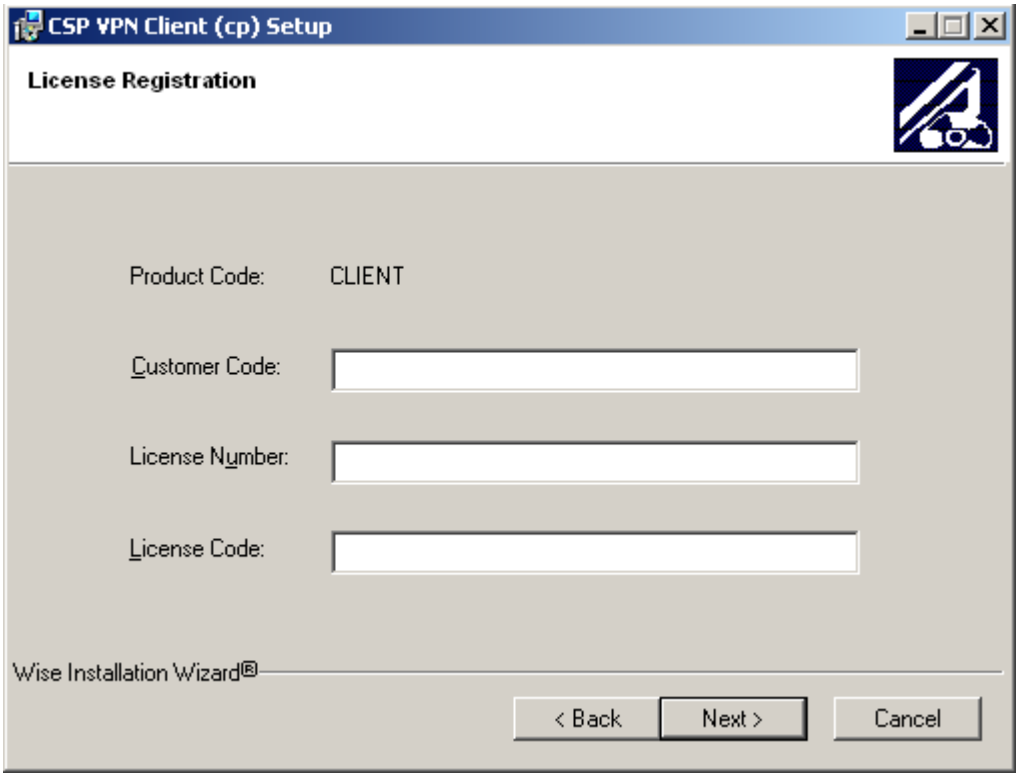


Рисунок 69

Стандартное окно визарда сообщает о готовности к инсталляции. Для начала инсталляции нажать Next:

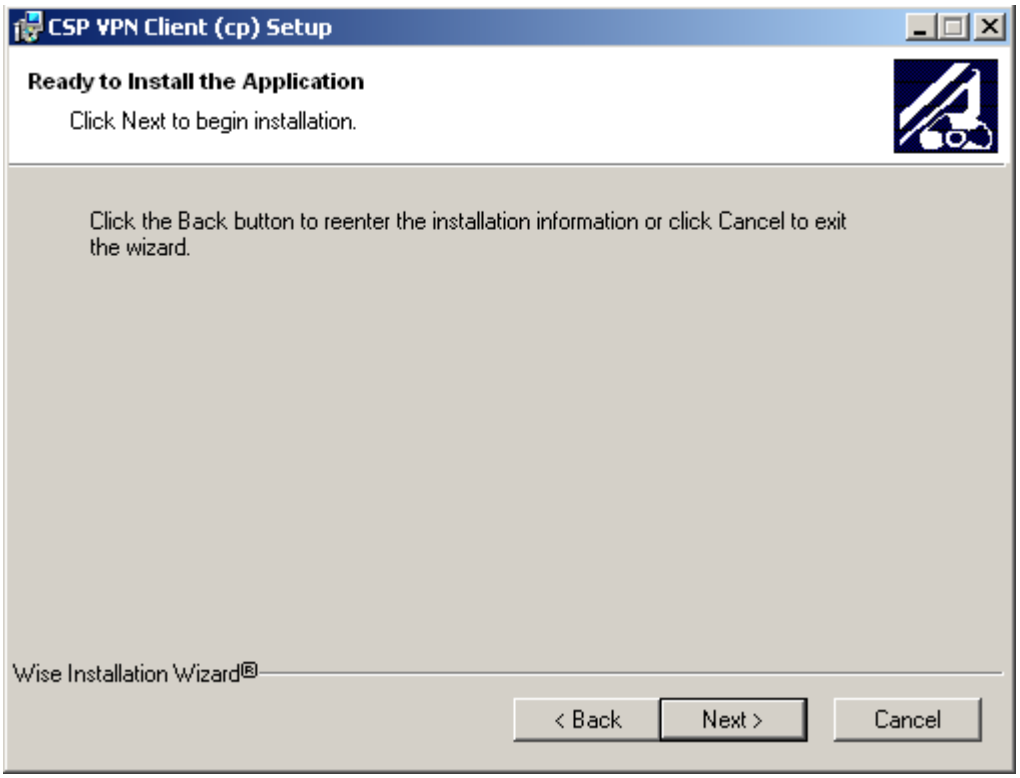


Рисунок 70

 Copyright © S-Terra CSP 2003 - 2015

Далее появляется окно с индикатором процесса инсталляции:

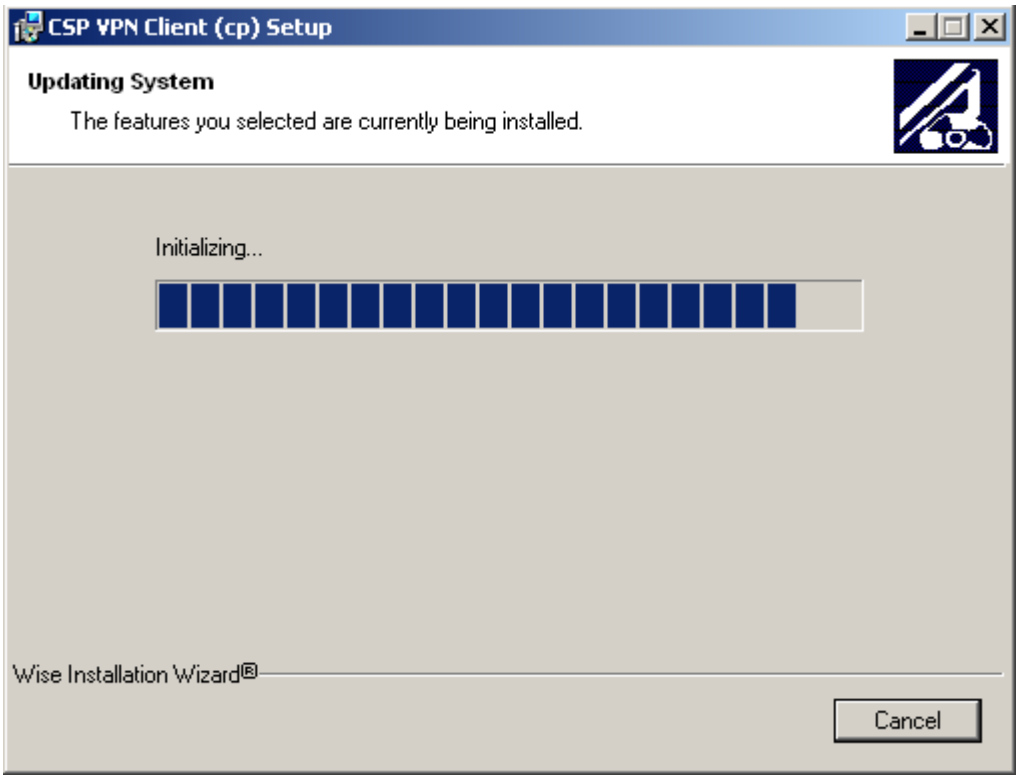


Рисунок 71

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель:

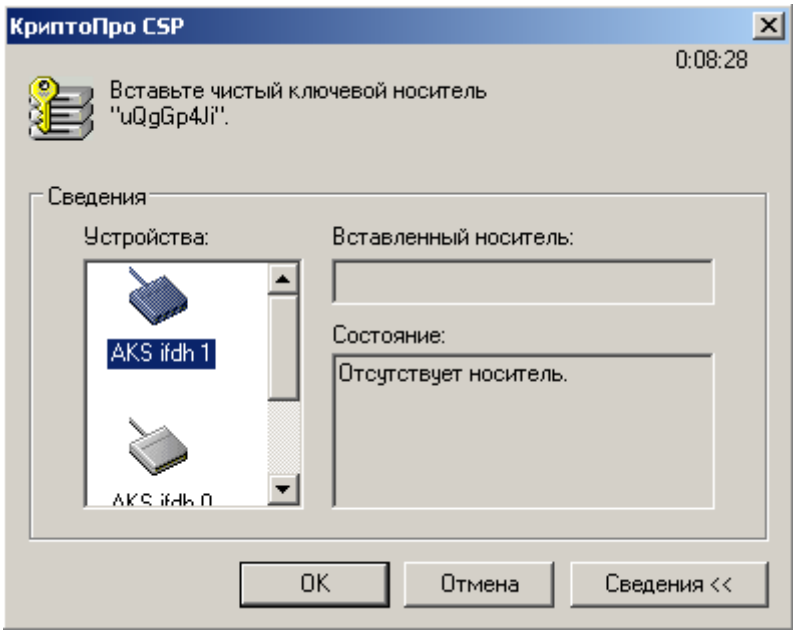


Рисунок 72

 Copyright © S-Terra CSP 2003 - 2015

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

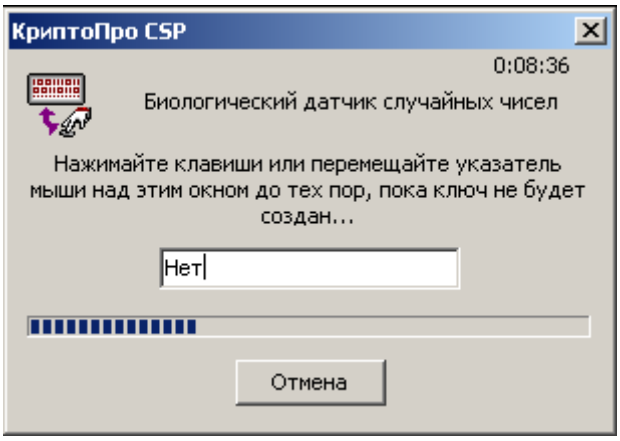


Рисунок 73

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

После завершения процедуры инсталляции нажать Finish:

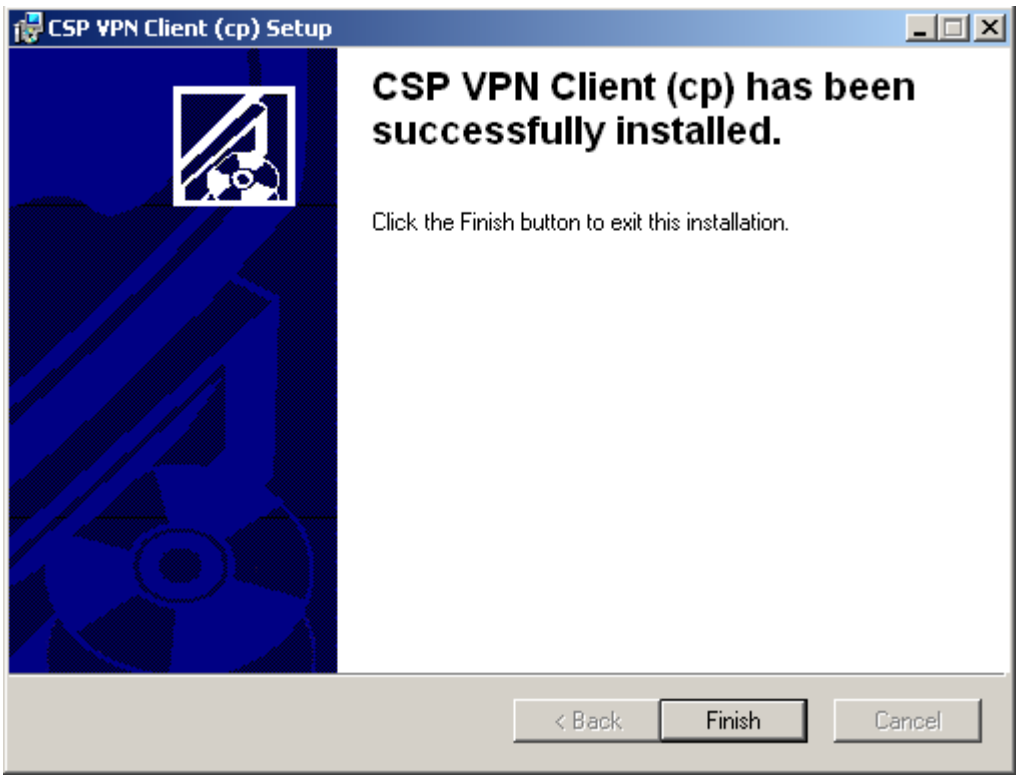


Рисунок 74

По окончании установки CSP VPN Client выдается окно (Рисунок 84) с предупреждением о необходимости перезагрузки операционной системы.

 Copyright © S-Terra CSP 2003 - 2015

12.3. Режим silent

В ОС **Windows Vista/Windows Server 2008/Windows 7** при установке CSP VPN Client выдается окно (Рисунок 58). Необходимо разрешить запуск инсталлятора – выберите предложение Разрешить.

В режиме silent происходит установка CSP VPN Client без запросов, но могут появляться либо системные диалоговые окна, либо некоторые интерактивные компоненты, относящиеся к криптоподсистеме.



Рисунок 75

Создается контейнер, в который будет записано начальное значение ДСЧ. Если ключевой считыватель Реестр уже инсталлирован, то в него и будет записан контейнер. Если Реестр не инсталлирован, то появится окно с предложением выбрать ключевой носитель:

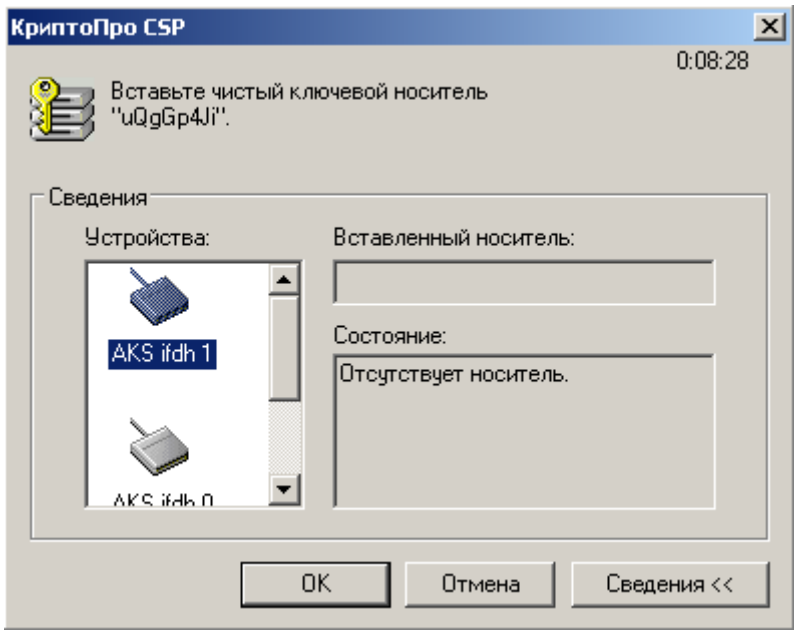


Рисунок 76

Предлагается «биологическая» инициализация ДСЧ – понажимайте клавиши или перемещайте указатель мыши:

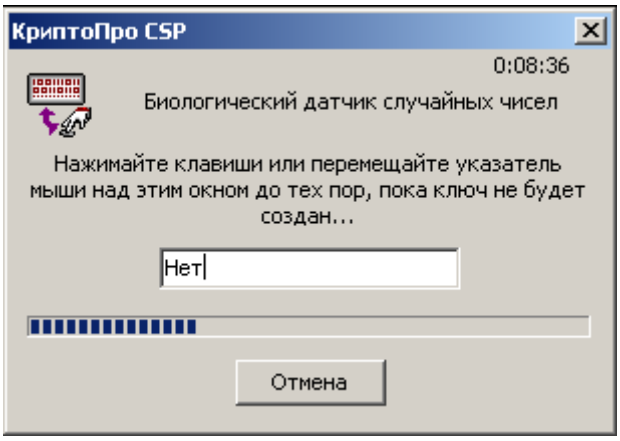


Рисунок 77

 Copyright © S-Terra CSP 2003 - 2015

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

По окончании установки CSP VPN Client происходит перезагрузка операционной системы без предупреждений.

В случае возникновения ошибок и прерывания инсталляции никакие сообщения на экран не выводятся. Эти сообщения можно посмотреть программой ОС Windows «Просмотр событий» или, если при подготовке инсталляционного пакета Администратором была указана опция протоколирования событий при инсталляции в файл, то сообщения можно посмотреть в заданном файле.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта.

12.4. Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов было задано копирование контейнера, то такое копирование контейнера с секретным ключом будет происходить при инсталляции CSP VPN Client.

В случае, если контейнер, в который происходит копирование уже существует, то выдается окно следующего вида:

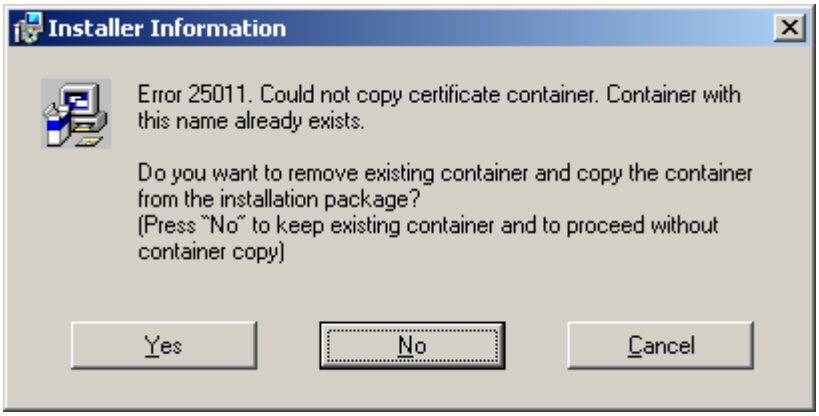


Рисунок 78

Если нажать "Yes", то существующий контейнер будет удален и процедура копирования будет продолжена. Если нажать "No", существующий контейнер останется, а процедура копирования будет отменена. Если нажать "Cancel", то инсталляция клиента будет прервана.

Опишем последовательность действий при копировании контейнера с внешнего ключевого носителя, например, дискеты, в Реестр так, как оно выглядит для пользователя.

В первом окне предлагается установить внешний ключевой носитель в устройство считывания, с которого будет производиться копирование контейнера, например, дискету. Это окно не появляется, если ключевой носитель уже установлен (например, дискета вставлена в дисковод):

 Copyright © S-Terra CSP 2003 - 2015

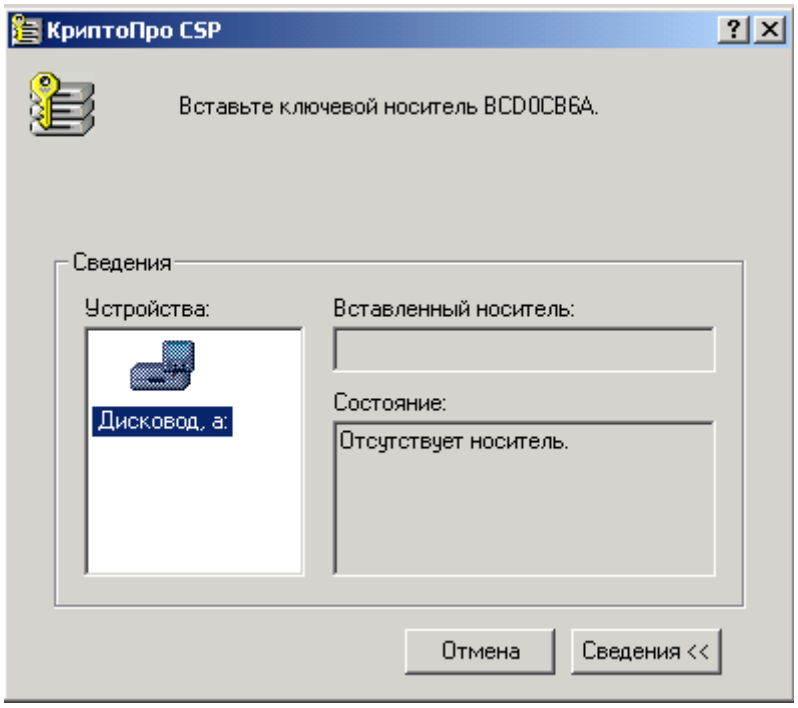


Рисунок 79

Отображается работа утилиты копирования:

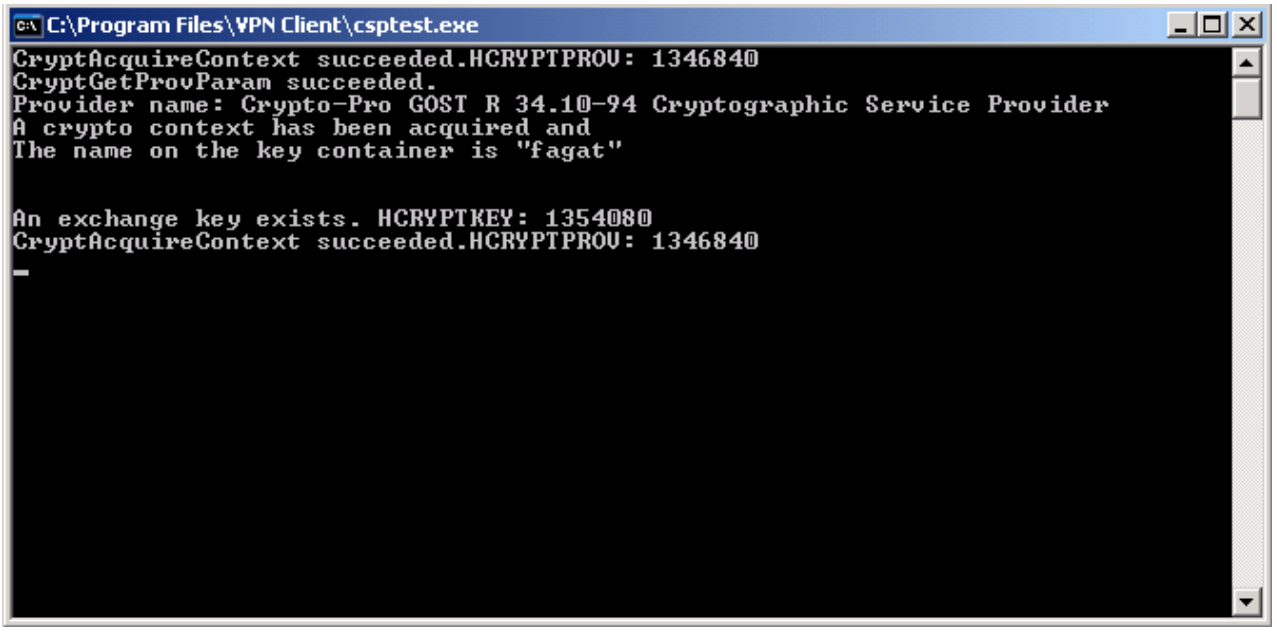


Рисунок 80

 Copyright © S-Terra CSP 2003 - 2015

Если исходный контейнер защищен паролем, а при подготовке инсталляционного файла он не был задан, то появляется окно с запросом пароля:

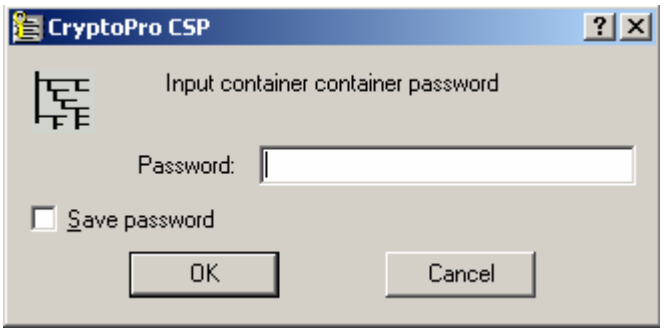


Рисунок 81

В окне с запросом пароля для нового контейнера надо ввести пароль, который обязательно должен совпадать с указанным паролем при подготовке инсталляционного файла. Если используется пустой пароль, достаточно нажать OK:

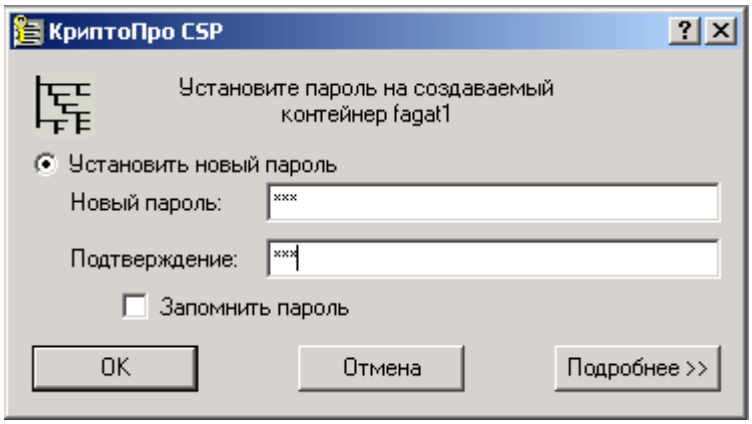


Рисунок 82

Если при копировании возникли ошибки, в текстовом окне появляется сообщение об ошибке и предложение нажать на Enter:



Рисунок 83

Если копирование прошло без ошибок, текстовое окно просто закрывается. Инсталляция Продукта продолжается.

Примечание: если инсталляции происходит в режиме `silent`, и на компьютере пользователя уже существует контейнер с указанным именем, в который происходит копирование, то инсталляция прерывается без выдачи на экран каких-либо запросов пользователю.

 Copyright © S-Terra CSP 2003 - 2015

12.5. Перезагрузка операционной системы

После установки CSP VPN Client в режимах `basic` и `normal` открывается окно, сообщающее о необходимости перезагрузки операционной системы:

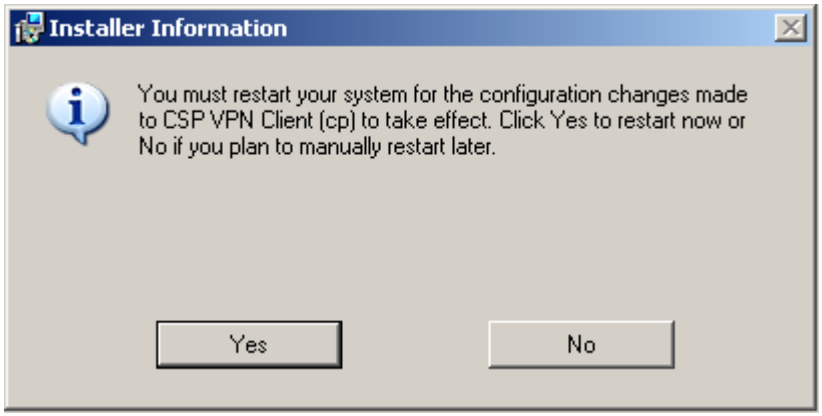


Рисунок 84

После нажатия кнопки Yes происходит перезагрузка операционной системы, а нажатие кнопки No закрывает окно без перезагрузки.

12.6. Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут появляться при инсталляции CSP VPN Client.

Таблица 2

	Текст сообщения	Примечание
25001	License check failed.	Неправильная лицензия
25002	CryptoPro must be installed before the product installation.	Перед установкой Продукта должно быть установлено CryptoPro
25006	RNG initialization failed. {Reason: <reason>.} Installation aborted, где <reason> может быть одной из следующих: Random initialization tool returned an error You must have Administrator privileges Random initialization tool not found Random initialization tool can't run: system error Random value initialization failed В отдельных случаях Reason может отсутствовать	Не удалось создать RNG контейнер. {Причина: <reason>} Инсталляция прервана, где причина может быть одной из следующих: Утилита для инициализации ДСЧ вернула ошибку Вы должны иметь администраторские привилегии Утилита для инициализации ДСЧ не найдена Не удалось запустить утилиту для инициализации ДСЧ: системная ошибка Инициализация ДСЧ провалилась

 Copyright © S-Terra CSP 2003 - 2015

	Текст сообщения	Примечание
25009	Copy certificate container failed. {Reason: <reason>.} Installation aborted. Source container path: <src>. Destination container path: <dst>.	Не удалось скопировать сертификатный контейнер. {Причина: <reason>} Инсталляция прервана. Путь к исходному контейнеру: <src>. Путь к новому контейнеру: <dst>.
25011	Could not copy certificate container. Container with this name already exists. Do you want to remove existing container and copy the container from the installation package? (Press “No” to keep existing container and to proceed without container copy)	Нельзя скопировать сертификатный контейнер, поскольку контейнер с таким именем уже есть. Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета? (Нажмите “No” для того, чтобы сохранить существующий контейнер и продолжить без копирования)
25016	Version {<Version> } of CryptoPro CSP is not supported. CryptoPro CSP version 3.6 must be installed before the product installation	Версия <Version> продукта КриптоПро CSP не поддерживается. Должно быть установлено КриптоПро CSP версии 3.6 до инсталляции продукта. Примечания: <Version> в сообщении может отсутствовать, если ее не удалось определить Для версии 3.6 с build меньше, чем 5402, к <Version> добавляется приписка “(beta)” К <Version> добавляется приписка “(unrecognized)”, если по каким-либо причинам не удалось определить build КриптоПро CSP.
25017	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен Продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	You must have Administrator privileges	Вам необходимы администраторские привилегии
	This product needs Windows 2000 or higher	Для Продукта необходима Windows 2000 или выше
25019	The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead.	**[Windows XP, Windows Server 2003]** Файл <dll_path> был ошибочно помечен, как предыдущая GINA DLL. Будет использована системная GINA DLL.
25020	The previous GINA DLL "<dll_path>" was not found. The system GINA DLL will be used instead.	**[Windows XP, Windows Server 2003]** Предыдущая GINA DLL <dll_path> не найдена. Будет использована системная GINA DLL.
25021	Driver "<driver_name>" installation failed. Product installation aborted.	Не удалось установить драйвер <driver_name>. Инсталляция продукта прервана.

 Copyright © S-Terra CSP 2003 - 2015

	Текст сообщения	Примечание
25022	Product "<Product_name version>" was advertised. You should uninstall it first before the installation.	Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement). Вы должны деинсталлировать его до инсталляции.
25023	There is no CryptoPro CSP driver library installed on the system. You should install it first before the installation. Product installation aborted.	Не установлена драйверная библиотека КриптоПро CSP. Вы должны инсталлировать ее до инсталляции продукта. Инсталляция продукта прервана.
25025	Windows Firewall setup failed.	**[Vista, Windows 2008, Windows 7]** Не удалось настроить Windows Firewall.
25026	You must have administrator privileges.	Вам необходимы администраторские привилегии.
25032	Version {<Version> } of CryptoPro CSP is higher than the supported one. It could be incompatible with the product. Do you want to continue the installation?	Версия КриптоПро CSP больше, чем поддерживаемая. Она может быть несовместима с продуктом. Продолжить инсталляцию?

13. Регистрация пользователя

При подготовке инсталляционного пакета возможно было установить интерактивный или неинтерактивный режим логина в Продукт.

ОС Windows XP/Windows Server 2003

В ОС Windows XP/Windows Server 2003 после перезагрузки ОС при интерактивном режиме появляется окно логина (Рисунок 89) в Продукт (см. раздел “Интерактивный режим логина в Продукт”). Это окно появляется только после инициализации VPN сервиса (см. раздел “Время инициализации VPN сервиса”).

Окно логина в ОС Windows XP появляется только после регистрации пользователя в Продукте или отказе от нее.

При неинтерактивном режиме логина в Продукт или переключении на него см. раздел “Неинтерактивный режим логина в Продукт”.

ОС Windows Vista/Windows Server 2008//Windows 7

В ОС Windows Vista/Windows Server 2008/Windows 7 после перезагрузки ОС при интерактивном режиме логина на экран выводятся иконки для выбора пользователя, иконка, отображающая текущий статус Продукта CSP VPN Client и окно логина в Продукт (Рисунок 85).

В ОС Windows Vista/Windows Server 2008/Windows 7 процессы входа в ОС и логина в Продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.



Рисунок 85

 Copyright © S-Terra CSP 2003 - 2015

В окне выбора пользователя (Рисунок 85) иконка, отображающая текущий статус Продукта, может быть смещена в нужном направлении, если ее положение неудобно (см. раздел “Изменение положения иконки текущего статуса Продукта”).

В ОС Windows Vista/Windows Server 2008/Windows 7 окно логина в Продукт автоматически появляется в интерактивном режиме, когда необходимо выбрать пользователя для входа в ОС:

- после загрузки системы
- при выходе пользователя из системы
- при смене пользователя.

При неинтерактивном режиме логина в Продукт или переключении на него см. раздел “Неинтерактивный режим логина в Продукт”.

Окно логина в Продукт (Рисунок 89) будет выводиться только при запущенном VPN-сервисе. Если к моменту вывода окна ОС Windows еще не запустила VPN-сервис, то Продукт будет ждать 30 секунд (по умолчанию). Если VPN-сервис не будет запущен и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 86). Чтобы данное окно не появлялось – увеличьте время инициализации сервиса (см. раздел “Время инициализации VPN сервиса”)

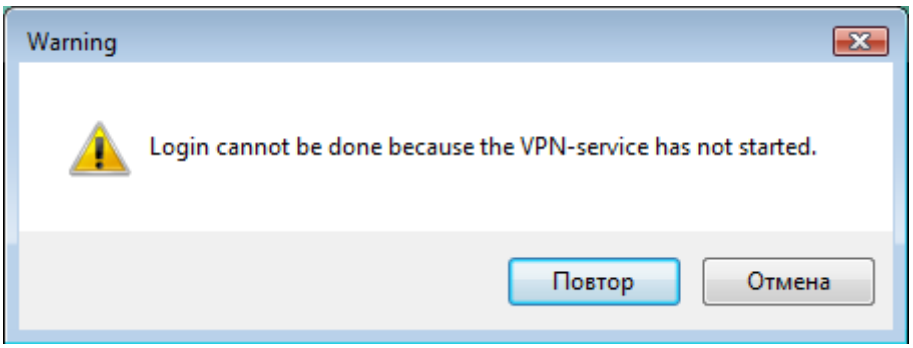


Рисунок 86

После успешной регистрации пользователя в Продукте иконка статуса Продукта изменит свой вид (Рисунок 87) (см. главу “Отображение текущего статуса Продукта”):



Рисунок 87

После входа пользователя в ОС иконка статуса Продукта будет размещена в панели задач.

Если отказаться от логина пользователя в Продукт, то потом зарегистрироваться в Продукте можно:

- нажав на иконку статуса Продукта в окне выбора пользователя, и в выпадающем меню выбрать предложение Login (Рисунок 88)
- либо после входа в ОС, нажав на иконку статуса Продукта в панели задач (см. раздел “Login/Logout”).

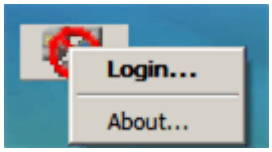


Рисунок 88

 Copyright © S-Terra CSP 2003 - 2015

13.1. Интерактивный режим логина в Продукт

При интерактивном режиме логина в Продукт после перезагрузки операционной системы открывается окно (Рисунок 89) для ввода и изменения пароля пользователя. По умолчанию пароль является пустым.

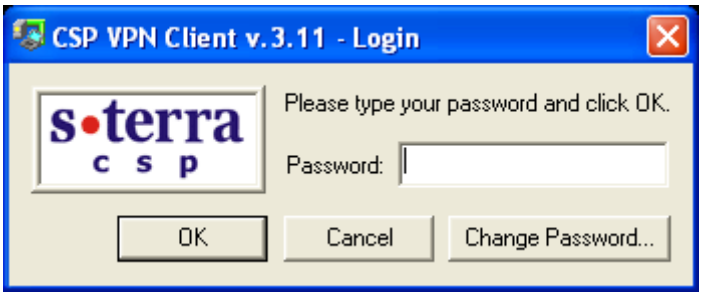


Рисунок 89

При нажатии на кнопку Change Password откроется окно, в котором можно изменить пароль пользователя:



Рисунок 90

Для смены пароля необходимо ввести старый пароль и новый с подтверждением правильности нового пароля. Если старый пароль вводится трижды неправильно, то каждая последующая попытка ввода пароля будет прерываться паузой на полминуты.

При успешной аутентификации пользователя в Продукт загружается локальная политика безопасности, заданная для данного пользователя администратором и находящаяся в базе Продукта.

Специальная политика `Log-off policy`, которая задается администратором при подготовке инсталляционного пакета, и служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений, загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя
- если при загрузке конфигурации обнаружены ошибки.

Политика `Log-off policy` работает по одному из двух правил:

- правило Drop All – удалять любой трафик, приходящий на компьютер пользователя

 Copyright © S-Terra CSP 2003 - 2015

- правило Default Driver Policy (DDP) – политика драйвера по умолчанию, может принимать одно из двух значений:
  - правило Passall – пропускать все пакеты. Значение по умолчанию
  - правило PassDHCP – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для конфигурирования TCP/IP стека по протоколу DHCP.

Политика Default Driver Policy (DDP), которая определяется администратором, загружается в следующих случаях:

- до старта VPN сервиса
- при остановке VPN сервиса.

13.2. Неинтерактивный режим логина в Продукт

При неинтерактивном режиме логина в Продукт автоматически производится попытка логина с пустым паролем (в качестве пароля используется пустая строка) и при успешном логине окно с запросом пароля (Рисунок 89) не появляется. При неуспешном логине - Продукт ведет себя как при интерактивном логине - будет выдано окно запроса пароля (Рисунок 89).

При установленном Продукте CSP VPN Client можно изменить интерактивный режим логина на неинтерактивный. Включение неинтерактивного режима осуществляется установкой значения, отличного от 0, переменной в реестре NonInteractiveLogin:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin.`

При значении 0 – будет включен интерактивный режим (значение по умолчанию).

13.3. Время инициализации VPN сервиса

В ОС Windows можно задать время инициализации VPN сервиса в реестре при помощи переменной `MaxServiceStartTimeout`:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\MaxServiceStartTimeout`

Эта переменная задает время в секундах ожидания запуска VPN сервиса. Если эта переменная не задана, то принимается значение по умолчанию, равное 30 секундам. Максимальное значение, которое можно задать – 600 секунд. При задании большего значения – устанавливается значение в 600 секунд.

При старте vpn-сервиса выполняется стартовый контроль целостности установленного Продукта CSP VPN Client, описанный в разделе «Стартовый и регламентный контроль целостности продукта».

13.4. Неинтерактивный режим логина в ОС

При интерактивном/неинтерактивном режиме логина в CSP VPN Client для автоматического входа пользователя в ОС Windows (не появляется окно Log On to Windows) выполните настройки, описанные для ОС Windows по адресу:

`http://support.microsoft.com/?kbid=315231`

Опишем здесь настройки трех переменных в Редакторе реестра:

- нажмите Пуск – Выполнить, введите `regedit`, нажмите `OK`
- в реестре войдите в ключ

 Copyright © S-Terra CSP 2003 - 2015

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`

- после двойного клика на переменной `DefaultUserName` в открывшемся окне в поле Значение введите имя пользователя и нажмите ОК
- двойным кликом на переменной `DefaultPassword` откройте окно и в поле Значение введите пароль пользователя, если эта переменная отсутствует, то создайте ее:
  - в окне Редактор реестра войдите в меню Правка, выберите предложение Создать – Строковый параметр
  - напечатайте имя переменной – `DefaultPassword` и нажмите Enter
  - двойным кликом на этой переменной откройте окно и в поле Значение введите пароль
- двойной клик на переменной `AutoAdminLogon` откроет окно, в котором в поле Значение введите 1 и нажмите ОК. Если переменная `AutoAdminLogon` отсутствует, то создайте ее:
  - в окне Редактор реестра войдите в меню Правка, выберите предложение Создать – Строковый параметр
  - напечатайте имя переменной – `AutoAdminLogon` и нажмите Enter
  - двойным кликом на этой переменной откройте окно и в поле Значение введите 1 и нажмите ОК
- Выйдите из Редактора реестра – Выход
- Нажмите Пуск – Перезагрузка – ОК.

После этого вход пользователя в ОС будет осуществляться автоматически.

Замечание

Время загрузки ОС Windows XP с продуктом CSP VPN Client зависит от нескольких факторов, в том числе:

- аппаратной платформы (CPU, объема памяти, диска)
- количества и качества установленного программного обеспечения
- степени фрагментации жесткого диска
- количества накопленного "информационного мусора" в реестре.

Установленный на компьютер CSP VPN Client позволяет создавать защищенное соединение до логина пользователя в ОС Windows XP, но для этого пользователь должен пройти дополнительную аутентификацию (окно регистрации в продукт) перед логином в ОС.

Сервис аутентификации дожидается запуска всех пользовательских сервисов и запуска CSP VPN Client. Для давно эксплуатирующийся системы, где установлено много приложений, время загрузки сервисов значительно возрастает. На компьютерах с небольшим объемом памяти процесс загрузки сервисов еще увеличивается, поскольку системе не хватает памяти и она начинает выгружать только что загруженные приложения в swap файл на диск.

Ожидание появления дополнительного окна аутентификации может расцениваться пользователем как запуск конкретного приложения CSP VPN Client, а не запуск всех приложений ОС. Пользователю кажется, что загрузка ОС становится значительно дольше, хотя объективные замеры с секундомером доказывают обратное.

Чтобы избежать описанной выше ситуации рекомендуется выполнить некоторые действия:

- удалить неиспользуемые приложения, запускающиеся в процессе загрузки Windows

- выполнить чистку и дефрагментацию реестра
- выполнить дефрагментацию жесткого диска.

 Copyright © S-Terra CSP 2003 - 2015

14. Стартовый и регламентный контроль целостности продукта

В состав CSP VPN Client входит файл `.hashes`, который устанавливается в каталог Продукта (по умолчанию – “Program Files\CSP VPN Client”).

Файл `.hashes` содержит строки вида (между хэш-суммой и именем файла один пробел):

```
<hash> <encoded_file_path>
```

где

`<hash>` – эталонное значение хэш-суммы для данного файла

`<encoded_file_path>` – полный путь к проверяемому файлу

При старте сервиса vpnsvc автоматически запускается утилита `cspvpn_verify` для проверки целостности установленного Продукта. При успешной проверке никакого сообщения на экран не выдается, а в файл `cspvpn_verify_err.log`, расположенный в каталоге Продукта, передается сообщение: `Verification SUCCESS: <n> files verified`.

При обнаружении ошибки работа утилиты прерывается и выдается сообщение об ошибке в файл `cspvpn_verify_err.log`.

Регламентный контроль целостности CSP VPN Client осуществляется во время работы Продукта запуском вручную утилиты `cspvpn_verify` из каталога установленного Продукта.

При успешной проверке и при обнаружении ошибки реакция будет такой же как и при стартовом контроле.

Возможные сообщения об ошибках

Таблица 3

	Сообщение об ошибке	Описание проблемы	Код возврата	Продолжение работы утилиты
1	Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.	1	
2	Integrity verification list “<file_.hashes_full_path >” not found	Отсутствует файл .hashes.	2	
3	Integrity verification list “<file_.hashes_full_path >” is corrupted	Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла).	3	

 Copyright © S-Terra CSP 2003 - 2015

4	Integrity verification tool call failed on file “<product_file_full_path> ”	Запуск cpverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).	4	+
5	File “<product_file_full_path> ” is corrupted	Один или больше файлов продукта повреждены (хэш-сумма не соответствует эталонной; также возможны и другие ситуации – например, отсутствующий файл – cpverify их не различает).	5	+

где

`<file_.hashes_full_path>` – полный путь к файлу `.hashes`

`<product_file_full_path>` – полный путь к файлу Продукта, на котором произошла ошибка.

При обнаружении ошибки по окончании работы утилиты выдается сообщение: `Verification FAILED`. Затем проверяется сервис vpnsvc и если он работает, то выполняется его аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

После устранения обнаруженной ошибки перезапустите сервис vpnsvc:

```
net start vpnsvc.
```

15. Отображение текущего статуса Продукта

Текущий статус Продукта отображает иконка, расположенная в панели задач.

Если пользователь не аутентифицировался, то иконка имеет вид:



Рисунок 91

Пользователь аутентифицировался, но Продукт не имеет ни одного защищенного соединения – иконка принимает вид:



Рисунок 92

Когда появляется хотя бы одно защищенное соединение, но трафик по этим соединениям отсутствует, то на иконке изменяется цвет "соединения" с серого на зеленый:



Рисунок 93

Если Продукт имеет хотя бы одно защищенное соединение и обрабатывает трафик по этим соединениям, то на иконке изменяется цвет "монитора" с синего на бирюзовый:



Рисунок 94

При наведение мышки на иконку всплывает информация о количестве "живых" SA (существующих на момент наведения мышки на иконку) и количестве байт обработанного трафика по всем существовавшим и существующим SA с момента загрузки операционной системы.



Рисунок 95

 Copyright © S-Terra CSP 2003 - 2015

15.1. Изменение положения иконки текущего статуса Продукта

В окне выбора пользователя (Рисунок 85) положение иконки, отображающей текущий статус Продукта, если оно неудобно, можно изменить с помощью переменной в реестре:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{7026F7B9-3C2E-4b80-A62E-69645BFF1190}\Position
```

Значением переменной `Position` является строка формата:

```
<int_x>,<int_y>
```

где

`int_x` – целое число, задающее смещение иконки по горизонтальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно левой стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно правой стороны экрана

`int_y` – целое число, задающее смещение иконки по вертикальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров
- положит.знач. – положение иконки отсчитывается относительно верхней стороны экрана
- отрицат.знач. – положение иконки отсчитывается относительно нижней стороны экрана.

 Copyright © S-Terra CSP 2003 - 2015

15.2. Login/Logout

При нажатии на иконку правой кнопкой мыши открывается меню следующего вида:

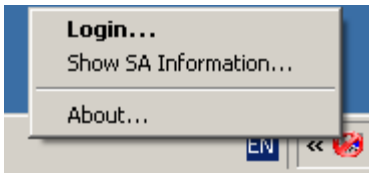


Рисунок 96

В зависимости от состояния системы (аутентифицировался пользователь или нет) будет показано предложение `Login` или `Logout`.

При выборе предложения `Login` появится окно логина в Продукт (Рисунок 89) для аутентификации пользователя и изменения пароля.

При выборе предложения `Logout` выполнится следующее:

- будут уничтожены все существующие SA с данным клиентом
- загрузится специальная политика Log-off policy
- предложение `Logout` изменится на `Login`.

15.3. SA Information

При выборе предложения `Show SA Information` – появится окно монитора созданных SA вида:

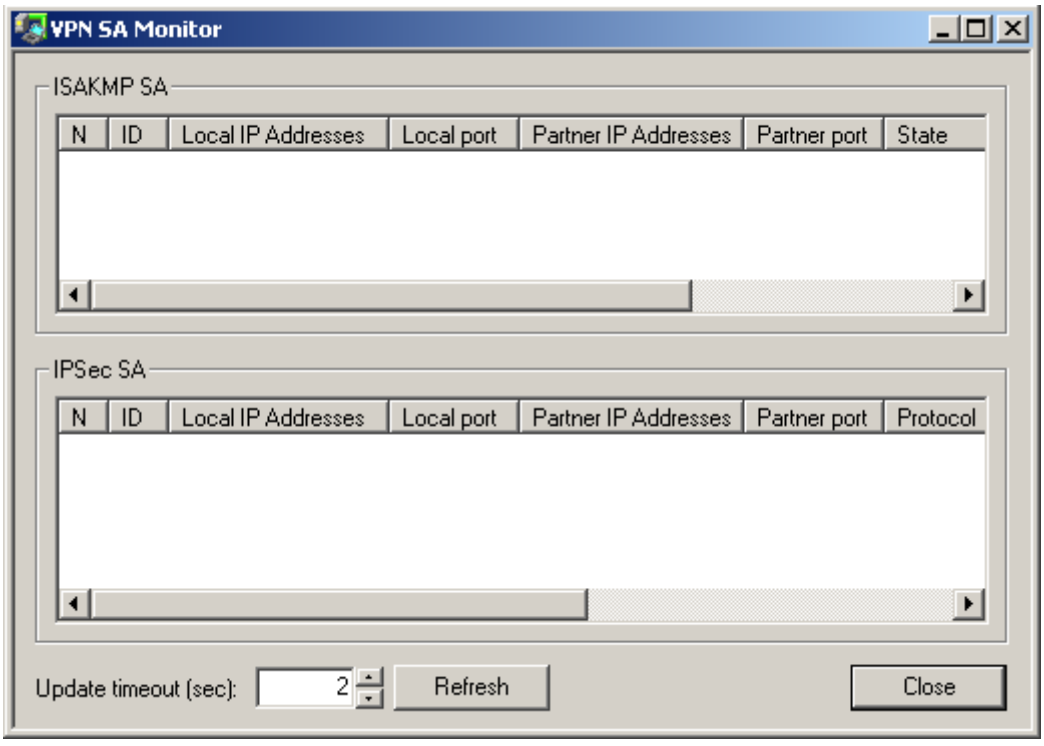


Рисунок 97

 Copyright © S-Terra CSP 2003 - 2015

где:

`ISAKMP SA` – список ISAKMP SA. Выводятся следующие поля:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA
- `Local IP Addresses` – локальные адреса
- `Local port` – локальный IKE порт
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерский IKE порт
- `State` – состояние SA:
  - `incomplete` – недостроенный
  - `ready` – рабочий
  - `configuration` – изменяемый
  - `deletion` – удаляемый
  - `unknown` – неизвестное состояние (не должно выводится)
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

`IPSec SA` – список IPsec SA с полями:

- `N` – порядковый номер в таблице
- `ID` – уникальный номер SA
- `Local IP Addresses` – локальные адреса
- `Local port` – локальные порты
- `Partner IP Addresses` – партнерские адреса
- `Partner port` – партнерские порты
- `Protocol` – сетевые протоколы
- `Action` – тип действия:
  - `AH`
  - `ESP`
  - `AH+ESP`
- `Type` – тип соединения:
  - `transport` – транспортный режим
  - `tunnel` – туннельный режим
  - `nat-t-transport` - транспортный режим через NAT
  - `nat-t-tunnel` - туннельный режим через NAT
- `Sent bytes` – количество отосланных байт
- `Received bytes` – количество полученных байт

`Update timeout (sec)` – время, через которое будут обновляться данные в таблице о созданных SA. Диапазон значений `1..9999`, начальное значение - `2`.

При выборе предложения `About` в меню выводится информация о версии Продукта:

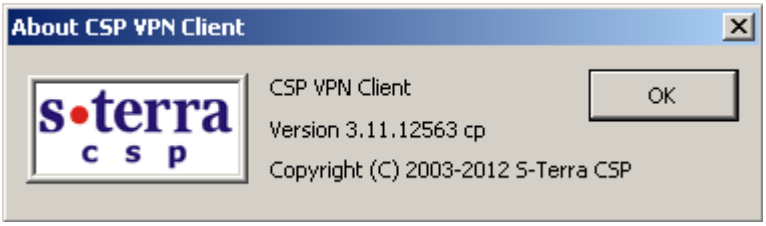


Рисунок 98

16. Деинсталляция CSP VPN Client

Деинсталляция CSP VPN Client производится стандартными средствами операционной системы – вызовом модуля Add/Remove Programs и выбором из списка строки CSP VPN Client.

При деинсталляции CSP VPN Client происходит включение стандартного сервиса, связанного с IPsec и IKE. В Windows XP/Windows Server 2003 – это Служба IPSEC, в Windows Vista/Windows Server 2008/Windows 7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности».

В Windows Vista/Windows Server 2008/Windows 7 при деинсталляции CSP VPN Client выдается окно (Рисунок 99). Необходимо разрешить запуск деинсталлятора.

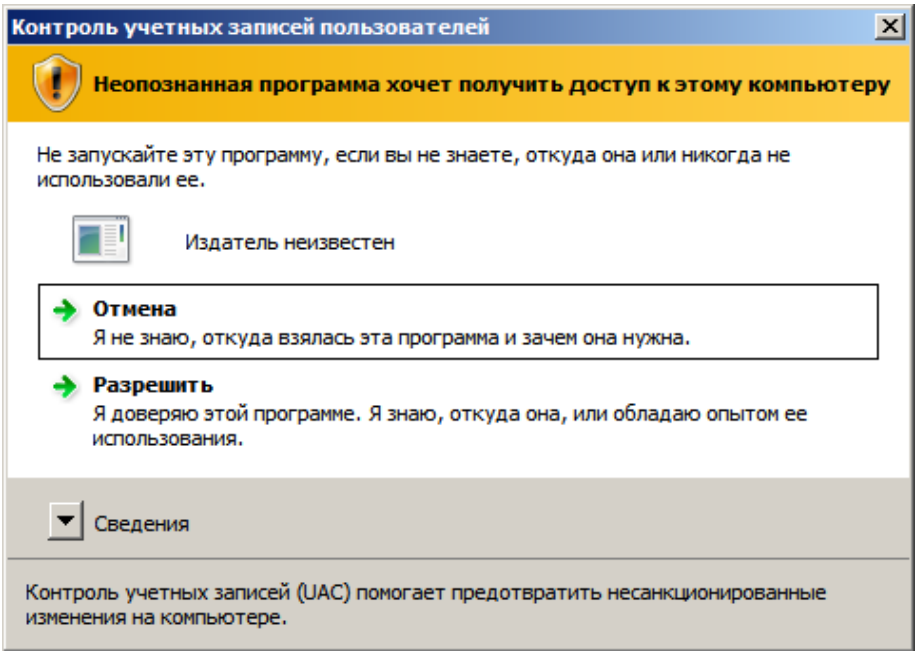


Рисунок 99

17. Восстановление CSP VPN Client

Во внештатных ситуациях – сбой в работе продукта, зависание продукта и др. перезагрузите LSP конфигурацию командой lsp_reload (если это возможно) или перезапустите компьютер. Если функции продукта не восстановились, то переустановите CSP VPN Client.

18. Создание локальной политики безопасности. Конфигурационный файл

Под политикой безопасности понимается совокупность правил, по которым обрабатываются пакеты входящего и исходящего трафиков. Пакеты могут проходить как пакетную фильтрацию так и обработку с использованием криптографических алгоритмов – построение защищенных (VPN) туннелей между партнерами.

Создание локальной политики безопасности (LSP – Local Security Policy) CSP VPN Client осуществляется путем написания конфигурационного файла в текстовом формате для VPN устройства.

 Copyright © S-Terra CSP 2003 - 2015

18.1. Описание грамматики LSP

Синтаксические диаграммы верхнего уровня языка описания конфигурации

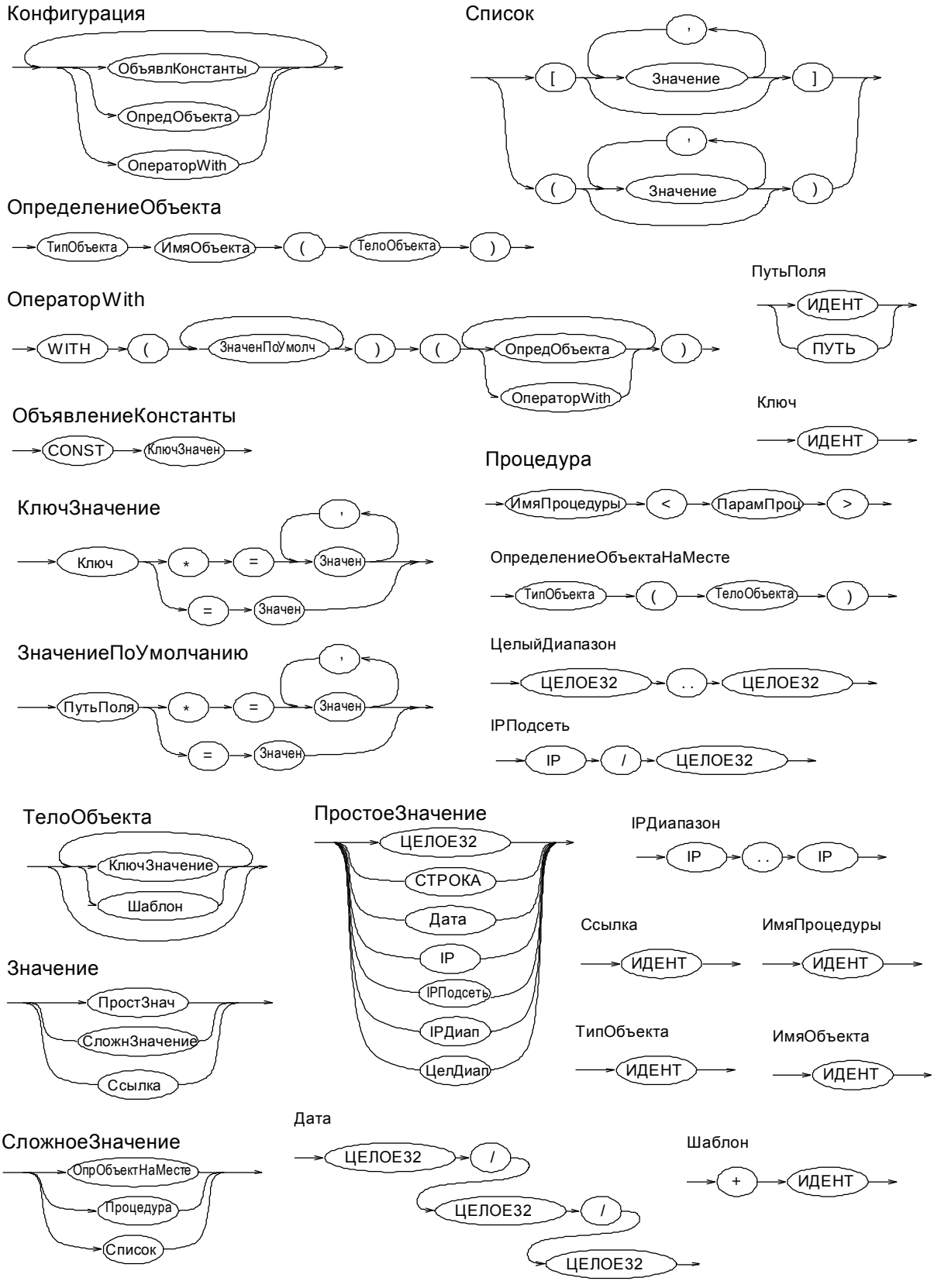


Рисунок 100

Описание LSP представляет собой последовательное описание структур данных, определяемых типом, именем, списком параметров (полей) и их значений. Синтаксис языка определяет формат описания структур данных, базовые типы значений полей структур. Синтаксические конструкции позволяют описывать иерархические структуры данных, число уровней которых не ограничено.

Терминальные символы

Терминальный символ ИДЕНТ обозначает идентификатор. Идентификатор состоит из латинских букв, цифр, символов '_' и '-'. Он должен начинаться с латинской буквы или символа '_'. Запрещено использование идентификаторов, совпадающих с ключевыми словами with и const. Внутри имен подстановок оператора with могут быть использованы символы '.'.

Примеры идентификаторов:

```
Moscow-16
_WWW_
IKECFGRequestAddress
IKERule
LOCAL_IP_ADDRESSES
```

Терминальный символ СТРОКА служит для обозначения строки, состоящей из любых символов, заключенных в двойные кавычки ("..") . Если внутри строки необходим символ двойной кавычки, то его следует дополнить слева символом '\' . Для использования символа '\' (back-slash)в строке, его нужно указать два раза ('\\' – двойной back-slash). Допустимо указывать и один back-slash, т.к. при перекодировании восстанавливается двойной back-slash.

Примеры задания значений типа СТРОКА:

```
Title = "Moon Gate LSP"
IntegrityAlg = "MD5-H96-KPDK"
X509SubjectDN *= "C=RU,O=OrgName,OU=qa0,CN=snickers0"
```

Терминальный символ ЦЕЛОЕ32 представляет 32-битное целое число без знака. Число может быть записано в десятичной или шестнадцатеричной системе счисления. Во втором случае оно должно начинаться цифрой и заканчиваться буквой 'h' или 'H'. В шестнадцатеричном и десятичном представлении запись числа не может быть длиннее 10 символов, включая букву 'h'.

Примеры задания числовых значений параметров:

```
RetryTimeBase = 4
BlacklogSessionsMax = 16
LifetimeKilobytes = 0abcdh
```

Терминальный символ IP обозначает сетевой адрес четвертой версии IP-протокола. IP-адрес состоит из четырех чисел, разделенных точками, где каждое из чисел принадлежит диапазону от 0 до 255.

Примеры IP-адресов:

```
PeerIPAddress = 192.168.2.1
```

Значения типа ДАТА

Тип ДАТА представляется тремя целыми числами без знака, разделенными символом '/' – число/месяц/год.

 Copyright © S-Terra CSP 2003 - 2015

Пример даты:

```
StartOfValidity = 24/03/ 2004
EndOfValidity = 3/6/2004
```

Ключевые слова

Ключевые слова `with`, `const` используются при создании специальных конструкций.

На диаграмме (Рисунок 100) эти ключевые слова написаны прописными (большими) буквами. В конфигурационном файле ключевые слова должны быть написаны строчными буквами.

Комментарии

Комментарии могут размещаться в любом месте текста между другими терминалами и являются разделителями, эквивалентными символам пробела. Вложения комментариев одного типа не допускаются. Поддерживаются следующие два вида комментариев:

Блочный. Начинается с символов "`(*`" и заканчивается символами "`*)`" или начинается символом '`{`' и заканчивается символом '`}`'.

Строковый. Начинается с символа '`#`', заканчивается символом перевода каретки `<LF>`.

Примеры комментариев:

```
20..30  # Диапазон чисел 20-30
Action *= (tunnel_IPsec_des_md5_action) (* будет описан
ниже *)
```

Разделители

В качестве разделителей в LSP-языке могут быть использованы следующие символы: пробел, табуляция, `<LF>` и `<CR>`. Переходом на новую строку считается символ `<LF>`.

Разделители необходимы только для отделения терминалов `ИДЕНТ`, `ЦЕЛОЕ32`, `IP`, ключевых слов `const`, `with` друг от друга.

Диапазоны значений

```
ProtocolID *= 20..30
```

Списки значений

При указании списка значений для какого-либо параметра перед знаком '=' должен стоять символ '`*`'. Если параметр может иметь список значений, но необходимо указать только одно, то символ '`*`' можно опустить.

```
GroupID *= MPDP_768, MODP_1024
```

Вложенные списки

Для описания вложенных списков могут использоваться круглые или квадратные скобки.

 Copyright © S-Terra CSP 2003 - 2015

```
ContainedProposals *= (IPsec_ah_md5, IPsec_esp_des3),
(IPsec_ah_md5, IPsec_esp_idea)
```

Ссылки на структуры

```
LocalCredential *= cert1
```

Определение вложенных структур

```
Transform *= IKETransform(
        CipherAlg *= "DES-CBC"
        HashAlg *= "MD5"
        GroupID *= MODP_768
        LifetimeSeconds = 86400
        LifetimeKilobytes = 4608000
        LifetimeDerivedKeys = 100000
)
```

Объявление структуры верхнего уровня

```
FilteringRule Client_Gate(
        LocalIPFilter* = FilterEntry( IPAddress *= 250.192.32.5
        )
        PeerIPFilter* = FilterEntry( IPAddress *= 10.10.12.4)
        Action* = ( Client_Gate )
)
```

Специальные конструкции

Для упрощения описания повторяющихся параметров предусмотрена возможность использования именованных констант, значений по умолчанию и шаблонов.

В отличие от других конструкций языка, которые подвергаются семантическому анализу, константы и шаблоны полностью обрабатываются на этапе синтаксического разбора.

Описание каждой **константы** начинается с ключевого слова `const`, за которым следует имя константы и ее значение (или список значений). Значением константы может являться любая конструкция, которая может быть значением поля структуры. Использование константы заключается в подстановке ее имени вместо значения поля структуры.

Пример:

```
const A = FilterEntry(
        IPAddress *= 10.10.12.5
        ProtocolID = 6
        Port =80
)
FilteringRule Filter_1 (
        PeerIPFilter* = A
        Action* = ( PASS)
)
```

 Copyright © S-Terra CSP 2003 - 2015

Шаблон (template) является константой, единственное значение которой является структурой того типа, к которой этот шаблон будет применен. Для использования шаблона, внутри описания структуры необходимо написать символ '+' и имя константы за ним. Подстановка шаблона заключается в копировании всех полей из структуры, которая является значением константы, в структуру, в которую шаблон подставляется.

Не допускается задавать одни и те же поля и в шаблоне и структуре, в которую он подставляется.

Пример описания:

```
const Transform_DES_MD5 = IKETransform(
        CipherAlg *= "DES-CBC"
        HashAlg *= "MD5"
        GroupID *= MODP_768
)
Transform *= IKETransform(
        + Transform_DES_MD5
        LifetimeSeconds = 86400
        LifetimeKilobytes = 4608000
)
Эквивалентное описание:
Transform *= IKETransform(
        CipherAlg *= "DES-CBC"
        HashAlg *= "MD5"
        GroupID *= MODP_768
        LifetimeSeconds = 86400
        LifetimeKilobytes = 4608000
)
```

Конструкция WITH используется для задания значений по умолчанию для полей структур, которые описываются внутри конструкции. После ключевого слова 'with' указываются пути к полям и значения по-умолчанию для них. Путь к полю структуры может быть записан двумя способами:

- первый вариант – это просто имя поля. В этом случае в каждую структуру, которая описана внутри with, будет добавлено указанное поле, если в структуре такого поля нет.
- во втором варианте путь записывается в форме тип_верх_ур.имя_поля1.имя_поля2 ... .имя_поляМ. В этом случае имя_поляМ с указанным значением будет добавлено только для структур, которые указаны в качестве значения соответствующего поля структуры уровнем выше. Тип струтуры, содержащей имя_поля1 должен быть тип_верх_ур. Значения добавляются только в те структуры, которые определены непосредственно внутри других, а не в виде ссылки.

Значения добавляются только в том случае, если в структуре явно не указано других значений для поля.

Пример:

```
(* Указание значения по-умолчанию, используя полное имя поля (путь).*)

with (
```

 Copyright © S-Terra CSP 2003 - 2015

```
   (* Значение по-умолчанию для FilteringRule.LocalIPFilte *)
   FilteringRule.LocalIPFilter = FilterEntry(
                                    IPAddress = 10.0.16.84))
(
FilteringRule f0 (
   PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)
   Action = (DROP))
FilteringRule f1 (
   PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
   Action = (PASS))
)
```

(* Та же конфигурация, сокращённая форма – задано значение по-умолчанию для всех структур верхнего уровня, независимо от типа.*)

```
with (
   LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84))
(
FilteringRule f0 (
   PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)
   Action = (DROP))
FilteringRule f1 (
   PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
   Action = (PASS))
)
```

(* Результирующая конфигурация*)

```
FilteringRule f0 (
    PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)
    LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84)
    Action = (DROP)
)
FilteringRule f1 (
   PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
   LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84)
   Action = (PASS)
)
```

18.2. Структура конфигурации

Структуру конфигурации можно разделить на три логические части:

- Заголовок (GlobalParameters)
- Глобальные параметры протокола IKE (IKEParameters)
- Правила фильтрации (FilteringRules)

Структура конфигурации предполагает наличие только одного заголовка (GlobalParameters), одной структуры глобальных параметров протокола IKE (IKEParameters) и неограниченное количество правил фильтрации (FilteringRule).

Диаграмма структуры конфигурации и взаимосвязь между ее элементами

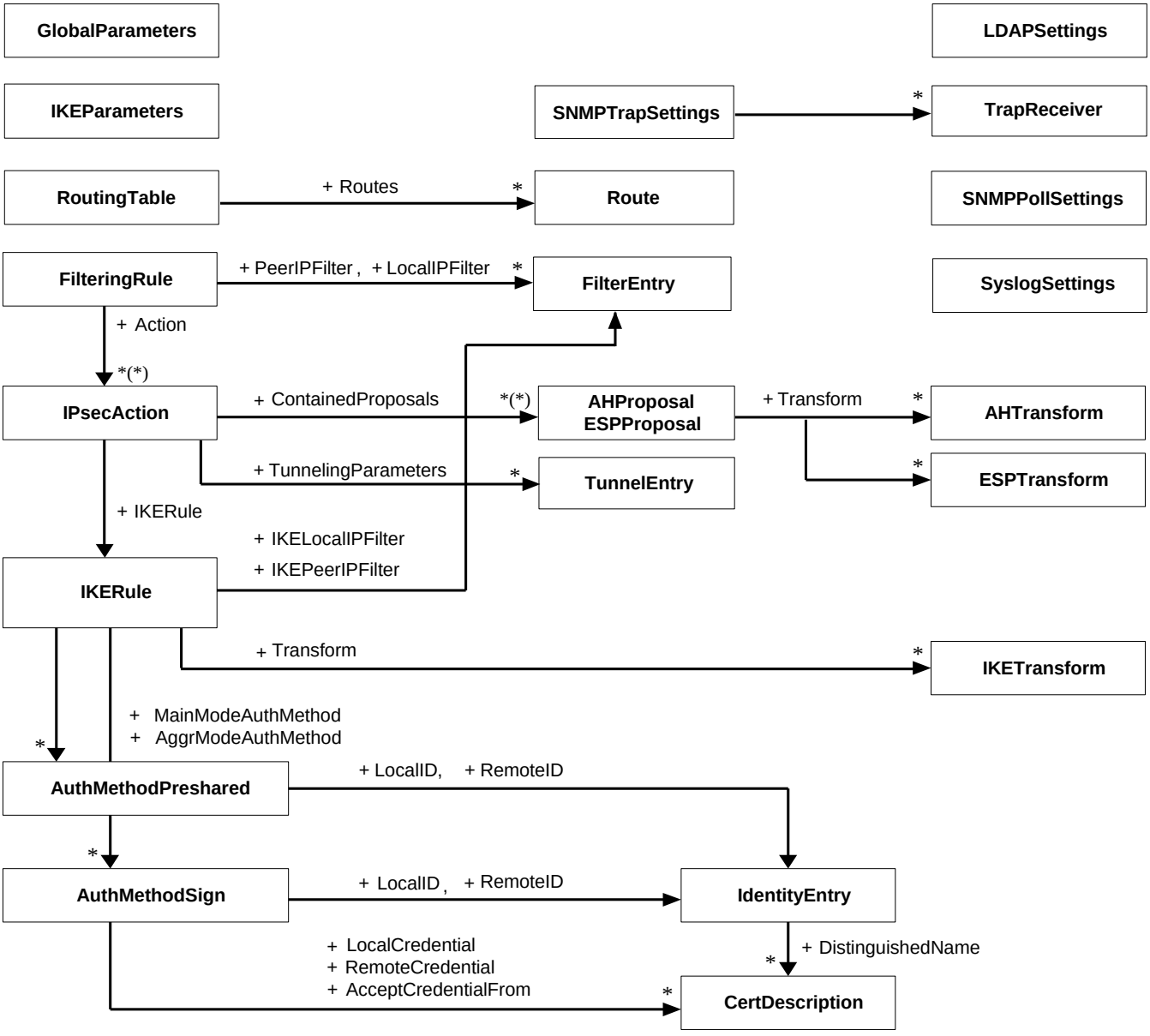


Рисунок 101

 Copyright © S-Terra CSP 2003 - 2015

Пояснения к диаграмме:

- в прямоугольниках указаны имена структур данных, составляющих локальную политику безопасности
- стрелка обозначает отношение использования между структурами данных
- рядом со стрелкой указан атрибут структуры, который ссылается на используемую структуру
- '*' рядом со стрелкой обозначает, что атрибут содержит список используемых структур
- '*(*)' обозначает, что атрибут содержит список списков используемых структур.

Таблица 4

Структура конфигурации в табличном виде

GlobalParameters		LDAPSettings
Title Version Type Serial StartOfValidity EndOfValidity CRLHandlingMode LDAPLogMessageLevel SystemLogMessageLevel PolicyLogMessageLevel CertificatesLogMessageLevel		Server Port SearchBase ConnectTimeout ResponseTimeout HoldConnectTimeout DropConnectTimeout
IKEParameters		**SyslogSettings**
SendRetries RetryTimeBase RetryTimeMax SACreationTimeMax InitiatorSessionsMax ResponderSessionsMax BlacklogSessionsMax BlacklogSessionsMin BlacklogSilentSessions BlacklogRelaxTime		*Server* Facility
SNMPPollSettings	**SNMPTrapSettings**	**TrapReceiver**
LocalIPAddress Port ReadCommunity SysLocation SysContact	*Receivers*	*IPAddress* Port *Community* Version SNMPv1AgentAddress
RoutingTable		
Routes _____*		**Route** *Destination* Gateway NetworkInterface Metric
FilteringRule		
PeerIPFilter _____* LocalIPFilter _____* NetworkInterfaces RefuseTCPPeerInit Action _____ |*(*)		**FilterEntry** **FilterEntry** IPAddress ProtocolID Port
IPsecAction _____|		

 Copyright © S-Terra CSP 2003 - 2015



 Copyright © S-Terra CSP 2003 - 2015

В таблице жирным шрифтом выделены имена структур, а курсивом – обязательные атрибуты.

Название структуры в таблице также является ссылкой на описание этой структуры и ее атрибутов.

Знак "*" (звездочка) в конце атрибута конфигурационного файла означает, что значения данного атрибута представлены в виде списка. Если знак "*" не установлен, то предполагается, что вместо списка будет использовано только одно значение или одна ссылка.

 Copyright © S-Terra CSP 2003 - 2015

18.3. Заголовок конфигурации

Заголовок конфигурации представляет собой структуру, описывающую общие параметры CSP VPN Client. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

Имя структуры GlobalParameters

Атрибуты Title
Version
Type
Serial
StartOfValidity
EndOfValidity
CRLHandlingMode
LDAPLogMessageLevel
SystemLogMessageLevel
PolicyLogMessageLevel
CertificatesLogMessageLevel

Пример:

```
GlobalParameters (
   Title = "Moon host LSP"
   Version = "3.11"
   Serial = "000000010000000E00000001"
   CRLHandlingMode = DISABLE
   LDAPLogMessageLevel = INFO
   SystemLogMessageLevel = INFO
   PolicyLogMessageLevel = INFO
   CertificatesLogMessageLevel = INFO
)
```

 Copyright © S-Terra CSP 2003 - 2015

Атрибут Title

Атрибут Title предназначен для краткого описания конфигурации (имя конфигурации).

Синтаксис Title = СТРОКА

Значение строка произвольного содержания

Значение по умолчанию пустая строка

Атрибут Version

Атрибут Version определяет версию спецификации конфигурации.

Синтаксис Version = СТРОКА

Значение строка вида [0-9].[0-9]

Значение по умолчанию пустая строка.

Атрибут Type

Атрибут Type специфицирует тип конфигурации, который определяет действия агента при ее активизации.

Синтаксис Type = **PERMANENT | TEMPORARY**

Значения PERMANENT – после успешной активизации конфигурации она сохраняется в базе Продукта, если она была активизирована из файла. При следующем запуске Продукта конфигурация будет автоматически активизирована из базы Продукта.

TEMPORARY – после успешной активизации, конфигурация не сохраняется в базе данных и используется только в текущем сеансе работы Продукта.

Значение по умолчанию PERMANENT.

Атрибут Serial

Атрибут Serial определяет уникальный серийный номер конфигурации.

Синтаксис Serial = СТРОКА

Значение строка содержит шестнадцатеричное представление серийного номера конфигурации

Значение по умолчанию пустая строка

 Copyright © S-Terra CSP 2003 - 2015

Атрибут StartOfValidity

Атрибут StartOfValidity определяет момент времени, до которого конфигурация не может быть активизирована.

Синтаксис StartOfValidity = ДАТА

Значение 01/1/0000 – 31/12/9999

Значение по умолчанию ограничения отсутствуют на активизацию конфигурации

Атрибут EndOfValidity

Атрибут EndOfValidity определяет момент времени, после которого конфигурация не может быть активизирована.

Синтаксис EndOfValidity = ДАТА

Значение 01/1/0000 – 31/12/9999

Значение по умолчанию ограничения отсутствуют на активизацию конфигурации

Атрибут CRLHandlingMode

Атрибут CRLHandlingMode определяет режим обработки списка отозванных сертификатов (CRL).

Синтаксис CRLHandlingMode = **DISABLE|OPTIONAL|BEST_EFFORT|ENABLE**

Значения DISABLE – при проверке сертификата CRL не обрабатывается

OPTIONAL – при проверке сертификата CRL используется только в случае, если он был предустановлен в базу Продукта или получен (и обработан) в процессе IKE обмена и является действующим

BEST_EFFORT – при проверке сертификата CRL используется только в том случае, если он является действующим, если это не так, то CRL может быть получен посредством протокола LDAP (агент смотрит адрес LDAP-сервера сначала в поле CDP сертификата, а затем ищет структуру LDAPSettings). Если CRL получить не удалось – сертификат принимается.

ENABLE – при проверке сертификата обязателен действующий CRL, если это не так, то CRL может быть получен посредством протокола LDAP. Если CRL получить не удалось – сертификат не принимается.

Значение по умолчанию ENABLE.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут LDAPLogMessageLevel

Атрибут LDAPLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с доступом к LDAP-серверу.

Синтаксис

LDAPLogMessageLevel = **DEBUG |**
INFO |
NOTICE |
WARNING |
ERR |
CRIT |
ALERT|
EMERG

Значения уровни детализации протоколирования определены в RFC 3164[3].

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования событий устанавливается опцией **-s в утилите make inst.exe**. Если общий уровень не менялся, то он имеет значение NOTICE.

Атрибут SystemLogMessageLevel

Атрибут SystemLogMessageLevel задает текущий уровень детализации протоколирования для системных событий.

Синтаксис

SystemLogMessageLevel = **DEBUG |**
INFO |
NOTICE |
WARNING |
ERR |
CRIT |
ALERT|
EMERG

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования событий устанавливается опцией **-s в утилите make inst.exe**. Если общий уровень не менялся, то он имеет значение NOTICE.

[3] RFC 3164: The BSD syslog Protocol

 Copyright © S-Terra CSP 2003 - 2015

Атрибут PolicyLogMessageLevel

Атрибут PolicyLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с применением локальной политики.

Синтаксис

PolicyLogMessageLevel = **DEBUG |**
INFO |
NOTICE |
WARNING |
ERR |
CRIT |
ALERT|
EMERG

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования событий устанавливается опцией **-s в утилите make_inst.exe**. Если общий уровень не менялся, то он имеет значение NOTICE.

Атрибут CertificatesLogMessageLevel

Атрибут CertificatesLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с получением, обработкой сертификатов и их сохранением их в базе Продукта.

Синтаксис

CertificatesLogMessageLevel = **DEBUG |**
INFO |
NOTICE |
WARNING |
ERR |
CRIT |
ALERT|
EMERG

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования событий устанавливается опцией **-s в утилите make_inst.exe**. Если общий уровень не менялся, то он имеет значение NOTICE.

 Copyright © S-Terra CSP 2003 - 2015

18.4. Структура LDAPSettings

Структура LDAPSettings задает настройки протокола LDAP, который используется для получения сертификатов и списков отозванных сертификатов (CRL). В конфигурации может присутствовать только одна структура данного типа. Этой структуре имя не присваивается.

В случае отсутствия структуры:

- получение сертификатов посредством протокола LDAP невозможно
- если атрибут **CRLHandlingMode** структуры **GlobalParameters** имеет значение ENABLE или BEST_EFFORT, то CRL может быть получен посредством протокола LDAP только при наличии в сертификате, для которого производится проверка подписи, расширения CDP (CRL Distribution Point) с адресом LDAP-сервера.

Имя структуры LDAPSettings

Атрибуты Server

Port

SearchBase

ConnectTimeout

ResponseTimeout

HoldConnectTimeout

DropConnectTimeout

Атрибут Server

Атрибут Server задает адрес LDAP-сервера, к которому производится запрос на поиск сертификатов. Указанный в этом атрибуте адрес используется, если сертификат, для которого производится проверка подписи, не содержит расширение CDP (CRL Distribution Point) с адресом LDAP-сервера либо в этом поле прописанный путь к LDAP-серверу является неполным и тогда добавляются данные из этой структуры.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP_PROTOCOL_ERROR (наиболее вероятная причина - не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

Для прохождения LDAP-пакетов до каждого используемого агентом LDAP-сервера в политике необходимо задать фильтр вида:

```
FilteringRule PassLdapTraffic(
      PeerIPFilter = FilterEntry(
        IPAddress = <LDAP-server IP-address from CRL Distibution
Points extension>
        ProtocolID = 6
        Port = <LDAP-server port>
      )
      LocalIPFilter = FilterEntry(
        IPAddress = LOCAL_IP_ADDRESSES
        ProtocolID = 6
      )
      RefuseTCPPeerInit = TRUE
      Action = [PASS]
    )
```

Синтаксис Server = IP

Значения IP - адрес

 Copyright © S-Terra CSP 2003 - 2015

Значение по умолчанию LDAP –сервер не указан. Поведение агента аналогично случаю отсутствия структуры LDAPSettings в политике.

Атрибут Port

Атрибут Port задает порт LDAP-сервера. Если атрибут Server не задан или расширение сертификата CRL Distribution Point содержит адрес LDAP-сервера, то данный атрибут игнорируется.

Синтаксис Port = ЦЕЛОЕ32

Значения Целое число из диапазона 1..65535

Значение по умолчанию 389.

Атрибут SearchBase

Атрибут SearchBase задает имя (Distinguished Name, DN) корневого X.500-объекта, в поддереве которого производится поиск сертификатов и CRL на LDAP-сервере. Указанное имя дополняет запрос, созданный на основе имени из сертификата или CRL, позволяя находить соответствующий X.500-объект в случае, когда исходное имя в запросе является частью имени этого объекта. Для запроса на основе URL данное имя не используется.

Синтаксис SearchBase = СТРОКА

Значения строковое представление DN в соответствии с RFC2253. Относительные имена (Relative Distinguished Name, RDN) указываются в порядке от объекта к корню.

Значение по умолчанию поиск производится по имени, полученному из сертификата или CRL.

Атрибут ConnectTimeout

Атрибут ConnectTimeOut позволяет ограничить время (в секундах) создания TCP-соединения с LDAP-сервером.

Синтаксис ConnectTimeOut = ЦЕЛОЕ32

Значение Целое число из диапазона 1..6000

Значение по умолчанию не устанавливается, что приводит к тому, что время создания TCP-соединения с LDAP-сервером ограничивается установленным для ОС временем создания TCP-соединения.

Примечание: Если в момент обращения к LDAP-серверу устройство, на котором он установлен, недоступно, то процесс создания TCP-соединения может занимать продолжительное время (до 3 минут, зависит от ОС). По этой причине могут наблюдаться внешние признаки зависания агента и это может служить причиной неудачной попытки создания соединения.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут ResponseTimeout

Поиск посредством протокола LDAP может занимать достаточно продолжительное время, оно зависит от многих факторов, в том числе от масштаба запроса и характеристик канала передачи данных. Данный атрибут позволяет ограничить время (в секундах), в течение которого ожидается ответ от LDAP-сервера на единичный запрос.

Синтаксис ResponseTimeOut = ЦЕЛОЕ32

Значение Целое число из диапазона 2..6000

Значение по умолчанию 200

Атрибут HoldConnectTimeout

Атрибут HoldConnectTimeout устанавливает период времени, в течение которого держится установленное соединение к серверу на случай, если придет к нему повторный запрос.

Синтаксис HoldConnectTimeOut = ЦЕЛОЕ32

Значение Целое число из диапазона 0..6000

При значении 0 после обмена с LDAP-сервером соединение с ним сразу закрывается.

В виду наличия погрешности в одну секунду не рекомендуется выставлять значение в 1 секунду, поскольку это может привести в некоторых случаях к немедленному закрытию соединения и к избыточному открытию нового соединения.

Значение по умолчанию 60

Атрибут DropConnectTimeout

Атрибут DropConnectTimeout устанавливает период времени, начиная с первой неудачной попытки создания соединения с LDAP-сервером, в течение которого новые попытки создания соединения с ним игнорируются.

Синтаксис DropConnectTimeOut = ЦЕЛОЕ32

Значение Целое число из диапазона 0..6000

При значении 0 в случае неудачной попытки установления соединения с LDAP-сервером новые попытки не игнорируются.

В виду наличия погрешности в одну секунду не рекомендуется выставлять значение в 1 секунду, поскольку это может привести в некоторых случаях к избыточным попыткам создания соединения;

Значение по умолчанию 5.

Пример

Пусть сертификат партнера имеет `Subject = "cn=candy,ou=nomadic".`

Для поиска такого сертификата на LDAP-сервере (`Active Directory` –Рисунок 102), необходимо указать атрибут `SearchBase`:

 Copyright © S-Terra CSP 2003 - 2015

```
LDAPSettings (
        Server = 10.1.1.1
        SearchBase="ou=scenario10,ou=QA,ou=GINS,dc=qamsca,dc=gin
        software, dc=ru"
)
```

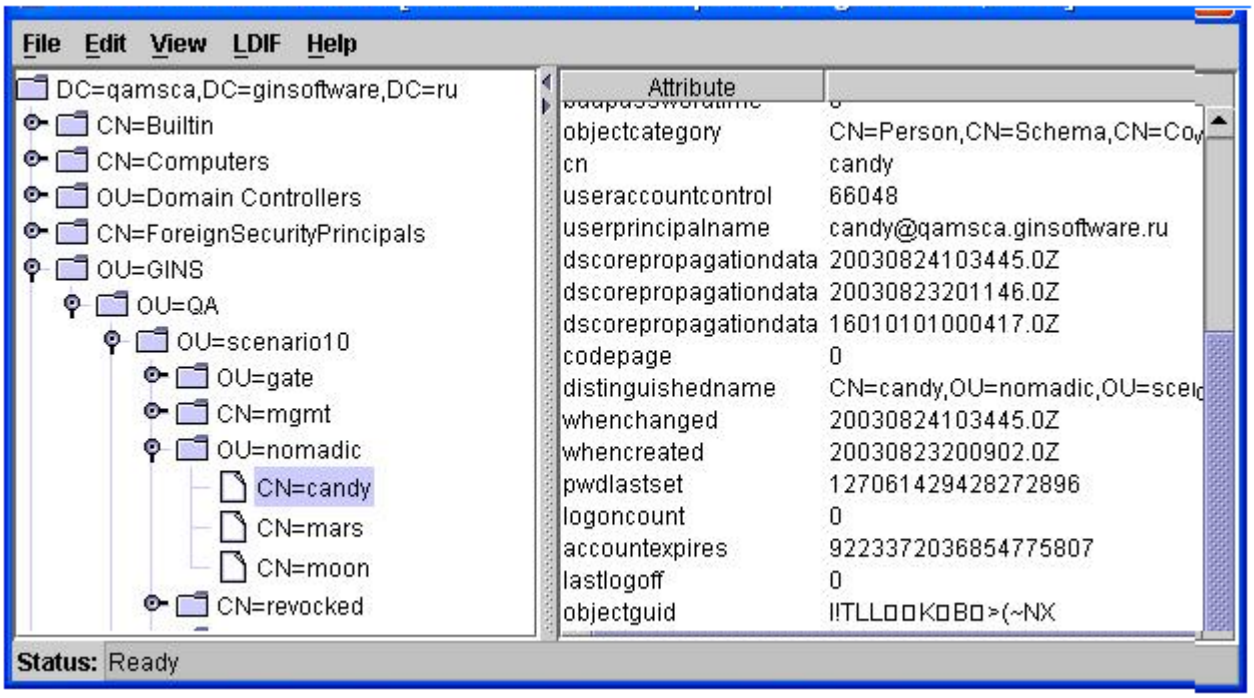


Рисунок 102

18.5. Структура IKEParameters

Структура IKEParameters описывает глобальные настройки протокола IKE. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

Имя структуры IKEParameters

Атрибуты SendRetries
RetryTimeBase
RetryTimeMax
SessionTimeMax
InitiatorSessionsMax
ResponderSessionsMax
BlacklogSessionsMax
BlacklogSilentSessions
BlacklogSessionsMin
BlacklogRelaxTime

Логику используемого механизма IKE-ретрансмиссий смотрите в разделе 18.5.1 “Обработка пакетов – ретрансмиссии”.

Атрибут SendRetries

Атрибут SendRetries устанавливает число попыток посылки IKE-пакетов партнеру.

Синтаксис SendRetries = ЦЕЛОЕ32

Значения Целое число из диапазона 1..30

Значение по умолчанию 5.

Атрибут RetryTimeBase

Атрибут RetryTimeBase позволяет установить начальный интервал в секундах между повторными попытками посылки IKE-пакетов партнеру. Если ответ не получен в течение начального интервала, то запрос посылается повторно и интервал между повторными попытками увеличивается в два раза. Этот интервал увеличивается в два раза до тех пор, пока:

- не будет получен ответ или
- значение интервала RetryTimeBase не достигнет значения RetryTimeMax (повторные попытки будут продолжаться с интервалом RetryTimeMax) и количество попыток не достигнет значения SendRetries.

Синтаксис RetryTimeBase = ЦЕЛОЕ32

Значения Целое число из диапазона 1...5

Значение по умолчанию 1.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут RetryTimeMax

Атрибут RetryTimeMax позволяет установить максимальный интервал в секундах между повторными попытками посылки IKE-пакетов партнеру. Если выставленное значение этого атрибута меньше, чем RetryTimeBase, то при загрузке конфигурации атрибуту RetryTimeMax присваивается значение RetryTimeBase.

Синтаксис RetryTimeMax = ЦЕЛОЕ32

Значения Целое число из диапазона 1...60

Значение по умолчанию 30.

Атрибут SACreationTimeMax

Атрибут SACreationTimeMax ограничивает время (в секундах) на каждую сессию IKE.

Синтаксис SACreationTimeMax = ЦЕЛОЕ32

Значения Целое число из диапазона 10...300

Значение по умолчанию 60.

Атрибут InitiatorSessionsMax

Атрибут InitiatorSessionsMax устанавливает максимально допустимое количество одновременно инициируемых IKE-сессий для всех партнёров.

Синтаксис InitiatorSessionsMax = ЦЕЛОЕ32

Значение число из диапозона 1-10000

Значение по умолчанию 30.

Атрибут ResponderSessionsMax

Атрибут ResponderSessionsMax определяет максимально допустимое количество одновременных обменов, проводимых VPN-устройством с одним неаутентифицированным партнером, в качестве ответчика. С таким партнером нет ни одного ISAKMP SA. Как только создается хотя бы один ISAKMP SA, данный атрибут ResponderSessionsMax перестает действовать.

Синтаксис ResponderSessionsMax = ЦЕЛОЕ32

Значения Целое число из диапозона 1..20

Значение по умолчанию 20.

Copyright © S-Terra CSP 2003 - 2015

Атрибут BlacklogSessionsMax

"Черный список" предназначен для защиты от DoS-атак (Denial of Service –отказ от обслуживания). "Черный список" минимизирует обработку IKE-пакетов от партнеров, находящихся в "черном списке". В случае первой неуспешной IKE-сессии, инициированной со стороны партнера, партнер сразу же заносится в "черный список". BlacklogSessionsMax устанавливает число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, только что попавшим в "черный список". При каждом следующем неудачном завершении IKE обмена число разрешенных одновременных IKE обменов для данного партнера снижается вдвое с округлением в меньшую сторону, вплоть до полного запрещения IKE трафика с данным партнером.

Примечание: как только партнер заносится в "черный список", для него текущее значение разрешенных одновременно проводимых IKE обменов не только начинает уменьшаться в два раза после каждого неуспешного завершения обмена, но и увеличиваться на единицу по истечении каждого интервала времени BlacklogRelaxTime (описанного далее).

Синтаксис BlacklogSessionsMax = ЦЕЛОЕ32

Значения Целое число из диапазона $0..(2^{32}-1)$.

Если значение равно 0, то "черный список" не используется[4].

Если значение BlacklogSessionsMax больше или равно ResponderSessionsMax, то атрибуту BlacklogSessionsMax присваивается значение ResponderSessionsMax-1.

Значение по умолчанию 16.

Атрибут BlacklogSessionsMin

Атрибут BlacklogSessionsMin позволяет установить минимальное число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, находящимся в "черном списке".

Синтаксис BlacklogSessionsMin = ЦЕЛОЕ32

Значения Целое число из диапазона $0..(2^{32}-1)$

Если это значение больше, чем BlacklogSessionsMax, то атрибуту BlacklogSessionsMin присваивается значение BlacklogSessionsMax.

Значение по умолчанию 0 – нет ограничения снизу на активные обмены с партнером, находящимся в "черном списке".

[4] При загрузке конфигурации с *отключенным* "черным списком" вся статистическая информация о "плохих" партнерах сбрасывается. Если же "черный список" *включен*, то к уже имеющейся накопленной статистике применяются новые параметры настроек "черного списка".

 Copyright © S-Terra CSP 2003 - 2015

Атрибут BlacklogSilentSessions

Атрибут BlacklogSilentSessions позволяет установить число активных обменов, инициированных партнером, находящимся в "черном списке", по достижении которого VPN-устройство перестает информировать партнера о причине отказа в создании IKE–контекста (ISAKMP SA).

Синтаксис BlacklogSilentSessions = ЦЕЛОЕ32

Значения Целое число из диапазона 0..(2^{32}-1)

Если это значение больше, чем BlacklogSessionsMax, то атрибуту BlacklogSilentSessions присваивается значение BlacklogSessionsMax.

Значение по умолчанию 4.

Атрибут BlacklogRelaxTime

Атрибут BlacklogRelaxTime устанавливает интервал времени (в секундах) релаксации "черного списка".

- За указанный период времени число разрешенных одновременных IKE обменов для каждого партнера, находящегося в "черном списке", увеличивается на единицу. По истечении следующего такого же интервала времени, текущие значения разрешенных одновременно проводимых IKE обменов для каждого партнера опять увеличивается на единицу и т.д. Этот интервал времени отсчитывается с момента последней загрузки конфигурации.
- Как только текущее значение разрешенных одновременно проводимых партнером IKE обменов начинает превышать значение BlacklogSessionsMax, такой партнер исключается из "черного списка".

Синтаксис BlacklogRelaxTime = ЦЕЛОЕ32

Значения Целое число из диапазона 0..(2^{32}-1).

0 – бесконечное время (партнер попадает в "черный список" навсегда).

Значение по умолчанию 120

Примечание: помимо механизма релаксации, партнер также может быть иключен из "черного списка" в следующих случаях:

при перезапуске сервиса

при загрузке конфигурации с отключенным "черным списком" (с атрибутом BlacklogSessionsMax = 0)

при инициации IKE обмена со стороны локального VPN устройства с целью установления ISAKMP (IPsec) соединения[5]

если партнеру удалось установить ISAKMP (IPsec) соединение с локальным VPN устройством, и тем самым партнер был успешно аутентифицирован.

[5] В данном случае считается, что локальное VPN устройство потенциально доверяет партнеру, с которым оно хочет установить соединение, и информация, накопленная в "черном списке", для такого партнера сбрасывается.

 Copyright © S-Terra CSP 2003 - 2015

18.5.1. Обработка пакетов – ретрансмиссии

1. Используемый механизм IKE-ретрансмиссий находится в общей концепции, согласно которой инициатор, исходя из наличия собственных ресурсов, проявляет настойчивость и добивается чего-то от ответчика, а ответчик, во первых, не доверяет инициатору насколько это возможно, во-вторых, по-максимуму бережет собственные ресурсы.
    - Инициатор, в большинстве случаев, являясь активной стороной, посылает очередной пакет IKE-обмена и затем перепосылает его (в соответствии с настройками ретрансмиссий – атрибуты **SendRetries**, **RetryTimeBase** и **RetryTimeMax**) до тех пор, пока не получит ответный пакет от ответчика.
        - Таким образом, инициатор выполняет работу за двоих:
            - если исходящий от инициатора пакет не дошел до ответчика, то ответчик его не обработает и, соответственно, никак не ответит инициатору. Но исходящий пакет инициатором может быть перепослан (возможно, с n-ой попытки), ответчик его получит, обработает и отошлёт ответ
            - если же проблема возникла на обратном пути (т.е. пакет от ответчика потерялся на пути к инициатору), то для инициатора эта ситуация детектируется точно так же, как и первая - то есть инициатор ответного пакета ждал, но за отведенный timeout так и не дождался. Тогда инициатор перепосылает свой последний исходящий пакет, ответчик снова его получает, распознает его как совпадающий с последним пакетом от инициатора, т.е. ретрансмиссию, и в ответ перепосылает свой последний пакет.

2. События для перепосылки:
    - для стороны, выполняющей активную роль в ретрансмиссиях, событием для перепосылки своего последнего пакета является таймер и отсутствие ответа от партнера
    - для пассивной стороны событием для перепосылки своего последнего пакета является получение ретрансмиссии от партнера.

3. В сценариях IKE, в которых ответчик обрабатывает последний пакет (Aggressive Mode и Quick Mode без поддержки Commit Bit), ответчик становится активной стороной при ожидании последнего пакета обмена. В этих случаях инициатор уже не может выполнять активную роль, так как он в любом случае по сценарию не получает ответный пакет.

 Copyright © S-Terra CSP 2003 - 2015

18.6. Структура SNMPPollSettings

Структура задает настройки для выдачи информации по запросу SNMP-менеджера. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

Имя структуры SNMPPollSettings

Атрибуты LocalIPAddress
Port
ReadCommunity
SysLocation
SysContact

Атрибут LocalIPAddress

Атрибут LocalIPAddress задаёт локальный IPv4-адрес, на который можно получать запросы от SNMP-менеджера.

Синтаксис LocalIPAddress = IP | **ANY**

Значения IP –адрес – любой из локальных IP-адресов
ANY – все локальные IP-адреса

Значение по умолчанию ANY

Атрибут Port

Атрибут Port задаёт порт, на который можно получать SNMP-запросы.

Синтаксис Port = ЦЕЛОЕ32

Значение целое число из диапазона 1..65535

Значение по умолчанию 161.

Атрибут ReadCommunity

Атрибут ReadCommunity играет роль пароля при аутентификации сообщений SNMP и разрешает SNMP-менеджеру чтение статистики из базы управления SNMP-агента.

Синтаксис ReadCommunity = СТРОКА

Значение произвольный формат

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут SysLocation

Атрибут SysLocation содержит информацию о физическом расположении SNMP-агента.

Синтаксис SysLocation = СТРОКА

Значение произвольный формат, например "Building 3/Room 214"

Значение по умолчанию пустая строка.

Атрибут SysContact

Атрибут SysContact содержит информацию о контактном лице, ответственном за работу SNMP-агента.

Синтаксис SysContact = СТРОКА

Значение произвольный формат, например e-mail, телефон и т.д.

Значение по умолчанию пустая строка.

 Copyright © S-Terra CSP 2003 - 2015

18.7. Структура SNMPTrapSettings

Структура задает настройки для выдачи агентом сообщений менеджеру о возникшем прерывании в виде SNMP-трапов. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается. При отсутствии этой структуры трап-сообщения не высылаются.

Имя структуры SNMPTrapSettings

Атрибуты Receivers

Атрибут Receivers

Атрибут Receivers задаёт список получателей SNMP-трапов и дополнительные настройки.

Синтаксис Receivers* = `TrapReceiver`

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

18.8. Структура TrapReceiver

Структура описывает одного получателя SNMP-трапов и дополнительные настройки для трапов, отсылаемых на него.

Имя структуры TrapReceiver

Атрибуты IPAddress
Port
Community
Version
SNMPv1AgentAddress

Атрибут IPAddress

Атрибут IPAddress описывает IP-адрес получателя SNMP-трапов.

Синтаксис IPAddress = IP

Значение IP- адрес

Значение по умолчанию не существует, атрибут обязательный.

Атрибут Port

Атрибут Port задает UDP-порт, на который SNMP-менеджеру будут высылаться трап-сообщения.

Синтаксис Port = ЦЕЛОЕ32

Значение целое число из диапазона 1..65535.

Значение по умолчанию 162.

Атрибут Community

Атрибут Community играет роль идентификатора отправителя трап-сообщения.

Синтаксис Community = СТРОКА

Значение произвольный формат

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут Version

Атрибут Version указывает версию SNMP, в которой формируются трап-сообщения.

Синтаксис Version = **V1 | V2C**

Значение V1 – SNMP версии 1

V2C – SNMP версии 2c

Значение по умолчанию `V1.`

Атрибут SNMPv1AgentAddress

Атрибут SNMPv1AgentAddress задает IP-адрес источника трап-сообщения, который прописывается в поле Agent address внутри SNMP-пакета. Этот атрибут указывается только для Version = V1.

Синтаксис SNMPv1AgentAddress = IP

Значение IP-адрес

Значение по умолчанию `0.0.0.0.`

 Copyright © S-Terra CSP 2003 - 2015

18.9. Структура SyslogSettings

В конфигурации может присутствовать только один экземпляр этой структуры, поэтому этой структуре не может быть присвоено имя.

Структура SyslogSettings задает текущие настройки для SYSLOG-клиента. Структура SyslogSettings также позволяет отключить использование протокола SYSLOG.

Если активной является DDP (политика по умолчанию) или в LSP отсутствует структура SyslogSettings, то действуют локальные настройки, выставляемые в утилите make_inst.exe и записываемые в файл syslog.ini.

Имя структуры SyslogSettings

Атрибуты Server

Facility

Атрибут Server

Атрибут Server задает адрес SYSLOG-сервера.

Синтаксис Server = IP | **NO_SYSLOG**

Значение IP – одиночный IP- адрес. Указание адреса 0.0.0.0 аналогично указанию константы NO_SYSLOG, которая приводит к отключению использования протокола SYSLOG. При указании адреса 127.0.0.1 сообщения посылаются на локальный хост.

NO_SYSLOG – указание этой константы отключает использование протокола SYSLOG.

Значение по умолчанию не существует, атрибут обязательный.

Атрибут Facility

Атрибут Facility позволяет задать источник сообщений протокола SYSLOG.

Синтаксис Facility = СТРОКА

Значение

LOG_KERN	система ядра
LOG_USER -	пользовательские программы
LOG_MAIL –	почтовая системв
LOG_DAEMON	прочие процессы
LOG_AUTH –	система авторизации и безопасности
LOG_SYSLOG	производятся самим SYSLOG
LOG_LPR –	подсистема печати
LOG_NEWS -	подсистема сетевых сообщений
LOG_UUCP -	подсистема UUCP
LOG_CRON –	системные часы
LOG_AUTHPRIV	
LOG_FTP	
LOG_NTP	
LOG_AUDIT	
LOG_ALERT	
LOG_CRON2	

 Copyright © S-Terra CSP 2003 - 2015

LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5
LOG_LOCAL6
LOG_LOCAL7 – значение по умолчанию

Значение по умолчанию `LOG_LOCAL7`.

18.10. Структура RoutingTable

Структура RoutingTable описывает таблицу маршрутизации. Таблица содержит записи, необходимые для работоспособности конфигурации, успешное добавление которых в таблицу проверяется на момент загрузки конфигурации.

Если таблица содержит записи, которые уже присутствуют в системной таблице маршрутизации, то загрузка конфигурации будет продолжена остановлена с соответствующей диагностикой.

При отгрузке конфигурации из системной таблицы маршрутизации будут удалены все указанные в конфигурации записи маршрутизации, которые могли существовать и до загрузки этой конфигурации (например, добавленные командой `route add`).

В конфигурации допускается только один экземпляр этой структуры. Этой структуре не может быть присвоено имя.

Имя структуры RoutingTable

Атрибуты Routes

Атрибут Routes

Атрибут Routes содержит список записей таблицы маршрутизации.

Синтаксис Routes* = **`Route`**

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

18.11. Структура Route

Структура Route описывает одну запись (маршрут) в таблице маршрутизации.

Имя структуры Route

Атрибуты Destination

Gateway

NetworkInterface

Metric

Атрибут Destination

Атрибут Destination задает адрес назначения (получателя) пакета.

Синтаксис Destination = IP | IP/ЦЕЛОЕ32

Значение IP – адрес

IP/ЦЕЛОЕ32 – IP-адрес с маской подсети

Для указания маршрута, который будет использоваться по умолчанию, IP-адрес и маска подсети должны иметь значение 0.0.0.0/ 0.

Маршрут по умолчанию – маршрут, по которому будет отправлен пакет, если IP-адрес назначения, указанный в заголовке пакета, не совпадает ни с одним адресом назначения в таблице маршрутизации.

Значение по умолчанию отсутствует, атрибут обязательный.

Атрибут Gateway

Атрибут Gateway задает IP-адрес устройства, на который нужно передать пакет для продвижения его к получателю пакета. Атрибут Gateway должен отсутствовать при наличии атрибута `NetworkInterface`.

Синтаксис Gateway = IP

Значение IP –адрес

Значение по умолчанию используется значение из атрибута NetworkInterface.

Атрибут NetworkInterface

Атрибут NetworkInterface указывает имя выходного интерфейса, на который нужно передать пакет для продвижения его к получателю пакета.. Атрибут NetworkInterface должен отсутствовать при наличии атрибута `Gateway.`

Синтаксис NetworkInterface = СТРОКА

Значение имя интерфейса

Значение по умолчанию используется значение из атрибута Gateway.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут Metric

Использовать этот атрибут не рекомендуется, так как в разных ОС имеет разный смысл и будет проигнорирован.

Атрибут Metric задает метрику маршрута. В качестве метрики маршрута может использоваться любой показатель: длину маршрута, число промежуточных маршрутизаторов, надежность, задержка, затраты на передачу и др.

Синтаксис Metric = ЦЕЛОЕ32

Значение целое значение из диапазона 1.. 255

Значение по умолчанию 1.

 Copyright © S-Terra CSP 2003 - 2015

18.12. Правила пакетной фильтрации. Структура FilteringRule

Правила пакетной фильтрации содержат условия срабатывания правила и те действия, которые необходимо произвести с пакетом, в случае попадания пакета под правило.

Порядок перечисления правил фильтрации сушественен, так как правила срабатывают в прямом порядке перечисления в конфигурации.

При получении TCP/IP пакета просматриваются правила в порядке указания в локальной политике (конфигурации) и сравниваются параметры заголовка пакета, относящиеся к удаленному IP-хосту, до нахождения первого подходящего правила. Если правило не найдено – пакет уничтожается.

Правило считается подходящим, если в структуре FilteringRule в атрибутах PeerIPFilter и LocalIPFilter указаны параметры, совпадающие с параметрами в TCP/IP заголовке пакетов.

В случае выходящих пакетов параметры в атрибуте LocalIPFilter сравниваются с адресом источника пакета. Параметры в атрибуте PeerIPFilter сравниваются с адресом получателя пакета.

Для входящих пакетов параметры в атрибуте LocalIPFilter сравниваются с адресом получателя пакета. Параметры в атрибуте PeerIPFilter сравниваются с адресом источника пакета.

Структура FilterEntry формирует условие срабатывания конкретного правила пакетной фильтрации для партнеров по взаимодействию.

Имя структуры	FilteringRule
Атрибуты	PeerIPFilter
	LocalIPFilter
	NetworkInterfaces
	RefuseTCPPeerInit
	Action

Схематическое представление взаимосвязей структуры FilteringRule:

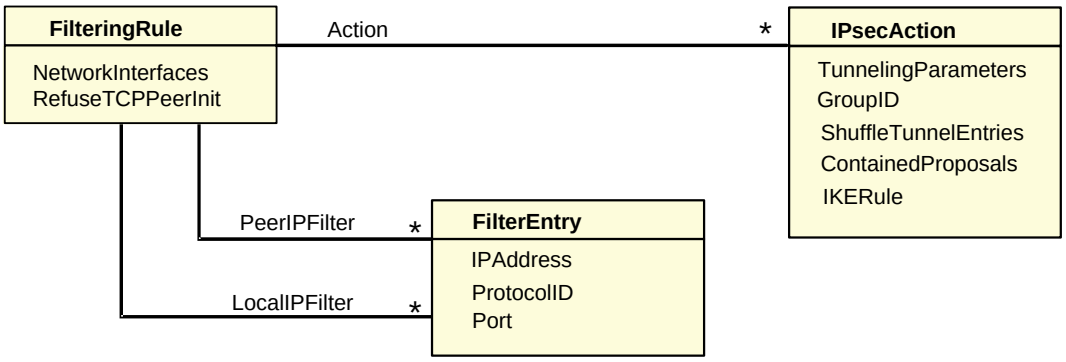


Рисунок 103

 Copyright © S-Terra CSP 2003 - 2015

Атрибут PeerIPFilter

Атрибут PeerIPFilter описывает параметры удаленного хоста, которые

- в случае выходящих пакетов будут сравниваться с адресом получателя пакета
- в случае входящих пакетов будут сравниваться с адресом источника пакета.

Этот атрибут представляет собой список структур FilterEntry.

Синтаксис PeerIPFilter* = `FilterEntry`

Значение по умолчанию весь сетевой трафик.

Атрибут LocalIPFilter

Атрибут LocalIPFilter описывает параметры защищаемого хоста, а также защищаемых подсетей, которые:

- в случае выходящих пакетов будут сравниваться с адресом источника пакета
- в случае входящих пакетов будут сравниваться с адресом получателя пакета.

Этот атрибут представляет собой список структур FilterEntry.

Синтаксис LocalIPFilter* = `FilterEntry`

Значение по умолчанию весь локальный и транзитный трафик.

Атрибут NetworkInterfaces

Атрибут NetworkInterfaces задает список сетевых интерфейсов, на которые могут приходить пакеты от партнера (с которых могут уходить пакеты партнеру).

Синтаксис NetworkInterfaces* = СТРОКА

Значения Список логических имен сетевых интерфейсов. Интерфейсы должны быть указаны в кавычках (кроме служебного слова ANY).

Значение по умолчанию ANY – задействуются все интерфейсы.

Атрибут RefuseTCPPeerInit

Атрибут RefuseTCPPeerInit задает блокировку входящих TCP-соединений; используется как дополнительное ограничение к действию.

Синтаксис RefuseTCPPeerInit* = **TRUE | FALSE**

Значения TRUE – уничтожается первый входящий TCP-пакет соединения, в результате отвергаются все TCP-соединения, инициированные извне

FALSE – не производится никаких дополнительных действий

Значение по умолчанию FALSE

 Copyright © S-Terra CSP 2003 - 2015

Атрибут Action

Атрибут Action описывает варианты действий, допускаемых VPN-устройством по взаимодействию с удаленным хостом.

Синтаксис Action *= (**IPsecAction** [, IPsecActionN]) | **(DROP)** | **(PASS)**

Значение

Действия формируются в виде списка цепочек из правил создания SA:

- в списке не должно быть одинаковых цепочек
- в списке вместо цепочки могут использоваться зарезервированные слова PASS или DROP. При этом:
  - определяется действие, которое будет применено к пакету, подпадающему под это правило пакетной фильтрации, при отсутствии соответствующего SA
  - в списке допускается только одна цепочка заданная таким образом
  - порядок указания такой цепочки в списке не имеет значения
- если в цепочке указано более одного правила, то все они, кроме последнего, должны иметь непустой атрибут **TunnelingParameters**..

Например,

[IPsecAction1] [IPsecAction2, IPsecAction3] [IPsecAction4] [PASS] [IPsecAction5]

Создание SA

Если устройство является инициатором соединения, то трафик будет обрабатываться в соответствии с первой цепочкой списка.

Если устройство является ответчиком, то правило обработки трафика выбирается путем сравнения каждой цепочки этого списка с каждой цепочкой своего списка и выбирается первая совпавшая цепочка.

Обработка трафика

Если выбранная цепочка состоит из двух правил [IPsecAction1, IPsecAction2] или более, то:

- исходящий трафик вначале обрабатывается контекстом, созданным по правилу IPsecAction2, а затем контекстом, созданным по правилу IPsecAction1
- для входящего трафика порядок применения контекстов обратный: вначале трафик обрабатывается контекстом, созданным по правилу IPsecAction1, а затем – IPsecAction2.

Значение по умолчанию (DROP)

Атрибут Firewall

Атрибут Firewall задает дополнительную фильтрацию пакетов по длине IP-пакета, смещению начала фрагмента пакета и контрольной сумме. Если длина пакета, смещение фрагмента пакета соответствуют заданным диапазонам значений в атрибуте Firewall – пакет уничтожается. Если контрольная сумма пакета совпадает с заданной в атрибуте Firewall – пакет уничтожается.

Синтаксис Firewall * = Firewall(

Name=”check_bad_ip_len_and_off”

 Copyright © S-Terra CSP 2003 - 2015

Args *=Totallen1, Totallen2, Fragoff1, Fragoff2

),

Firewall(

Name=”check_bad_ip_checksum”

Args *=Checksum

),

Значения

Totallen1, Totallen2 – задают диапазон длины IP-пакета в байтах

Fragoff1, Fragoff2 – задают диапазон смещения начала фрагмента внутри оригинального пакета в блоках по 8 байт

Checksum – задает значение контрольной суммы пакета.

Для исключения проверки по длине пакета, задайте диапазон 0, 65535.

Для исключения проверки по смещению фрагмента, задайте диапазон 0, 8191.

При получении пакета дополнительная проверка применяется только к открытым пакетам.

При задании атрибута Firewall сначала выполняется проверка на соответствие всем атрибутам структуры FilteringRule, а затем дополнительная проверка. При этом допускаются следующие значения в атрибутах:

PeerIPFilter, LocalIPFilter – IP-адреса, любые протоколы, Порты – не допускаются

Action – только значение [PASS]

NetworkInterfaces – ограничений нет

Firewall – дополнительные проверки.

В атрибуте Firewall проверки осуществляются последовательно. Если длина пакета и смещение начала фрагмента пакета попадают в соответствующие заданные диапазоны значений одновременно – пакет уничтожается, если нет – выполняется следующая проверка. При совпадении контрольной суммы – пакет уничтожается, при несовпадении - пакет пропускается, по следующим структурам FilteringRule проверка не выполняется.

Таким образом, пропускаются все пакеты, кроме тех, , у которых длина пакета и смещение фрагмента попадают в заданные диапазоны, или контрольная сумма равна заданной.

При уничтожении пакета выдается сообщение с указанием совпавших параметров, которое можно получить, задав команду klogview –l –f 0x80.

В LSP структуры FilteringRule с атрибутом Firewall должны быть расположены раньше, чем структуры FilteringRule с IPsec-фильтрами и портами.

Пример

```
FilteringRule f1 (
PeerIPFilter = FilterEntry(IPAddress = 10.0.16.2)
LocalIPFilter = FilterEntry(IPAddress = 0.0.0.0..255.255.255.255)
Action = [PASS]
NetworkInterfaces = "eth0"
Firewall *=
Firewall (
Name = "check_bad_ip_len_and_off"
Args *= 0, 200, 3, 02000h
```

```
),
Firewall (
Name = "check_bad_ip_checksum"
Args *= 5549h
))
```

18.13. Структура FilterEntry

Структура FilterEntry описывает параметры IP-заголовка пакета. Структура FilterEntry формирует условие срабатывания конкретного правила пакетной фильтрации.

Имя структуры FilterEntry

Атрибуты IPAddress

ProtocolID

Port

Атрибут IPAddress

Атрибут IPAddress описывает список адресов, состоящий из одиночных адресов, диапазонов адресов и подсетей, или всех локальных адресов устройства для срабатывания конкретного правила (FilteringRule).

Синтаксис IPAddress *= (IP, IP..IP, IP/ЦЕЛОЕ32) | **LOCAL_IP_ADDRESSES**

Значения IP – IP-адрес

IP..IP – диапазон IP-адресов

IP/ЦЕЛОЕ32 – IP-адрес с маской

LOCAL_IP_ADDRESSES – все локальные адреса устройства

Значение по умолчанию всевозможные IP-адреса.

Атрибут ProtocolID

Атрибут ProtocolID описывает список протоколов для срабатывания конкретного правила (FilteringRule).

Синтаксис ProtocolID *= ЦЕЛОЕ32

Значение целое число из диапазона 0..255.

Значение 0 означает все сетевые протоколы.

Значение по умолчанию все протоколы.

Атрибут Port

Атрибут Port описывает список идентификаторов портов для указанных протоколов объекта. Если атрибут ProtocolID отсутствует, то указанные порты будут применяться и к TCP(6) и к UDP(17).

Синтаксис Port *= ЦЕЛОЕ32

Значение целое число из диапазона 0..65535.

Значение 0 означает все порты для указанных протоколов.

Значение по умолчанию все порты.

Примечание:

В случае указания атрибута Port в отсутствии атрибута ProtocolID:

 Copyright © S-Terra CSP 2003 - 2015

- пакеты протоколов TCP и UDP подпадут под фильтр при условии совпадения порта;
- пакеты протоколов, не относящихся к TCP и UDP, которые по IP-адресам попадают на данный фильтр и не отфильтровываются раньше, будут уничтожены с диагностикой "no matching filtering rule".

18.14. Структура IPsecAction

Структура IPsecAction задает правило создания контекста соединения для протоколов семейства IPsec. Этой структуре может быть присвоено имя.

Имя структуры	IPsecAction
Атрибуты	TunnelingParameters
	ShuffleTunnelEntries
	CryptoContextsPerIPSecSA
	GroupID
	ContainedProposals
	IKERule
	NoPathMTUDiscovery
	NoSmoothRekeying

Структура IPsecAction

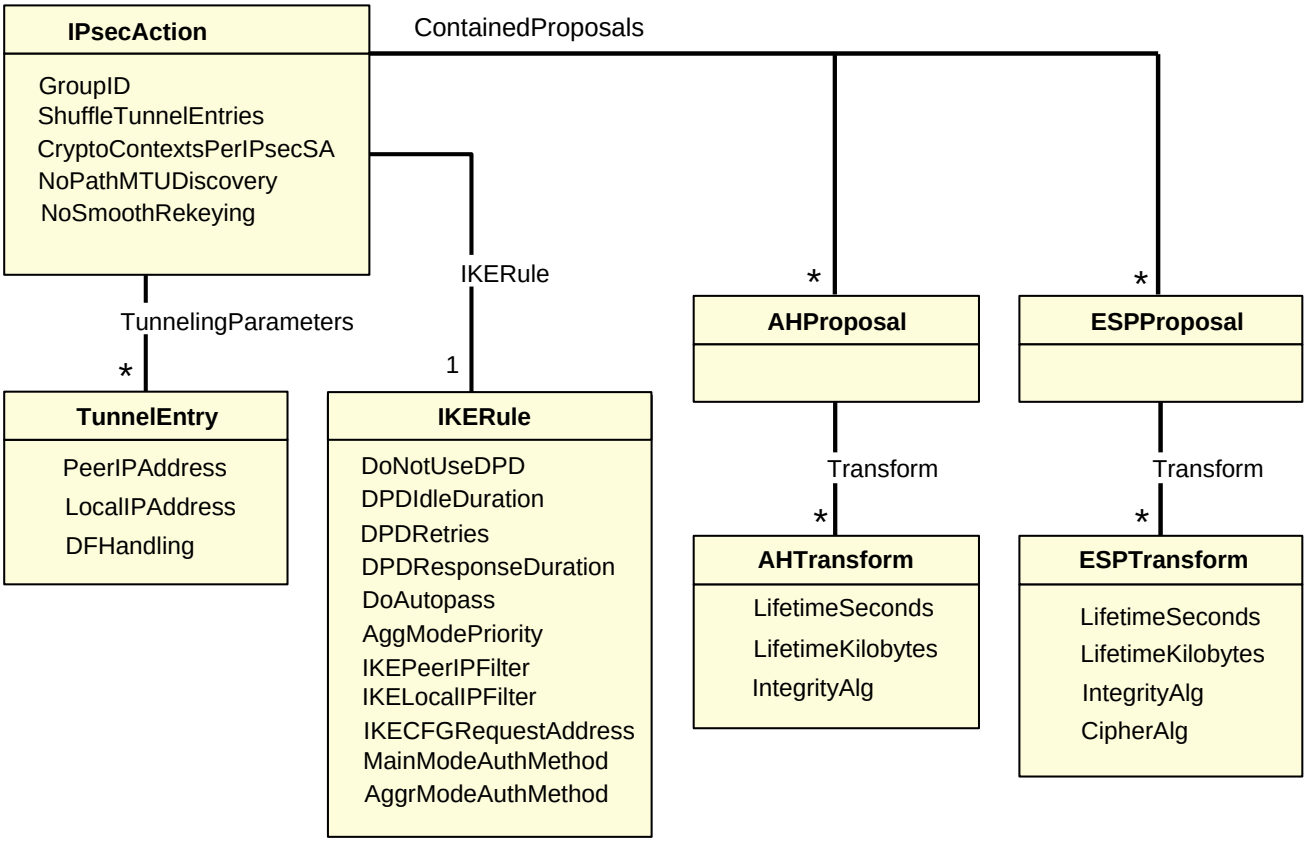


Рисунок 104

 Copyright © S-Terra CSP 2003 - 2015

Атрибут TunnelingParameters

Атрибут TunnelingParameters описывает параметры внешнего IP-заголовка пакета, который добавляется в туннельном режиме IPsec. Если в TunnelingParameters указано более одного элемента, то элементы используются как альтернативные партнеры. Если не удалось установить IPsec-туннель с партнером, то производиться попытка установить туннель со следующим партнером в списке, и так далее до окончания списка.

Синтаксис TunnelingParameters* = **TunnelEntry**

Значение по умолчанию используется транспортный режим.

Предупреждение: если между партнерами обнаружен NAT, то создавать соединение в транспортном режиме нельзя.

Атрибут ShuffleTunnelEntries

Атрибут ShuffleTunnelEntries задает порядок применения структур **TunnelEntry** в атрибуте TunnelingParameters. Атрибут ShuffleTunnelEntries игнорируется, если атрибут TunnelingParameters не задан.

Синтаксис ShuffleTunnelEntries = **TRUE | FALSE**

Значения TRUE – при загрузке конфигурации туннели в списке TunnelingParameters перемешиваются случайным образом

FALSE – при загрузке конфигурации туннели в списке TunnelingParameters применяются в порядке перечисления

Значение по умолчанию FALSE

Атрибут CryptoContextsPerIPSecSA

Атрибут CryptoContextsPerIPSecSA задает количество открываемых криптографических контекстов на один IPsec SA, созданный по этому правилу IPsecAction. Если данный атрибут не указан в правиле, то количество контекстов задается параметром из файла agent.ini DefaultCryptoContextsPerIPSecSA Наличие нескольких криптографических контекстов позволяет распараллелить обработку пакетов одним IPsec SA.

Синтаксис CryptoContextsPerIPSecSA = ЦЕЛОЕ32

Значения Целое число из диапазона 1..128.

Значение по умолчанию 1.

Атрибут IKERule

Атрибут IKERule является ссылкой на правило создания контекста соединения для ISAKMP-инициатора.

Синтаксис IKERule = **IKERule**

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут GroupID

Атрибут GroupID задает параметры получения ключевого материала. Используется алгоритм Диффи-Хеллмана либо VKO GOST R 34.10-2001 [RFC4357]. Параметры задаются в виде списка.. Если список не пуст, то для инициатора соединения ключевой материал всегда задаётся согласно первому компоненту списка. Для ответчика присланное предложение инициатора сравнивается последовательно со всеми элементами своего списка.

Синтаксис GroupID* = **VKO_1B, MODP_768, MODP_1024, MODP_1536**

Значения VKO_1B – используется алгоритм VKO GOST R 34.10-2001

MODP_768 – длина ключа 768 бит – группа 1

MODP_1024 – длина ключа 1024 бита - группа 2

MODP_1536 – длина ключа 1536 бит - группа 5

Значение по умолчанию ключевой материал заимствуется из первой фазы IKE.

Атрибут ContainedProposals

Каждая из структур AHProposal и ESPProposal содержит список вариантов преобразований (transforms). Структуры AHProposal и ESPProposal могут группироваться, позволяя обрабатывать трафик комбинацией протоколов AH и ESP.

Атрибут ContainedProposals содержит список единичных структур AHProposal и ESPProposal или их пар в порядке убывания приоритета.

Синтаксис ContainedProposals *= Proposal

Proposal *= (`AHProposal [,ESPProposal]`) | `ESPProposal`

Число элементов списка неограничено. Все элементы списка должны быть различными.

Один элемент списка содержит до двух преобразований с различными протоколами.

Если элемент списка содержит AHProposal и ESPProposal, то они должны следовать в указанном порядке.

Инициатор соединения посылает партнеру все варианты параметров защиты соединения, указанные в атрибуте ContainedProposals, с целью их согласования во время второй фазы IKE –сессии.

Ответная сторона присланные предложения инициатора соединения последовательно сравнивает с каждым элементом своего списка предложений и выбирает первое совпавшее. При переборе более приоритетным является список на стороне ответчика.

Параметры преобразований и комбинация протоколов AH и ESP определяют качество защиты соединения.

Запись `(ah1, esp1),(esp2),(ah3)` означает, что рассматриваются варианты контекстов: либо связка `(ah1, esp1),` либо proposal `esp2,` либо proposal `ah3.`

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

Пример

```
ContainedProposals *=
(IPsec_ah_md5, IPsec_esp_des3),(IPsec_ah_md5, IPsec_esp_idea)
(* (AH(MD5) и ESP(DES3) или AH(MD5) и ESP(IDEA) *)


ContainedProposals *=
(IPsec_ah_md5, IPsec_esp_des3),(IPsec_ah_md5)
  (* (AH(MD5) и ESP(DES3) или  AH(MD5) *)


ESPProposal IPsec_esp_idea(
  Transform *= ESPTransform(
    CipherAlg = "IDEA-CBC"
  )
)
AHProposal IPsec_ah_md5(
  Transform *= AHTransform(
    IntegrityAlg* = "MD5-H96-HMAC"
  )
)
ESPProposal IPsec_esp_des3(
  Transform *= ESPTransform(
    CipherAlg = "DES3-K168-CBC"
  )
)
```

Атрибут NoSmoothRekeying

Атрибут NoSmoothRekeying задает режим "мягкой" смены ключевого материала.

Синтаксис NoSmoothRekeying = **TRUE | FALSE**

Значения TRUE – заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего IPsec соединения, новый IPsec SA создаётся только по запросу из ядра – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате, во время создания нового IPsec SA IP-трафик приостанавливается, а при интенсивном трафике возможна потеря пакетов.

FALSE – заблаговременно, незадолго до окончания действия IPsec соединения, на его основе (с теми же параметрами) проводится IKE-сессия (Quick Mode) по созданию нового IPsec SA – rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика.[6]

Значение по умолчанию FALSE

NoPathMTUDiscovery

Этот атрибут отключает алгоритм "Path MTU Discovery" (выявление максимального размера блока передачи, проходящего на всем пути от отправителя к получателю без фрагментации) для IPsec SA, создаваемых по данному правилу.

Синтаксис: NoPathMTUDiscovery = **TRUE | FALSE**

[6]Для проведения rekeying-а необходимо, чтобы время жизни обновляемого соединения было существенно больше времени, которое отводится на проведение IKE-сессии.

Значения: FALSE – производится обработка ICMP-сообщений типа destination unreachable/fragmentation needed, приходящих в ответ на IPsec-пакеты. На основе этих сообщений вычисляется эффективное значение MTU трассы (максимальный размер блока, проходящий по всему каналу без фрагментации).

TRUE – берется значение MTU сетевого интерфейса, через который отправляется пакет.

Значение по умолчанию FALSE

18.15. Структура TunnelEntry

Структура TunnelEntry описывает параметры внешнего IP-заголовка пакета при использовании туннельного режима IPsec.

Имя структуры TunnelEntry

Атрибуты PeerIPAddress

LocalIPAddress

DFHandling

Атрибут PeerIPAddress

Атрибут PeerIPAddress описывает туннельный адрес. Этот адрес используется для двух целей – адрес получателя во внешнем IP-заголовке и адрес IKE-партнера, если последний не задан явно.

Синтаксис PeerIPAddress = IP

Значение по умолчанию

- если туннельный адрес используется как адрес получателя во внешнем IP заголовке, то
  - для исходящего пакета берется адрес IKE партнера
- если туннельный адрес используется как адрес IKE партнера:
  - для исходящего пакета берется адрес из IP пакетов, вызвавших создание соединения
  - для входящего пакета – принимается любой адрес

Атрибут LocalIPAddress

Атрибут LocalIPAddress описывает туннельный адрес локального VPN-устройства.

Синтаксис LocalIPAddress = IP

Значение по умолчанию для исходящего пакета - любой из адресов сетевого интерфейса, с которого отправляется пакет.

Атрибут DFHandling

Атрибут DFHandling задает алгоритм формирования DF (Don't Fragment) бита внешнего IP-заголовка для туннельного режима IPsec.

Синтаксис DFHandling = **COPY | SET | CLEAR**

Значения COPY - копировать DF бит из внутреннего заголовка во внешний заголовок

SET - всегда устанавливать DF бит внешнего заголовка в 1

CLEAR – всегда сбрасывать DF бит внешнего заголовка в 0.

Значение по умолчанию COPY.

 Copyright © S-Terra CSP 2003 - 2015

Пример структуры IPsecAction

```
IPsecAction tunnel_ipsec_des_md5_action(
  TunnelingParameters *= TunnelEntry(
    PeerIPAddress = 192.168.2.1
    DFHandling = CLEAR
  )

  IKERule = ike_r
  GroupID *= MODP_768, MODP_1024
  ContainedProposals *= (ipsec_ah_md5,  ipsec_esp_des),
(ipsec_esp_des_md5)
)

ESPProposal ipsec_esp_des(
  Transform *= ESPTransform(
    CipherAlg *= "DES-CBC"
  )
)

AHProposal I ipsec_ah_md5(
  Transform *= AHTransform(
    IntegrityAlg *= "MD5-H96-HMAC"
  )
)

ESPProposal ipsec_esp_des_md5(
  Transform *= ESPTransform(
    CipherAlg *= "DES-CBC"
    IntegrityAlg *= "MD5-H96-HMAC"
  )
)
```

 Copyright © S-Terra CSP 2003 - 2015

18.16. Структуры AHProposal и ESPProposal

Структура AHProposal задает список криптографических преобразований (transforms) протокола AH в порядке убывания приоритета, которые допускаются для обработки трафика. Трафик – количество килобайт данных, обработанных данным контекстом.

Структура ESPProposal определяет список преобразований (transforms) протокола ESP в порядке убывания приоритета, которые допускаются для обработки специфицированного трафика.

Имя структуры AHProposal

Атрибуты Transform

Имя структуры ESPProposal

Атрибуты Transform

Атрибут Transform

Атрибут Transform задает список возможных групп параметров протокола AH (для структуры AHProposal) или ESP (для структуры ESPProposal), необходимых для создания SA, расположенных в порядке убывания их приоритета.

Синтаксис Transform *= `AHTransform` # для структуры AHProposal

Transform *= `ESPTransform` # для структуры ESPProposal

Должен присутствовать хотя бы один трансформ.

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

18.17. Структура AHTransform

Структура AHTransform задает параметры контекста (SA) AH.

Имя AHTransform

Атрибуты LifetimeSeconds

LifetimeKilobytes

IntegrityAlg

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает максимальное время существования контекста (SA) AH (в секундах).[7]

Синтаксис LifetimeSeconds = ЦЕЛОЕ32

Значение число из диапазона 1.. 4 294 967 295.

Значение по умолчанию 28800 (8 часов).

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах. Трафик – количество килобайт данных, обработанных данным контекстом.[8]

Синтаксис LifetimeKilobytes = ЦЕЛОЕ32

Значение число из диапазона 1..4 294 967 295.

Значение по умолчанию нет ограничений на действие SA.

Атрибут IntegrityAlg

Атрибут IntegrityAlg задает набор предлагаемых/допустимых алгоритмов проверки целостности в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм проверки целостности пакета.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов (их комбинацию) проверки целостности, то используйте альтернативный подход: в атрибуте Transform структуры AHProposal укажите список структур AHTransform, а в каждой структуре AHTransform задайте только один алгоритм проверки целостности.

Синтаксис IntegrityAlg* = СТРОКА

[7] В случае использования связок (AH+ESP) в качестве элементов списка ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформах уравниваются в меньшую сторону.

[8] В случае использования связок (AH+ESP) в качестве элементов списка ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформах уравниваются в меньшую сторону.

 Copyright © S-Terra CSP 2003 - 2015

Значение Возможные значения:

"MD5-H96-KPDK" - Keyed MD5

"MD5-H96-HMAC" - HMAC MD5 (96 бит)

"SHA1-H96-HMAC" - HMAC SHA-1 (96 бит)

"GR341194CPRO1-H96-HMAC-254" – реализация ГОСТ Р 34.11-94 (96 бит)

Значение по умолчанию не существует, атрибут обязательный.

18.18. Структура ESPTransform

Структура ESPTransform задает параметры контекста (SA) ESP.

Имя	ESPTransform
Атрибуты	LifetimeSeconds
	LifetimaKilobytes
	CipherAlg
	IntegrityAlg

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает максимальное время существования контекста в секундах.[9]

Синтаксис	LifetimeSeconds = ЦЕЛОЕ32
Значение	Целое число из диапазона 1..4 294 967 295.
Значение по умолчанию	28800 (8 часов).

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах. Трафик – количество килобайт данных, обработанных данным контекстом.[10]

Синтаксис	LifetimeKilobytes = ЦЕЛОЕ32
Значение	Целое число из диапазона 1..4 294 967 295.
Значение по умолчанию	нет ограничений на действие SA.

Атрибут CipherAlg

Атрибут CipherAlg задает набор предлагаемых/допустимых алгоритмов шифрования трафика в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм шифрования трафика.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

[9] В случае использования связок (AH+ESP) в качестве элементов списка ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформах уравниваются в меньшую сторону

[10] В случае использования связок (AH+ESP) в качестве элементов списка ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформах уравниваются в меньшую сторону

 Copyright © S-Terra CSP 2003 - 2015

Если же существует необходимость задать несколько алгоритмов шифрования, то используйте альтернативный подход: в атрибуте Transform структуры ESPProposal укажите список структур ESPTransform, а в каждой структуре ESPTransform задайте только один алгоритм шифрования.

Синтаксис CipherAlg* = СТРОКА

Значение Возможные значения:

"NULL" – NULL (данные не шифруются)

"DES-CBC_IV64" – DES в режиме CBC с явным IV длиной 64 бита

"DES-CBC_IV32" – DES в режиме CBC с явным IV длиной 32 бита

"DES-CBC" – DES в режиме CBC

"DES3-K168-CBC" – DES3 в режиме CBC

"IDEA-CBC" – IDEA в режиме CBC

"AES-K128-CBC" – AES в режиме CBC с длиной ключа 128

"AES-K192-CBC" – AES в режиме CBC с длиной ключа 192

"AES-K256-CBC" – AES в режиме CBC с длиной ключа 256

"G2814789CPRO1-K256-CBC-254" – реализация ГОСТ 28147-89 в режиме CBC

"G2814789CPRO1-K288-CNTMAC-253" – реализация ГОСТ 28147-89 в комбинированном режиме (гаммирование и вычисление имитовставки) в соответствии со спецификацией ESP_GOST-4M-IMIT (Методические рекомендации по использованию комбинированного алгоритма шифрования вложений IPsec ESP на основе ГОСТ 28147-89 (Проект) "rus-fedchenko-cpesp-ipsecme-gost-00-rt.pdf").

Значение по умолчанию не существует, атрибут обязательный.

Атрибут IntegrityAlg

Атрибут IntegrityAlg задает набор предлагаемых/допустимых алгоритмов проверки целостности пакета в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм проверки целостности пакета.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов проверки целостности (их комбинацию), то используйте альтернативный подход: в атрибуте Transform структуры ESPProposal укажите список структур ESPTransform, а в каждой структуре ESPTransform задайте только один алгоритм проверки целостности пакета.

Синтаксис IntegrityAlg* = СТРОКА

Значение Возможные значения:

"MD5-H96-KPDK" – Keyed MD5

"MD5-H96-HMAC" – HMAC MD5 (96 бит)

"SHA1-H96-HMAC" – HMAC SHA-1 (96 бит)

"GR341194CPRO1-H96-HMAC-65534" – реализация ГОСТ Р 34.11-94 (96 бит)

 Copyright © S-Terra CSP 2003 - 2015

Значение по умолчанию при отсутствии в связке контекстов компонента AHProposal, список должен содержать хотя бы один элемент. Иначе функциональность проверки целостности пакетов возлагается на протокол AH.

Пример структуры ESPProposal

```
ESPTransform esp_trf_01(
 LifetimeSeconds = 28800
 LifetimeKilobytes = 4608000
 CipherAlg  *= "G2814789CPRO1-K256-CBC-254"
 IntegrityAlg *= "GR341194CPRO1-H96-HMAC-65534"
)
ESPTransform esp_trf_02(
 LifetimeSeconds = 28800
 LifetimeKilobytes = 4608000
 CipherAlg  *= "G2814789CPRO1-K256-CBC-254"
 IntegrityAlg *= "MD5-H96-HMAC"
)
ESPTransform esp_trf_03(
 LifetimeSeconds = 28800
 LifetimeKilobytes = 4608000
 CipherAlg  *= "G2814789CPRO1-K256-CBC-254"
 IntegrityAlg *= "SHA1-H96-HMAC"
)
ESPProposal ESP_1(
 Transform *= esp_trf_01,esp_trf_02,esp_trf_03
)
```

 Copyright © S-Terra CSP 2003 - 2015

18.19. Структура IKERule

Структура IKERule описывает правило создания контекста соединения для протокола IKE.

Имя структуры	IKERule
Атрибуты	IKEPeerIPFilter
	IKELocalIPFilter
	DoNotUseDPD
	DPDIdleDuration
	DPDResponseDuration
	DPDRetries
	IKECFGRequestAddress
	DoAutopass
	AggrModeAuthMethod
	MainModeAuthMethod
	AggrModePriority
	Transform

Схематическое представление структуры IKERule и структур, на которые ссылаются атрибуты IKERule:

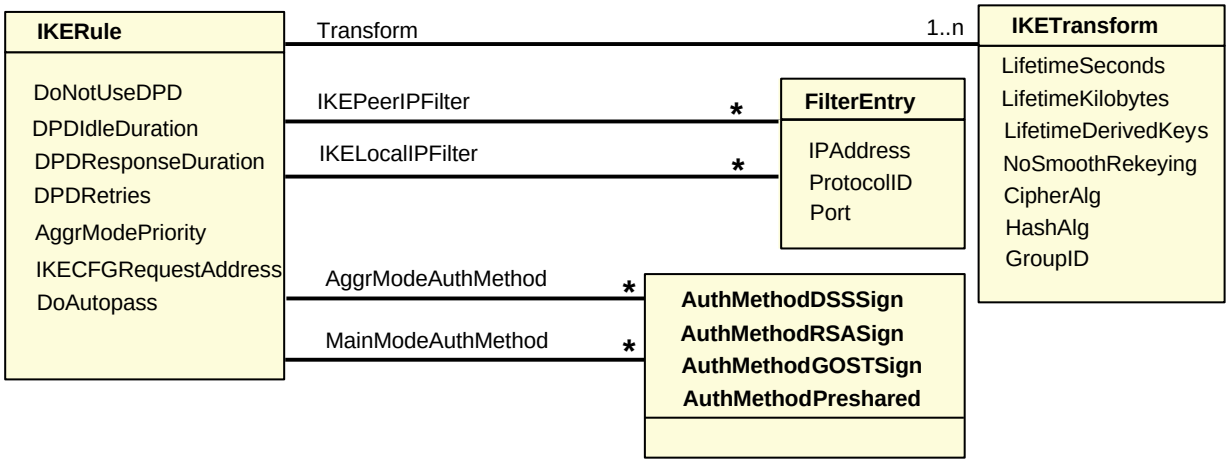


Рисунок 105

 Copyright © S-Terra CSP 2003 - 2015

Атрибут IKEPeerIPFilter

Атрибут IKEPeerIPFilter описывает список допустимых IP-адресов партнера, при которых применяется данное правило.

Этот атрибут используется VPN-устройством, выступающим в роли ответчика IKE-сессии, при проверке UDP-заголовка первого (входящего) пакета.

Для VPN-устройства, выступающего в роли инициатора создания IKE-сессии, этот атрибут игнорируется.

Синтаксис IKEPeerIPFilter* = **FilterEntry**

Значения В качестве элементов списка могут использоваться структуры **FilterEntry**, используемые в **FilteringRule**, либо самостоятельные структуры **FilterEntry**. При этом для каждого элемента:

адрес: учитываются все единичные IP-адреса и диапазоны. При наличии хотя бы одного элемента без IP-адресов, принимается логика проверки IP-адреса IKE-партнера по умолчанию.

значения протоколов игнорируются. При анализе входящего ISAKMP-пакета в качестве протокола всегда подразумевается UDP.

значения портов игнорируются. При анализе входящего ISAKMP-пакета допускаются любые порты партнера.

Значение по умолчанию

При проверке IP-адреса IKE-партнера учитываются все возможные значения IP-адресов, используемых в структурах **TunnelEntry** в списках **TunnelingParameters** всех возможных структур **IPsecAction**, которые в свою очередь используют текущее правило **IKERule**. Если в какой-либо из таких структур **TunnelEntry** не задано поле PeerIPAddress, то данное правило **IKERule** может быть использовано с любым партнером.

Если в структурах **IPsecAction** атрибут **TunnelingParameters** отсутствует (работает транспортный режим), то IP-адрес IKE-партнера проверяется по атрибуту **PeerIPFilter** всех структур **FilteringRule**, в которых используется данное правило **IPsecAction**.

Атрибут IKELocalIPFilter

Атрибут IKELocalIPFilter описывает список допустимых локальных IP-адресов, при которых применяется данное правило.

Этот атрибут используется VPN-устройством, выступающим в роли ответчика IKE-сессии, при проверке UDP-заголовка первого (входящего) пакета.

Для VPN-устройства, выступающего в роли инициатора создания IKE-сессии, этот атрибут игнорируется.

Синтаксис IKELocalIPFilter* = **FilterEntry**

Значения В качестве элементов списка могут использоваться структуры **FilterEntry**, используемые в **FilteringRule**, либо самостоятельные структуры **FilterEntry**. При этом для каждого элемента:

адрес: учитываются все единичные IP-адреса и диапазоны. При наличии хотя бы одного элемента без IP-

 Copyright © S-Terra CSP 2003 - 2015

адресов, принимается логика проверки IP-адреса IKE-партнера по умолчанию.

значения протоколов игнорируются. При анализе входящего ISAKMP-пакета в качестве протокола всегда подразумевается UDP.

значения портов игнорируются. При анализе входящего ISAKMP-пакета допускаются следующие локальные порты:

согласно **IKEParameters**→DefaultPort (по умолчанию – 500)

4500 (используется для NAT Traversal).

Значение по умолчанию адрес – любой из локальных адресов VPN-устройства

протокол – UDP

порт – 500.

Атрибут DoNotUseDPD

Атрибут DoNotUseDPD задает режим использования протокола DPD (Dead Peer Detection).

Синтаксис DoNotUseDPD = **TRUE | FALSE**

Значение TRUE – не использовать протокол DPD

FALSE – использовать протокол DPD

Значение по умолчанию FALSE.

Атрибут DPDIdleDuration

Атрибут DPDIdleDuration задает допустимый период времени отсутствия входящего трафика от партнера, по истечении которого, при наличии исходящего трафика, активируется DPD-сессия. Если атрибут DoNotUseDPD = TRUE, то атрибут DPDIdleDuration игнорируется.

Синтаксис DPDIdleDuration = ЦЕЛОЕ32

Значение целое значение из диапазона 1..32767

Значение по умолчанию 60.

Атрибут DPDResponseDuration

Атрибут DPDResponseDuration задает время ожидания ответа от партнера на DPD запрос в секундах. Если атрибут DoNotUseDPD = TRUE, то атрибут DPDResponseDuration игнорируется.

Синтаксис DPDResponseDuration = ЦЕЛОЕ32

Значение целое значение из диапазона 1..300

Значение по умолчанию 5.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут DPDRetries

Атрибут DPDRetries задает число попыток провести DPD обмен. Если все попытки закончились неудачей, защищенное соединение (IKE-контекст) считается "мертвым", и производится попытка создать его заново. Если атрибут DoNotUseDPD = TRUE, то атрибут DPDRetries игнорируется.

Синтаксис DPDRetries = ЦЕЛОЕ32

Значение целое значение из диапазона 1..10

Значение по умолчанию 3.

Атрибут IKECFGRequestAddress

Атрибут IKECFGRequestAddress задает режим работы IKECFG-клиента.

Синтаксис IKECFGRequestAddress = **TRUE** | **FALSE**

Значение TRUE – агент является активным IKECFG-клиентом, т.е.агент инициирует посылку запроса на получение внутреннего IP-адреса у партнера сразу после создания IKE SA. Возможны следующие варианты дальнейшей работы агента:

Состояние партнера		**Дальнейшие действия агента**
Партнер является IKECFG-сервером	Успешно выделен IP-адрес из IKECFG-пула	a) Инициируется вторая фаза IKE b) Полученный адрес будет использован в качестве локального для пакетов, которые будут обрабатываться IPsec SA, созданными на основе исходного ISAKMP SA (включая его потомков – rekeying).
	Выдача адреса невозможна в ходе текущей IKECFG-сессии	Инициируется вторая фаза создания соединения, в ходе которой может быть инициирована новая IKECFG-сессия со стороны партнера для выдачи IP-адреса.
	Ошибка выдачи адреса (например, пул адресов исчерпан)	Создание соединения будет остановлено.
Партнер не является IKECFG-сервером		Инициируется вторая фаза создания соединения.

FALSE - агент является пассивным IKECFG-клиентом, т.е. IKECFG-сессия может быть проведена только по инициативе партнера, если он является IKECFG –сервером.

Значение по умолчанию FALSE

 Copyright © S-Terra CSP 2003 - 2015

Атрибут DoAutopass

Атрибут DoAutopass задает автоматическое создание фильтра для пропускания ISAKMP-трафика.

Синтаксис DoAutopass = TRUE | FALSE

Значение TRUE:

автоматически пропускать ISAKMP-пакеты, соответствующие атрибутам **IKEPeerIPFilter** и **IKELocalIPFilter**

при отсутствии IP-адреса в атрибуте **IKEPeerIPFilter** , IP-адреса для построения фильтра берутся из атрибута **TunnelingParameters** всех структур **IPsecAction**, ссылающихся на данное правило IKE

для структур **IPsecAction**, ссылающихся на данное правило IKE, в которых атрибут **TunnelingParameters** отсутствует, IP-адреса берутся из атрибутов **PeerIPFilter**, **LocalIPFilter** всех структур **FilteringRule**, имеющих ссылки на такие **IPsecAction**

FALSE:

не пропускать автоматически ISAKMP-трафик. Правило фильтрации (Filtering Rule) с действием PASS должно быть задано явно (вручную) для пропускания ISAKMP-трафика.

Значение по умолчанию FALSE.

Атрибут AggrModeAuthMethod

Атрибут AggrModeAuthMethod содержит список структур, определяющих способ и параметры аутентификации в агрессивном режиме IKE. В списке не должно быть задано двух одинаковых методов аутентификации.

Примечание: Хотя бы один из атрибутов AggrModeAuthMethod или MainModeAuthMethod должен быть задан.

Синтаксис AggrModeAuthMethod* = AuthMethodDSSSign | AuthMethodRSASign | FuthMethodGOSTSign | AuthMethodPreshared

Значение AuthMethodDSSSign – Аутентификация DSA подписью

AuthMethodRSASign – Аутентификация RSA подписью

AuthMethodGOSTSign – Аутентификация при помощи подписи алгоритмом ГОСТ34.10

AuthMethodPreshared – Аутентификация при помощи предустановленного ключа.

Значение по умолчанию При отсутствии MainModeAuthMethod атрибут является обязательным.

При наличии атрибута MainModeAuthMethod Aggressive Mode не проводится.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут MainModeAuthMethod

Атрибут MainModeAuthMethod содержит список структур, определяющих способ и параметры аутентификации в основном режиме IKE. В списке не должно быть задано двух одинаковых методов аутентификации.

Примечание: Хотя бы одно из атрибутов AggrModeAuthMethod или MainModeAuthMethod должен быть задан.

Синтаксис MainModeAuthMethod* = AuthMethodDSSSign | AuthMethodRSASign | FuthMethodGOSTSign | AuthMethodPreshared

Значение

AuthMethodDSSSign – Аутентификация DSA подписью

AuthMethodRSASign – Аутентификация RSA подписью

AuthMethodGOSTSign – Аутентификация при помощи подписи алгоритмом ГОСТ3410

AuthMethodPreshared – Аутентификация при помощи предустановленного ключа.

Значение по умолчанию При отсутствии атрибута AggrModeAuthMethod атрибут является обязательным.

При наличии атрибута AggrModeAuthMethod Main Mode не проводится.

Атрибут AggrModePriority

AggrModePriority задает режим использования Aggressive Mode. Атрибут используется только для инициатора в случае, если заданы значения MainModeAuthMethod и AggrModeAuthMethod одновременно. Атрибут игнорируется, если задан только один режим (Main Mode или Aggressive Mode)

Синтаксис AggrModePriority = **TRUE** | **FALSE**

Значение TRUE – Aggressive Mode является более приоритетным, инициатор начинает первую фазу IKE в "агрессивном" режиме.

FALSE – Main Mode является более приоритетным, то инициатор начинает первую фазу IKE в "основном" режиме.

Значение по умолчанию FALSE.

Атрибут Transform

Атрибут Transform задает список допустимых групп параметров протокола ISAKMP для создания SA. Количество элементов списка не ограничего.

Синтаксис Transform* = `IKETransform`

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

18.20. Структура IKETransform

Структура IKETransform задает набор параметров, необходимых для создания ISAKMP SA.

Имя структуры IKETransform

Атрибуты LifetimeSeconds
LifetimaKilobytes
LifetimeDerivedKeys
NoSmoothRekeying
CipherAlg
HashAlg
GroupID

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает время существования IKE- контекста (в секундах).

Синтаксис LifetimeSeconds = ЦЕЛОЕ32

Значение Целое число из диапазона 1..4 294 967 295.

Значение по умолчанию нет ограничений на действие SA.

Для совместимости IOS-партнером (Cisco) нужно всегда указывать в своем предложении атрибут LifetimeSeconds – время жизни в секундах и высылать IOS-партнеру. В противном случае, IOS будет пытаться поместить в принятое предложение новый атрибут – время жизни SA по времени, которое IOS-ом будет установлено для создаваемого SA. Это является неприемлемым для агента и CSP VPN Gate, будучи партнером IOS, прекращает у становление соединения.

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах.

Синтаксис LifetimeKilobytes = ЦЕЛОЕ32

Значение Целое число из диапазона 1..4 294 967 295.

Значение по умолчанию нет ограничений на действие SA.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут LifetimeDerivedKeys

Атрибут LifetimeDerivedKeys задает ограничение по числу IPsec SA (числу успешных Quick Mode - QM), которые можно сделать с использованием одного IKE-контекста.

Синтаксис LifetimeDerivedKeys = ЦЕЛОЕ32

Значение Целое число из диапазона 1..4 294 967 295.

Значение по умолчанию нет ограничений на действие SA по числу созданных под его защитой IPsec SA.

Атрибут NoSmoothRekeying

Атрибут NoSmoothRekeying задает режим "мягкой" смены ключевого материала.

Синтаксис NoSmoothRekeying = **TRUE | FALSE**

Значение TRUE – заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего ISAKMP SA, новый ISAKMP SA создаётся только по запросу из ядра на создание IPsec SA – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате процесс создания IPsec SA существенно задерживается

FALSE – заблаговременно, незадолго до окончания действия ISAKMP SA, на его основе (по тем же правилам и с теми же Identity) проводится IKE-сессия по созданию нового ISAKMP SA – rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика[11]

Значение по умолчанию FALSE

Атрибут CipherAlg

Атрибут CipherAlg задает набор предлагаемых/допустимых алгоритмов шифрования для ISAKMP.

Рекомендуется указывать не список алгоритмов, а только один алгоритм шифрования.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов шифрования (их комбинацию), то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только один алгоритм шифрования (см. Пример структуры IKERule).

[11] Для проведения rekeying необходимо, чтобы время жизни обновляемого соединения было существенно больше времени, которое отводится на проведение IKE-сессии.

 Copyright © S-Terra CSP 2003 - 2015

Синтаксис CipherAlg* = СТРОКА

Значение возможные значения:

"DES-CBC" - DES в режиме CBC

"IDEA-CBC" - IDEA в режиме CBC

"DES3-K168-CBC" - DES3 в режиме CBC

"AES-K128-CBC" - AES в режиме CBC с длиной ключа 128

"AES-K192-CBC" - AES в режиме CBC с длиной ключа 192

"AES-K256-CBC" - AES в режиме CBC с длиной ключа 256

"G2814789CPRO1-K256-CBC-65534" – реализация ГОСТ 28147-89 в режиме CBC

Значение по умолчанию не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

Атрибут HashAlg

Атрибут HashAlg задает набор предлагаемых/допустимых алгоритмов вычисления хэша для ISAKMP.

Рекомендуется указывать не список алгоритмов, а только один алгоритм хэширования.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов хэширования, то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только один алгоритм хэширования (см. Пример структуры IKERule).

Синтаксис HashAlg* = СТРОКА

Значение "MD5"

"SHA1"

"GR341194CPRO1-65534" – реализация ГОСТ Р 34.11-94

Значение по умолчанию не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

Атрибут GroupID

Атрибут GroupID описывает предлагаемые/допустимые параметры выработки ключевого материала для ISAKMP. Используется алгоритм VKO ГОСТ Р 34.10-2001 [RFC4357] либо алгоритм Диффи-Хеллмана.

Рекомендуется указывать не список параметров, а только один элемент списка..

Если же указан список и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать список то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только один элемент списка (см. Пример структуры IKERule – MainMode).

При использовании атрибута GroupID для Aggressive Mode число предлагаемых элементов списка должно быть равно единице. Это связано с тем, что в Aggressive Mode вычисление ключевых пар в соответствии с предлагаемым алгоритмом производится сразу, не дожидаясь ответа от партнера.

 Copyright © S-Terra CSP 2003 - 2015

Синтаксис GroupID* = **VKO_1B, MODP_768, MODP_1024, MODP_1536**

Значение VKO_1B – используется алгоритм VKO GOST R 34.10-2001

MODP_768 – стандартная Oakley-группа с длиной ключа 768 бит – группа 1

MODP_1024 – стандартная Oakley-группа с длиной ключа 1024 бита – группа 2

MODP_1536 – стандартная Oakley-группа с длиной ключа 1536 бит – группа 5

Значение по умолчанию не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

Примечание

Стоит отметить, что в правиле IKE (IKERule) предоставление партнеру выбора различных элементов списка возможно только в основном режиме IKE (MainMode). Если правило IKE предусматривает агрессивный режим (присутствует структура AggrModeAuthMethod), то в этом правиле IKERule во всех структурах IKETransform атрибут GroupID должен иметь только одно значение и оно должно быть одинаковым во всех структурах IKETransform, т.е. должна быть указана одна и та же Oakley-группа либо VKO_1B.

Пример структуры IKERule

```
IKETransform ike_trf_01(
 LifetimeSeconds = 28800
 CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
 HashAlg *= "GR341194CPRO1-65534"
 GroupID *= VKO_1B
)
IKETransform ike_trf_02(
 LifetimeSeconds = 28800
 CipherAlg  *= "G2814789CPRO1-K256-CBC-65534"
 HashAlg *= "GR341194CPRO1-65534"
 GroupID *= MODP_1536
)
IKETransform ike_trf_03(
 LifetimeSeconds = 28800
 CipherAlg  *= "DES-CBC"
 HashAlg *= "GR341194CPRO1-65534"
 GroupID *= MODP_1024
)
IKETransform ike_trf_04(
 LifetimeSeconds = 28800
 CipherAlg  *= "AES-K128-CBC"
 HashAlg *= "GR341194CPRO1-65534"
 GroupID *= MODP_768
)
IKERule ike_rule(
 DoNotUseDPD = FALSE
 DPDIdleDuration = 60
 DPDResponseDuration = 5
 DPDRetries = 3
 MainModeAuthMethod *= auth_method_01
 Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
 DoAutopass = TRUE
)
IdentityEntry auth_identity_01(
)
```

 Copyright © S-Terra CSP 2003 - 2015

```
AuthMethodPreshared auth_method_01(
 SharedIKESecret = "dfd"
 LocalID = auth_identity_01
)
```

18.21. Структуры для аутентификации

Схема данных структур AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign, AuthMethodPreshared, описывающих идентификационную информацию, предполагаемую к использованию при создании IKE контекста соединения, представлена на рисунке ниже.

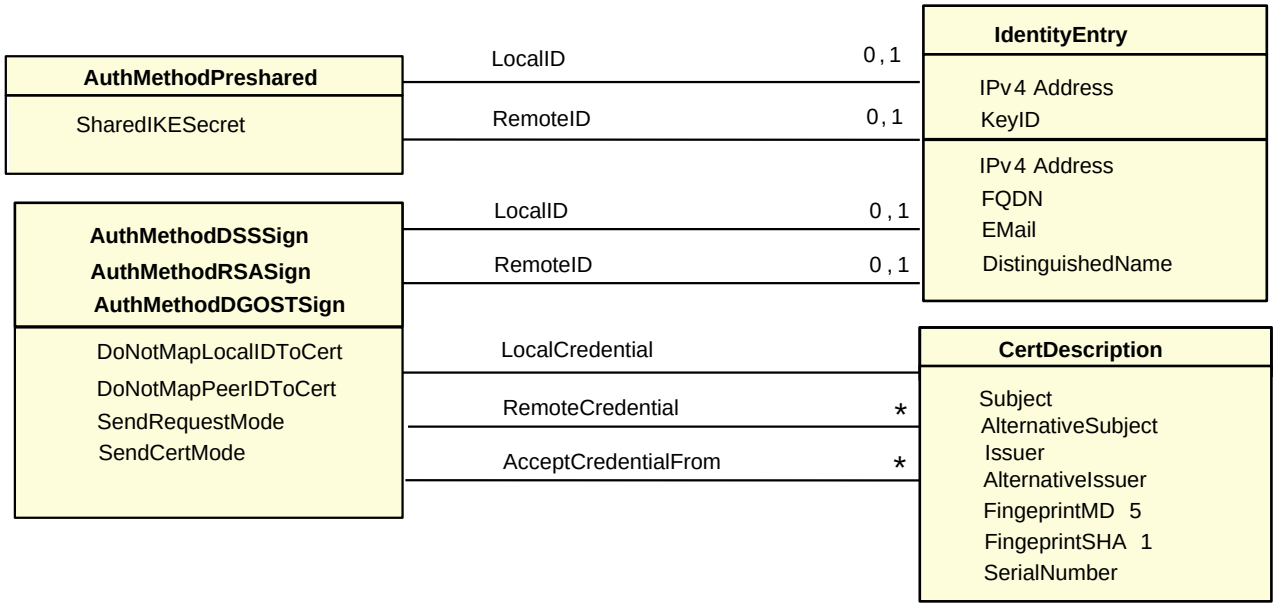


Рисунок 106

18.22. Структуры AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign

Указанная структура задает аутентификационную информацию при использовании сертификатов. Алгоритм (RSA, DSA, GOST), указанный в названии структуры, является криптографическим алгоритмом.

AuthMethodDSSSign – аутентификация DSS подписью.

AuthMethodRSASign – аутентификация RSA подписью.

AuthMethodGOSTSign – аутентификация при помощи подпис и алгоритмом ГОСТ3410-2001.

Имя структур AuthMethodDSSSign
AuthMethodRSASign
AuthMethodGOSTSign

Атрибуты LocalID
RemoteID
LocalCredential
RemoteCredential
AcceptCredentialFrom
DoNotMapLocalIDToCert
DoNotMapRemoteIDToCert
SendRequestMode
SendCertMode

Атрибут LocalID

Атрибут LocalID задает идентификационную информацию данного VPN-устройства.

Синтаксис LocalID =`IdentityEntry`

В структуре IdentityEntry допускается задание одного значения одному из идентификаторов типа `IPv4Address`, `FQDN`, `EMail`, `DistinguishedName`.

При задании значения атрибуту DistinguishedName использование в строке Subject зарезервированного слова TEMPLATE недопустимо.

При задании значения атрибуту IPv4Address использование диапазона IP-адресов недопустимо.

Если значение задано зарезервированным словом USER_SPECIFIC_DATA, то в качестве идентификатора будет использовано соответствующее значение из локального сертификата. Если в сертификате соответствующее значение отсутствует, то ISAKMP-сессия будет прервана.

Значение по умолчанию первый IP-адрес сетевого интерфейса, с которого отсылаются ISAKMP-пакеты партнеру.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут RemoteID

Атрибут RemoteID задает требования к идентификационной информации партнера.

Синтаксис RemoteID = `IdentityEntry`

В структуре IdentityEntry допускается задание нескольких идентификаторов типа `IPv4Address`, `FQDN`, `Email`, `DistinguishedName`.

Значение по умолчанию принимается любой ID партнера.

Атрибут LocalCredential

Атрибут LocalCredential задает требуемые характеристики сертификата данного VPN-устройства. В случае использования аутентификации на алгоритме ГОСТ Р 3410 локальный сертификат используется, если его секретный ключ доступен.

Синтаксис LocalCredential = `CertDescription`

Значение по умолчанию требования отсутствуют. Используется первый локальный сертификат.

Атрибут RemoteCredential

Атрибут RemoteCredential задает требуемые характеристики сертификата партнера по взаимодействию.

Синтаксис RemoteCredential* = `CertDescription`

Значение по умолчанию требования отсутствуют, допускается любой сертификат.

Атрибут AcceptCredentialFrom

Атрибут AcceptCredentialFrom задает требуемые характеристики CA-сертификата, удостоверяющего подлинность сертификата партнера.

Синтаксис AcceptCredentialFrom* = `CertDescription`

Значение по умолчанию используется любой из тех CA, которому мы доверяем.

Copyright © S-Terra CSP 2003 - 2015

Атрибут DoNotMapLocalIDToCert

Атрибут DoNotMapLocalIDToCert задает режим использования локального идентификатора при поиске локального сертификата.

Синтаксис DoNotMapLocalIDToCert = **TRUE** | **FALSE**

Значение TRUE – при поиске локального сертификата используются описания сертификатов, указанные в атрибуте LocalCredential. Значение атрибута LocalID игнорируется

FALSE - при поиске локального сертификата используется список CertDescription. Каждый элемент этого списка является объединением атрибута LocalID (используется первое значение) и CertDescription из атрибута LocalCredential. Объединение строится по следующим правилам:

если LocalID задан зарезервированным словом USER_SPECIFIC_DATA, то результирующий CertDescription совпадает с исходным CertDescription из атрибута LocalCredential

если LocalID задан типом DistingueshedName, то:

если в исходном CertDescription задано поле Subject, то множество его атрибутов должно являться подмножеством атрибутов значения LocalID. Если это условие не выполняется, то соединение не установится

результирующий CertDescription получается заменой или добавлением значения поля Subject из LocalID в исходном CertDescription

если LocalID задан типом, отличным от DistingueshedName, то:

если в исходном CertDescription задано поле такого же типа, то их значения должны совпадать. Если это не выполняется, то соединение не установится

результирующий CertDescription получается добавлением значения LocalID в исходный CertDescription.

Значение по умолчанию FALSE

Атрибут DoNotMapRemoteIDToCert

Атрибут DoNotMapRemoteIDToCert задает режим использования идентификатора партнера при поиске его сертификата.

Синтаксис DoNotMapRemoteIDToCert **= TRUE** | **FALSE**

Значение TRUE – при поиске сертификата партнера используются описания сертификатов, указанные в атрибуте RemoteCredential, значение атрибута RemoteID игнорируется

FALSE – при поиске сертификата партнера используется список CertDescription. Каждый элемент этого списка является объединением присланного идентификатора партнера и CertDescription из атрибута RemoteCredential. Правила объединения совпадают с ранее описанными правилами в атрибуте DoNotMapLocalIDToCert.

Значение по умолчанию FALSE.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут SendRequestMode

Атрибут SendRequestMode определяет логику отсылки запроса на сертификат партнера.

Синтаксис SendRequestMode = **AUTO | NEVER | ALWAYS**

Значение AUTO – запрос высылается, если возможный сертификат партнера отсутствует

NEVER – запрос не высылается

ALWAYS – запрос высылается всегда

Значение по умолчанию AUTO

Атрибут SendCertMode

Атрибут SendCertMode определяет логику отсылки локального сертифика в процессе первой фазы IKE на запрос партнера. В своем запросе партнер может и указать какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отсылается.

Синтаксис SendCertMode = **AUTO** | **NEVER** | **ALWAYS| CHAIN**

Значение AUTO – автоматически определяется, когда необходима отсылка локального сертификата партнеру:

если партнер не прислал запроса, то сертификат не отсылается

если партнер прислал запрос и соответствующий сертификат был найден, то партнеру высылается либо сертификат либо найденная цепочка сертификатов

если партнер прислал запрос и этот запрос не был удовлетворен, то сертификат не высылается.

NEVER – сертификат не высылается

ALWAYS – сертификат высылается всегда

CHAIN – сертификат высылается всегда, причем в составе с цепочкой доверительных CA:

имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

Значение по умолчанию AUTO.

 Copyright © S-Terra CSP 2003 - 2015

18.23. Структура AuthMethodPreshared

Структура AuthMethodPreshared задает аутентификационную информацию при использовании предустановленных (Preshared) ключей.

Имя структуры AuthMethodPreshared

Атрибуты LocalID

RemoteID

SharedIKESecret

Атрибут LocalID

Атрибут LocalID задает идентификационную информацию данного VPN-устройства. В структуре IdentityEntry допускается задание только одного идентификатора с одним значением.

При задании значения атрибуту `IPv4Address` использование диапазона IP-адресов недопустимо.

Использование зарезервированного слова USER_SPECIFIC_DATA недопустимо.

Синтаксис LocalID = **`IdentityEntry`**

Значение по умолчанию локальный IP-адрес из IKE-пакета.

Атрибут RemoteID

Атрибут RemoteID задает требования к идентификационной информации партнера. В структуре IdentityEntry допускается задание нескольких идентификаторов разных типов.

Синтаксис RemoteID = **`IdentityEntry`**

Значение по умолчанию принимается любой ID партнера.

Атрибут SharedIKESecret

Атрибут SharedIKESecret определяет ссылку на предустановленный секретный ключ.

В атрибуте указывается имя предустановленного (Preshared) ключа, хранимого в базе данных Продукта.

Синтаксис SharedIKESecret = СТРОКА

Значение имя предустановленного (Preshared) ключа.

Значение по умолчанию не существует, атрибут обязательный.

 Copyright © S-Terra CSP 2003 - 2015

18.24. Структура IdentityEntry

Структура IdentityEntry описывает идентификационную информацию. Варианты задания этой структуры приведены в описаниях структур **Структура AuthMethodPreshared** и **AuthMethod{DSS|RSA|GOST}Sign**.

Имя структуры IdentityEntry

Атрибуты IPv4Address – IPv4 адрес

FQDN – FQDN хоста

EMail – EMail пользователя

DistinguishedName – DN в формате X509Subject

KeyID –- Идентификатор ключа

Если структура IdentityEntry используется определенным методом аутентификации, то атрибуты, не соответствующие данному методу, игнорируются. Атрибуты, используемые для определенных методов аутентификации:

- `AuthMethodPreshared`
  - `IPv4Address`
  - `KeyID`
- `AuthMethod{DSS|RSA|GOST}Sign`
  - `IPv4Address`
  - FQDN
  - `EMail`
  - `DistinguishedName`.

Атрибут IPv4Address

Атрибут IPv4Address задает описание идентификатора по указанным IP-адресам.

Синтаксис для данного VPN устройства:

IPv4Address = IP | **USER_SPECIFIC_DATA**

для партнера:

IPv4Address* = IP|IP..IP|IP/ЦЕЛОЕ32|
USER_SPECIFIC_DATA

Значения для данного VPN устройства:

IP – один IP-адрес

для партнера:

IP – список IP-адресов

IP..IP – список диапазонов IP-адресов

IP/ЦЕЛОЕ32 – список подсетей с IP-адресом и маской

 Copyright © S-Terra CSP 2003 - 2015

Если задано значение USER_SPECIFIC_DATA, то берется первый IP-адрес из расширения **Subject Alternative Name** локального сертификата, используемого для подписи. Если IP-адрес в сертификате отсутствует, то соединение не создается.

Если заданы диапазоны IP-адресов либо подсети, то это означает, что принимается любой Identity типа IP-адрес, если значение IP, присланное партнером в таком Identity, попадает в указанный диапазон, либо подсеть.

Значение по умолчанию используются другие атрибуты.

Атрибут FQDN

Атрибут FQDN (Fully Qualified Domain Name – полностью определенное доменное имя) задает описание идентификатора хоста по указанным DNS именам.

Синтаксис FQDN* = СТРОКА | **USER_SPECIFIC_DATA**

Значения для AuthMethodPreshared – атрибут игнорируется;

для AuthMethod{DSS|RSA|GOST}Sign:

строки вида "host.domain". Шаблоны не допускаются.

если задано значение `USER_SPECIFIC_DATA`, то при проверке/отсылке Identity используется поле **DNS** расширения **Subject Alternative Name** соответствующего сертификата, используемого соответственно для проверки/формирования подписи.

Значение по умолчанию используются другие атрибуты.

Атрибут EMail

Атрибут EMail задает описание идентификатора пользователя по указанным Email-адресам.

Синтаксис Email* = СТРОКА | **USER_SPECIFIC_DATA**

Значения для AuthMethodPreshared – атрибут игнорируется

для AuthMethod{DSS|RSA|GOST}Sign:

строки вида "user@host.domain". Шаблоны не допускаются.

если задано значение USER_SPECIFIC_DATA, то при проверке/отсылке Identity используется поле **EMail** расширения **Subject Alternative Name** сертификата, используемого соответственно для проверки/формирования подписи.

Значение по умолчанию используются другие атрибуты.

Атрибут DistinguishedName

Атрибут DistinguishedName задает описание идентификатора по указанным DN (уникальное имя в формате X509Subject.).

Синтаксис DistinguishedName* = `CertDescription` | **USER_SPECIFIC_DATA**

Значения для AuthMethodPreshared – атрибут игнорируется

для AuthMethod{DSS|RSA|GOST}Sign:

в каждой структуре CertDescription допускается использовать только поле Subject

если задано значение USER_SPECIFIC_DATA, то при проверке/отсылке Identity используется полное описание раздела **Subject Name** сертификата, используемого соответственно для проверки/формирования подписи.

Значение по умолчанию используются другие атрибуты

Атрибут KeyID

Атрибут KeyID задает описание Identity по указанным идентификаторам Preshared ключей.

Синтаксис KeyID* = СТРОКА

Значение строка, содержащая шестнадцатеричное представление идентификаторов ключей.

Для AuthMethodPreshared:

рекомендуется при составлении идентификатора ключа использовать шестнадцатеричное представление только печатных символов без пробела: Именно такое ограничение существует при формировании конфигурации IOS.

шаблоны не допускаются.

Для AuthMethod{ DSS|RSA|GOST}Sign – атрибут игнорируется.

Значение по умолчанию используются другие атрибуты.

Пример

```
AuthMethodPreshared auth_key (
    RemoteID = IdentityEntry(
 IPv4Address *= 192.168.13.117, 192.168.13.118
 )
    SharedIKESecret = "cskey"
)
```

 Copyright © S-Terra CSP 2003 - 2015

18.25. Структура CertDescription

Структура CertDescription используется для задания собственного идентификатора и идентификатора партнера, для задания характеристик локального сертификата и сертификата партнера.

Для задания СТРОКИ в атрибутах этой структуры смотрите формат DN в разделе "Формат задания DistinguishedName в LSP".

Имя структуры CertDescription

Атрибуты Subject

AlternativeSubject

Issuer

AlternativeIssuer

FingerprintMD5

FingerprintSHA1

SerialNumber

Атрибут Subject

Атрибут Subject задает значение/шаблон поля Subject сертификата.

Синтаксис Subject* = **TEMPLATE | COMPLETE**, СТРОКА

Значение TEMPLATE – флаг, при котором указанная строка представляет собой незаконченное значение поля Subject сертификата.При поиске и сравнении, поле Subject сертификата должно содержать указанную строку

COMPLETE – флаг, при котором указанная строка представляет собой законченное значение поля Subject сертификата. При поиске и сравнении поле Subject сертификата должно совпадать с указанным множеством атрибутов и их значениями (с точностью до порядка указания в сертификате) в строке.

Предупреждение: DN в строке должен быть задан точно также, как он задан в сертификате: необходимо строго соблюдать количество пробелов и регистр символов.

Значение по умолчанию если задана строка, но опущен флаг TEMPLATE или COMPLETE , то по умолчанию он равен COMPLETE;

если не задана строка, то поле Subject сертификата принимает любые значения.

Пример: Допустимые варианты:

```
Subject* = TEMPLATE, "ou=eng"

Subject* = "ou=eng", TEMPLATE

Subject* = COMPLETE,
"c=RU,o=co.,ou=eng,cn=engineer"

Subject* = "c=RU, o=co, ou=eng, cn=engineer"
```

Недопустимые варианты:

```
Subject *= TEMPLATE, "ou=eng", COMPLETE

Subject *= "ou=eng", "ou=qa"
```

 Copyright © S-Terra CSP 2003 - 2015

Атрибут AlternativeSubject

Атрибут AlternativeSubject задает значение/шаблон Alternative Subject Extension сертификата.

Синтаксис AlternativeSubject = СТРОКА

Значение по умолчанию любое значение Alternative Subject Extension сертификата.

Атрибут Issuer

Атрибут Issuer задает значение/шаблон поля Issuer сертификата.

Синтаксис Issuer* = **TEMPLATE | COMPLETE**, СТРОКА

Значение TEMPLATE – флаг, при котором указанная строка представляет собой незаконченное значение поля Issuer сертификата. При поиске и сравнении, поле Issuer сертификата должно содержать указанную строку.

COMPLETE – флаг, при котором указанная строка представляет собой законченное значение поля Issuer сертификата. При поиске и сравнении, поле Issuer сертификата должно совпадать с указанным множеством атрибутов и их значениями (с точностью до порядка указания в сертификате) в строке.

Предупреждение: DN в строке должен быть задан точно также, как он задан в сертификате:
необходимо строго соблюдать количество пробелов и регистр символов.

Значение по умолчанию если задана строка, но опущен флаг TEMPLATE или COMPLETE , то по умолчанию он равен COMPLETE;

если не задана строка, то поле Issuer сертификата принимает любые значения.

Атрибут AlternativeIssuer

Атрибут AlternativeIssuer задает значение/шаблон Alternative Issuer Extension сертификата.

Синтаксис AlternativeIssuer = СТРОКА

Значение по умолчанию любое значение Alternative Issuer Extension сертификата.

 Copyright © S-Terra CSP 2003 - 2015

Атрибут FingerprintMD5

Атрибут FingerprintMD5 задает значение хеш-функции алгоритма MD5 по бинарному представлению сертификата.

Синтаксис FingerprintMD5 = СТРОКА

Значение шестнадцатеричная запись значения хэш-функции, длина строки должна быть равна 32 символам.

Значение по умолчанию любое значение хэш-функции.

Атрибут FingerprintSHA1

Атрибут FingerprintSHA1 задает значение хеш-функции алгоритма SHA1 по бинарному представлению сертификата.

Синтаксис FingerprintSHA1 = СТРОКА

Значение шестнадцатеричная запись значения хэш-функции, длина строки должна быть равна 40 символам.

Значение по умолчанию любое значение хэш-функции.

Атрибут SerialNumber

Атрибут SerialNumber задает значение серийного номера сертификата.

Синтаксис SerialNumber = СТРОКА

Значение шестнадцатеричная запись серийного номера.

Значение по умолчанию любое значение серийного номера.

Пример

```
RemoteCredential* = CertDescription(
    Issuer* = COMPLETE, " CN=S-Terra CenterCA, O=S-Terra, L=Moscow,
                          C=RU"
    Subject* = TEMPLATE, "CN=S-Terra, OU=QA"
    AlternativeSubject = "EMAIL=inform@s-terra.com,
             DNS= tester.s-terra.com, IP =10.10.10.10"
    SerialNumber =  "567A99991E1F"
)
```

 Copyright © S-Terra CSP 2003 - 2015

18.25.1. Формат задания DistinguishedName (GeneralNames) в LSP

Текстовое представление DN

Текстовое представление DistinguishedName (GeneralNames), далее просто имени, задается в соответствии с RFC2253:

```
distinguishedName = [name]; may be empty string

name  name-component *("," name-component)

name-component = attributeTypeAndValue *("+" attributeTypeAndValue)

attributeTypeAndValue = attributeType "=" attributeValue

attributeType = (ALPHA 1*keychar) / oid
keychar = ALPHA / DIGIT / "-"

oid = 1*DIGIT *("." 1*DIGIT)

attributeValue = string

string = *( stringchar / pair )
         / "#" hexstring
         / QUOTATION *( quotechar / pair ) QUOTATION; only from v2

quotechar = <any character except "\" or QUOTATION >

special = "," / "=" / "+" / "<" /  ">" / "#" / ";"

pair = "\" ( special / "\" / QUOTATION / hexpair )
stringchar =<any character except one of special, "\" or QUOTATION>

hexstring = 1*hexpair
hexpair = hexchar hexchar

hexchar = DIGIT / "A" / "B" / "C" / "D" / "E" / "F"
          / "a" / "b" / "c" / "d" / "e" / "f"

ALPHA = <any ASCII alphabetic character>;(decimal 65-90 and 97-122)
DIGIT = <any ASCII decimal digit>       ;(decimal 48-57)
QUOTATION = <the ASCII double quotation mark character '"' decimal
34>
```

Дополнения и отступления от RFC2253

В Агенте версии 3.0 имеются следующие дополнения и отступления от RFC2253:

- символ "/" является разделителем компонент имени, т.е. допустим следующий синтаксис:

  ```
  name = name-component *("/" name-component)
  ```

  - для того, чтобы использовать этот символ как значащий, его необходимо проэскейпить.
- распознаются следующие сокращения типов атрибутов (attributeType) DistinguishedName:

X.500 Attribute Type	Сокращение
countryName	C
stateName	ST
localityName	L
organizationName	O
organizationalUnitName	OU
commonName	CN
title	T
surname	SN
givenName	GN
initials	I
streetAddress	STREET
nameQualifier	NQ
generationQualifier	GQ
userid	UID
domainComponent	DC

- регистр, в котором записано сокращение, не имеет значения.

- Строковое задание GeneralNames сведено к синтаксису, описанному в RFC2253. Распознаются следующие сокращения типов атрибутов имени GeneralNames:

Тип атрибута	Сокращение
otherName	OTHERNAME
rfc822Name	EMAIL
dNSName	DNS
directoryName	DN
uniformResourceIdentifier	URI
iPAddress	IP
registeredID	RID

- регистр, в котором записано сокращение, не имеет значения

 Copyright © S-Terra CSP 2003 - 2015

- задание атрибутов `x400Address и ediPartyName` в строковом представлении не поддерживается.
- Согласно RFC2253 символы `’"’(кавычки) и ’\’(back-slash)` являются служебными. Согласно описанию Терминального символа СТРОКА, при задании любого строкового значения в LSP указанные символы так же используются как служебные. Поэтому:
  - каждая отдельно стоящая кавычка в строковом представлении должна быть дополнена слева символом `’\’` в LSP
  - каждое сочетание `’\"’` в строковом представлении должно быть дополнено слева `’\\’` в LSP.

Примеры

Имя в сертификате	Строковое представление	В LSP
`O=Sergey, Danila and company`	`O=Sergey\, Danila and company`	`Subject="O=Sergey\, Danila and company"`
`O=JSC "Horns and hoofs"`	`O=JSC \"Horns and hoofs\"`	`Subject="O=JSC \\\"Horns and hoofs\\\""`
`CN=Device#4`	`CN="Device#4"`	`Subject="CN=\"Device#4\""`

 Copyright © S-Terra CSP 2003 - 2015

18.26. Работа с сертификатами

Отсылка локального сертификата

Для отсылки локального сертификата партнеру по IKE в LSP-конфигурации необходимо:

в структуре **AuthMethodGOSTSign** задать атрибут **SendCertMode** со значением:

- ALWAYS – всегда отсылать локальный сертификат
- CHAIN – всегда отсылать локальный сертификат, CA сертификат и промежуточные CA сертификаты.

Получение сертификата партнера

Сертификат партнера можно получить либо по протоколу IKE либо по протоколу LDAP.

Сначала агент пытается получить сертификат партнера по IKE, если партнер не прислал сертификат, а прислал свой идентификатор. Агент по этому идентификатору ищет сертификат партнера сначала в своей базе Продукта, если не нашел, то продолжает поиск на LDAP-сервере.

Получение сертификата партнера по IKE

Для получения сертификата партнера по IKE в LSP-конфигурации нужно:

- в структуре **AuthMethodGOSTSign** задать атрибут **SendRequestMode** со значением ALWAYS – всегда запрашивать сертификат партнера
- в конфигурации партнера в структуре **AuthMethodGOSTSign** задать атрибут **SendCertMode** со значением:
  - ALWAYS – высылать сертификат
  - CHAIN – высылать локальный сертификат, CA сертификат с цепочкой промежуточных CA.

Получение сертификата партнера по LDAP

В этом случае партнер присылает свой идентификатор, а агент по Subject будет искать сертификат партнера на LDAP-сервере. Для прохождения LDAP-пакетов до LDAP-сервера необходимо в LSP-конфигурации задать соответвующий фильтр:

- задать структуру **LDAPSettings** с IP-адресом LDAP-сервера:
  - если прислан идентификатор типа DN:
    - агент по Subject ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере
  - если прислан идентификатор другого типа:
    - для получения Subject в локальной конфигурации задаются атрибуты **RemoteID**, **RemoteCredential**, **DoNotMapRemoteIDToCert**
      - если DoNotMapRemoteIDToCert = TRUE, то Subject будет составляться из RemoteCredential
      - если DoNotMapRemoteIDToCert = FALSE, то Subject будет составляться из RemoteCredential и RemoteID.
    - по составленному Subject агент ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере.

 Copyright © S-Terra CSP 2003 - 2015

Проверка сертификата по CRL

Для проверки сертификата партнера по CRL в LSP-конфигурации нужно:

- в структуре **GlobalParameters** задать атрибут **CRLHandlingMode**, при значениях этого атрибута:
  - `optional` – используется действующий CRL из базы Продукта
  - `enable` и `best_effort` – действующий CRL может быть получен по LDAP.

Для получения CRL с LDAP-сервера сначала проверяется поле CDP в проверяемом сертификате, если поле CDP отсутствует, то в конфигурации должна быть задана структура LDAPSettings с адресом LDAP-сервера. В базу Продукта с LDAP-сервера загружается действующий CRL и по нему проверяется сертификат партнера.

Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответвующий фильтр.

 Copyright © S-Terra CSP 2003 - 2015

18.27. Примеры локальных политик безопасности

Условные обозначения:



Сценарий 1

Пример локальной политики безопасности для клиента при удаленном доступе к подсети 10.10.12.0/24. Трафик между клиентом и шлюзом безопасности (CSP VPN Gate) защищен туннелем, работающим по протоколу ESP. Аутентификация взаимодействующих сторон осуществляется на основе сертификатов X.509.

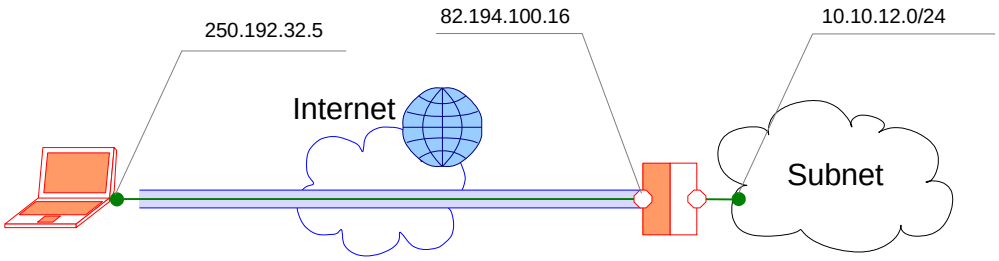


Рисунок 107

```
GlobalParameters(
 Title = "LSP for Client's remote access to Subnet"
 Version = "3.11"
)

FilteringRule Filter_client_Subnet(
 LocalIPFilter* = FilterEntry( IPAddress *= 250.192.32.5 )
 PeerIPFilter* = FilterEntry( IPAddress *= 10.10.12.0..
                                          10.10.12.255 )
 Action* = ( Client_Gate )
)

IPsecAction Client_Gate(
 TunnelingParameters* = TunnelEntry(
       LocalIPAddress = 250.192.32.5
       PeerIPAddress = 82.194.100.16
       DFHandling=COPY
 )
 ContainedProposals* = (ESP_Client_Gate)
 IKERule = IKE_Client_Gate
)
```

```
ESProposal ESP_Client_Gate(
 Transform* = ESPTransform(
       CipherAlg* = "G2814789CPRO1-K256-CBC-254"
       LifetimeSeconds = 3600
 )
)


IKERule IKE_Client_Gate(
 Transform* = IKETransform(
       CipherAlg* = "G2814789CPRO1-K256-CBC-65534"
       HashAlg* = "GR341194CPRO1-65534"
       GroupID* = MODP_768
 )
 AggrModeAuthMethod* = auth_gost
 MainModeAuthMethod* = auth_gost
 DoAutopass = TRUE
)

AuthMethodGOSTSign auth_gost(
 LocalID = IdentityEntry(
       DistinguishedName* = USER_SPECIFIC_DATA
 )
 RemoteCredential* = CertDescription(
       Issuer* =COMPLETE, "C=RU,O=S-Terra,OU=Devel,
                           CN=gate.s-terra.com"
       Subject* = TEMPLATE, "OU=Devel,CN=gate.s-terra.com"
       SerialNumber = "1234abcd"
 )
 AcceptCredentialFrom* = CertDescription(
       Issuer* = COMPLETE,"C=RU,O=S-Terra_CSP,
                           OU=Public,CN=CorporateCA"
       Subject* = TEMPLATE, "C=RU,CN=CorporateCA"
       SerialNumber = "3dda4d4a"
 )
 SendRequestMode = ALWAYS
 SendCertMode = ALWAYS
)
```

Сценарий 2

Пример локальной политики безопасности для клиента при удаленном доступе к двум подсетям 10.10.1.0/24 и 12.14.10.0/24. Трафик между клиентом и шлюзом безопасности (CSP VPN Gate) к первой подсети защищен туннелем, работающим по протоколу ESP. Трафик между клиентом и шлюзом безопасности (CSP VPN Gate) ко второй подсети защищен туннелем, работающим по протоколам AH и ESP. Аутентификация взаимодействующих сторон осуществляется на основе предустановленных ключей (Preshared Keys). На внешних интерфейсах шлюзов безопасности G1 и G2 защита снимается. Ко всем остальным ресурсам интернет клиенту разрешен открытый IP (незащищенный) трафик.

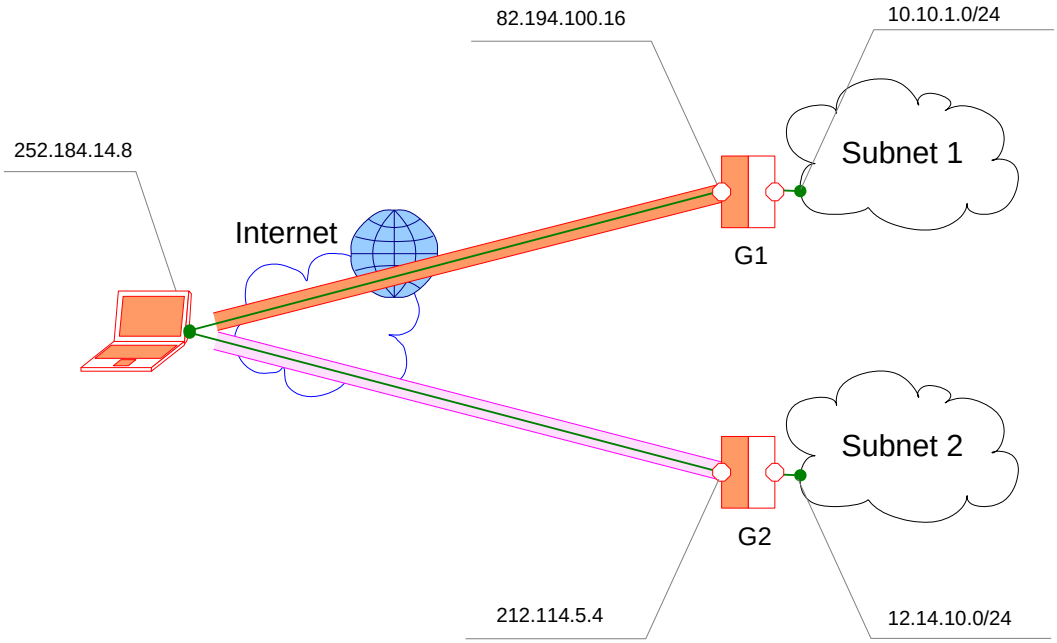


Рисунок 108

```
GlobalParameters (
 Title = "LSP for Client's remote access to Subnet1 and 2"
 Version = "3.11"
)

FilteringRule Filter_client_Subnet1(
 LocalIPFilter* = FilterEntry( IPAddress *= 252.184.14.8 )
 PeerIPFilter* = FilterEntry( IPAddress *= 10.10.1.0..
 10.10.1.255 )
 Action* = ( Client_Gate1 )
)
IPsecAction Client_Gate1(
 TunnelingParameters* = TunnelEntry(
       LocalIPAddress = 252.184.14.8
       PeerIPAddress = 82.194.100.16
       DFHandling=COPY
 )
 ContainedProposals* = (ESP_Client_Gate1)
 IKERule = IKE_Client_Gate1
)
ESPProposal ESP_Client_Gate1(
 Transform* = ESPTransform(
       IntegrityAlg* = "GR341194CPRO1-H96-HMAC-254"
       CipherAlg *="G2814789CPRO1-K256-CBC-254"
       LifetimeSeconds = 3600
```

 Copyright © S-Terra CSP 2003 - 2015

```
 )
)
IKERule IKE_Client_Gate1(
 Transform* = IKETransform(
       CipherAlg* = "G2814789CPRO1-K256-CBC-65534"
       HashAlg* = "GR341194CPRO1-65534"
       GroupID* = MODP_768
 )
 AggrModeAuthMethod* = auth_key_gate1
 MainModeAuthMethod* = auth_key_gate1
 DoAutopass = TRUE
)

AuthMethodPreshared auth_key_gate1(
 RemoteID = IdentityEntry( IPv4Address *=82.194.100.16 )
 SharedIKESecret = "key_gate1"
)

FilteringRule Filter_client_Subnet2(
 LocalIPFilter* = FilterEntry( IPAddress *= 252.184.14.8 )
 PeerIPFilter* = FilterEntry( IPAddress *= 12.14.10.0..12.14.10.255
)
 Action* = ( Client_Gate2 )
)
IPsecAction Client_Gate2(
 TunnelingParameters* = TunnelEntry(
       LocalIPAddress = 252.184.14.8
       PeerIPAddress = 212.114.5.4
       DFHandling=COPY
 )
 ContainedProposals* = (AH_Client_Gate2,ESP_Client_Gate2)
 IKERule = IKE_Client_Gate2
)
ESPProposal ESP_Client_Gate2(
 Transform* = ESPTransform(
       IntegrityAlg* = "GR341194CPRO1-H96-HMAC-254"
       CipherAlg *= "G2814789CPRO1-K256-CBC-254"
       LifetimeSeconds = 3600
 )
)
AHProposal AH_Client_Gate2(
 Transform* = AHTransform(
       IntegrityAlg* = "GR341194CPRO1-H96-HMAC-254"
       LifetimeSeconds = 3600
 )
)
IKERule IKE_Client_Gate2(
 Transform* = IKETransform(
       CipherAlg* = "G2814789CPRO1-K256-CBC-65534"
       HashAlg* = "GR341194CPRO1-65534"
       GroupID* = MODP_768
 )
 AggrModeAuthMethod* = auth_key_gate2
 MainModeAuthMethod* = auth_key_gate2
 DoAutopass = TRUE
)
AuthMethodPreshared auth_key_gate2(
 RemoteID = IdentityEntry( IPv4Address *=212.114.5.4 )
 SharedIKESecret = "key_gate2"
)
FilteringRule Pass_All(
 Action* = (PASS)
)
```

 Copyright © S-Terra CSP 2003 - 2015

Сценарий 3

Пример локальной политики безопасности для клиента при удаленном доступе к серверу 10.10.12.5 в подсети 10.10.12.0/24 по протоколу http. Трафик между клиентом и шлюзом безопасности (CSP VPN Gate) защищен туннелем, работающим по протоколу ESP.Кроме того, правила фильтрации не разрешают доступ к другим ресурсам подсети. Аутентификация взаимодействующих сторон осуществляется на основе сертификатов. На внешнем интерфейсе шлюза безопасности защита снимается.

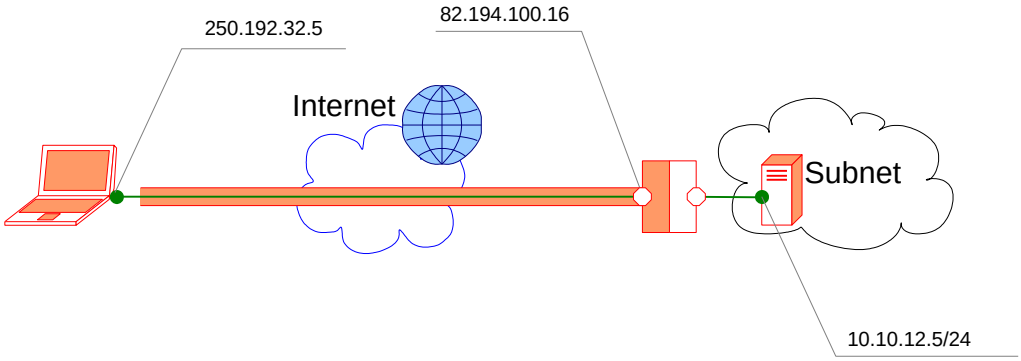


Рисунок 109

```
GlobalParameters (
 Title = "LSP for Client's remote access to Subnet to
                  Server"
 Version = "3.11"
 IKEInitiatorSessionMax=100
)

FilteringRule Filter_client_Subnet_Server(
 LocalIPFilter* = FilterEntry(
       IPAddress *= 250.192.32.5
       ProtocolID = 6
 )
 PeerIPFilter* = FilterEntry(
       IPAddress *= 10.10.12.5
       ProtocolID = 6
       Port =80
 )
 Action* = ( Client_Gate )
)

IPsecAction Client_Gate(
 TunnelingParameters* = TunnelEntry(
       LocalIPAddress = 250.192.32.5
       PeerIPAddress = 82.194.100.16
       DFHandling=COPY
 )
 ContainedProposals* = (ESP_Client_Gate)
 IKERule = IKE_Client_Gate
)

ESPProposal ESP_Client_Gate(
 Transform* = ESPTransform(
       IntegrityAlg* = "GR341194CPRO1-H96-HMAC-254"
       CipherAlg *= "G2814789CPRO1-K256-CBC-254"
       LifetimeSeconds = 3600
 )
```

 Copyright © S-Terra CSP 2003 - 2015

```
)
IKERule IKE_Client_Gate(
 Transform* = IKETransform(
 CipherAlg* = "G2814789CPRO1-K256-CBC-65534"
 HashAlg* = "GR341194CPRO1-65534"
 GroupID* = MODP_768
 LifetimeSeconds = 86400
 LifrtimeKilobytes = 4608000
 LifetimeDerivedKeys =10000
 )
 AggrModeAuthMethod* = auth_cert
 MainModeAuthMethod* = auth_cert
 DoAutopass = TRUE
)

AuthMethodGOSTSign auth_cert(
 LocalID = IdentityEntry( DistinguishedName* =
                                    USER_SPECIFIC_ДАТА
 )
 RemoteCredential* = CertDescription(
       Issuer* = COMPLETE, "C=RU,O=S-Terra,OU=QA,CN=S-Terra"
       SerialNumber =  "3dda4d4a"
       Subject* = TEMPLATE, "C=RU,O=S-Terra"
       AlternativeIssuer = "EMAIL=information@s-terra.com"
       AlternativeSubject = "IP = 82.194.100.16"
 )
 AcceptCredentialFrom* = CertDescription(
       Issuer* = COMPLETE, "C=RU,O=S-Terra,OU=Devel,
                                    CN=S-Terra_CA"
       SerialNumber =  "3dda4d4a"
       AlternativeSubject = "DNS= tester.s-terra.com"
 )
 SendRequestMode =  ALWAYS
 SendCertMode =  ALWAYS
 )
)
```

 Copyright © S-Terra CSP 2003 - 2015

19. Протоколирование событий

Настройка Syslog-клиента производится администратором при подготовке инсталляционного пакета пользователя. Администратор определяет IP-адрес хоста, на который будут посылаться сообщения о событиях, уровень важности сообщений и источник сообщений.

Настройка Syslog-клиента для протоколирования событий осуществляется в конфигурационном файле (LSP) и утилите `make_inst.exe`. В конфигурационном файле производятся текущие настройки Syslog, а в утилите `make_inst.exe` – общие настройки Syslog.

19.1. Текущие настройки

В конфигурационном файле текущие настройки для Syslog-клиента осуществляются в двух структурах. В структуре **`GlobalParameters`** устанавливаются текущие уровни важности протоколируемых событий, разделенных на четыре раздела:

- `Атрибут SystemLogMessageLevel` задает уровень важности для системных событий
- `Атрибут PolicyLogMessageLevel` задает уровень важности для событий, связанных с применением политики безопасности
- `Атрибут CertificatesLogMessageLevel` задает уровень важности для событий, связанных с сертификатами
- `Атрибут LDAPLogMessageLevel` задает уровень важности для событий, связанных с доступом к LDAP серверу.

В структуре **`SyslogSettings`** задается адрес Syslog-сервера, на который посылаются сообщения, и источник сообщений. В этой структуре можно отключить использование протокола Syslog.

19.2. Общие настройки

Задание общих настроек Syslog-клиента осуществляется в **`утилите make_inst.exe`**. В ключе `-s` задается общий уровень важности протоколируемых событий. В ключе `-t` указывается IP-адрес сервера, на который будут посылаться сообщения о протоколируемых событиях. В ключе `-y` указывается источник сообщений.

19.3. Действие текущих и общих настроек

Общие настройки вступают в действие при отсутствии загруженной локальной политики безопасности (когда действует Default Driver Policy) или отсутствии текущих настроек.

Текущие настройки отсутствуют, если в структуре **`GlobalParameters`** нет настроек для разных событий и структура **`SyslogSettings`** отсутствует.

Если заданы текущий уровень протоколирования событий и общий уровень, то протоколирование будет происходить по уровням лога, заданных для разных событий.

 Copyright © S-Terra CSP 2003 - 2015

19.4. Получение лога в Windows

Для получения лога в Windows можно использовать Продукт Kiwi Syslog Daemon (http://www.kiwisyslog.com), Tri Action Syslog Daemon и др.

19.5. Список протоколируемых событий

Каждому протоколируемому событию присваивается фиксированный идентификатор (MSG ID) и соответствующий ему уровень важности (Severity) для протокола Syslog: EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Выдаваемые сообщения и описание событий по этим сообщениям представлены в Таблица 5 – Таблица 9.

Сообщения уровня ERROR

Таблица 5

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Локальный сертификат непригоден	ERR	CERT	Searching local certificate failed. Reason: %s[12]. Subject: %s Issuer: %s SN: %s
2	Секретный ключ локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
3	Контейнер ключа локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера

[12] revoked | expired | not verified

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	Секретный ключ не соответствует локальному сертификату. Это возможно только после установки OCI	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inconsistent with the certificate где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
5	Неуспешная попытка установить соединение в качестве инициатора	ERR	POLICY	Connection request FAILED, Reason: %s[13], ip: %s, protocol: %s[14], IKERule: "%s", IPsecAction: "%s", FilteringRule: “%s”[15], Stopped at: %s[16]
6	Обнаружены некорректные данные в базе данных, связанные с LSP	ERR	POLICY	There is a bad lsp object in product db: '%{1}s', %{1}s – имя некорректного файла описания объекта в базе данных
7	Обнаружена более чем одна активная LSP в базе данных	ERR	POLICY	There are at least two active configurations in product db: '%{1}s' and '%{2}s' %{1}s – имя первого файла описания объекта в базе данных с активной LSP %{2}s – имя второго файла описания объекта в базе данных с активной LSP
8	Ошибка в записи маршрутизации	ERR	SYSTEM	Invalid route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address)

[13] Session timeout | Invalid packet | No proposal chosen | Invalid ID | Authentication failed | Process blocked by Local Policy (попытка установить соединение блокируется из-за перезагрузки LSP) | Internal error

[14] ISAKMP либо IPsec

[15] Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[16] Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
9	Ошибка при добавлении записи в таблицу маршрутизации	ERR	SYSTEM	Failed to add routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, unknown network interface, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: already exists.
10	Ошибка при удалении записи из таблицы маршрутизации	ERR	SYSTEM	Failed to delete routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway-я или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: not found.

Сообщения уровня WARNING

Таблица 6

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	В файле x509conv.ini указана неподдерживаемая кодировка	WARNING	CERT	Unsupported encoding "%{1}s" has been specified in x509conv.ini, "%{2}s" will be used %{1}s – неподдерживаемая кодировка %{2}s – кодировка, которая будет использована для соответствующего ASN.1-типа

 Copyright © S-Terra CSP 2003 - 2015

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
2	В файле x509conv.ini указан неизвестный параметр	WARNING	CERT	Unexpected parameter "%{1}s" has been specified in x509conv.ini, ignored %{1}s – имя неизвестного параметра
3	Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8	WARNING	CERT	Certificate with subject "%{1}s" has incompatible attribute value encoding. Probably, the connection won't be established. Please, configure x509conv.ini according to actual attribute encoding. %{1}s – строковое представление поля Subject сертификата
4	LDAP запрос {1} закончился неудачей. Причина: {2}	WARNING	LDAP	LDAP request failed. Reason: %{2}s[17]. Query[18]: "%{1}s".
5	Неуспешная попытка установить соединение в качестве ответчика	WARNING	POLICY	Incoming connection request FAILED, Reason: %s[19], ip: %s, protocol: %s[20], IKERule: "%s", IPsecAction: "%s"[21], FilteringRule: “%s”[22], Stopped at: %s[23]
6	Значение параметра DefaultCryptoContextsPerIPSecSA задано неверно	WARNING	POLICY	DefaultCryptoContextsPerIPSecSA in "agent.ini" is not valid (must be from 1 to 128), %{1}d will be used instead. %{1}d – значение, которое будет использовано для параметра DefaultCryptoContextsPerIPSecSA

[17] Create request failed – Не удалось сформировать корректный запрос

Failed to parse message – Ошибка разбора сообщения LDAP

Timeout

LDAP server is not responding – LDAP сервер недоступен

Request canceled – Запрос прерван (например при выгрузке конфигурации)

Unknown – Причина неизвестна

[18] Здесь и далее Query показывается в виде URL. По возможности пишется адрес LDAP-сервера (как правило во всех случаях, кроме “LDAP request ignored…”). Данный Query может отличаться от URL, указанного в сообщении о формировании LDAP-запроса (случай “CRL by URL”), если исходный URL не содержал адреса LDAP-сервера.

[19] Session timeout | Limit of %u responded sessions achieved | Invalid packet | No proposal chosen | No rule chosen | Invalid ID | Authentication failed | Internal error

[20] ISAKMP либо IPsec

[21] Если на момент вывода сообщения правило ISAKMP, либо IPsec не выбрано, то сведения о нём не выводятся

[22] Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[23] Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
7	В правиле IKERule задано несколько трансформов с различными группами. Если в качестве инициатора Агент будет использовать Aggressive Mode, то в этом случае будут высылаться только трансформы с такой же группой как у первого трансформа в правиле.	WARNING	POLICY	WARNING: IKERule '%{2}s', line %{3}d: in Aggressive Mode initiator will use %{1}s only. %{1}s – название выбранной группы, по которой будет работать Агент в качестве инициатора в Aggressive Mode. %{2}s – имя IKERule, для которого выведена эта диагностика %{3}d – строка, на которой располагается IKERule.

Сообщения уровня NOTICE

Таблица 7

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Результат LDAP запроса {1} – объекты не найдены	NOTICE	LDAP	LDAP request result: NOT FOUND. Query: "%{1}s".
2	Результат LDAP запроса {1} – найдено {2} объектов	NOTICE	LDAP	LDAP request result: %{2}s object(s) found. Query: "%{1}s".
3	Присвоен IP-адрес из удалённого IKECFG-пула	NOTICE	POLICY	VPN ip-address %s obtained, Partner: %s:%d[24]
4	Партнёру присвоен IP-адрес из IKECFG-пула	NOTICE	POLICY	VPN ip-address %s assigned to external host Partner: %s:%d[25]
5	Превышено ограничение на количество инициированных IKE-сессий. Инициированная сессия отложена до завершения любой активной инициированной IKE-сессии.	NOTICE	POLICY	[ISAKMP]: Exchange pended. Limit of %u initiated sessions achieved. Partner: %s:%d[26]
6	Превышено ограничение на количество IKE-сессий, инициированных партнерами. Запрос от партнера игнорируется, новая сессия не создается.	NOTICE	POLICY	[ISAKMP]: Exchange cancelled. Limit of %u responded sessions achieved. Partner: %s:%d[27]

[24] ip:port

[25] ip:port

[26] ip:port. Порт партнёра может указываться нулевым в случаях, когда он ещё не определен. Это возможно, поскольку ISAKMP обмен на момент вывода сообщения ещё не начат, а другие источники фактической информации о партнёре могут быть недоступны. Порт партнера в таких случаях определяется после возобновления ISAKMP обмена.

27 ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
7	Старт сервиса	NOTICE	SYSTEM	Service started, version %s
8	Остановка сервиса	NOTICE	SYSTEM	Service stopped
9	Доступ Пользователя к Агенту	NOTICE	SYSTEM	User logged in
10	Отключение доступа Пользователя к Агенту	NOTICE	SYSTEM	User logged out

Сообщения уровня INFO

Таблица 8

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Установлено соединение	INFO	POLICY	Connection established, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], FilteringRule: “%s”, IPsecAction: “%s” где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол FilteringRule: “%s” – фильтр, на который загружена созданная цепочка IPsec SA-ев IPsecAction: “%s” – правило IPsecAction по которому создалось соединение
2	Получен ISAKMP-пакет от партнера, с которым запрещен IKE-трафик[28]	INFO	POLICY	Inbound IKE packet dropped, Reason: Access denied, Partner: %s:%d[29]

[28] Партнер (идентифицируется по паре ip:port) может быть помещен в «черный список», если с ним нет ни одного ISAKMP соединения, и за определенный промежуток времени он неуспешно пытался установить ISAKMP соединение достаточно большое количество раз. При получении нового IKE-пакета от такого партнера любая обработка IKE-пакетов игнорируется, поэтому невозможно определить намерение партнера: это может быть новая попытка установления ISAKMP соединения, продолжение старых попыток, информационное сообщение, либо просто пакет неправильного формата. Обмен с таким партнером разрешается спустя установленный промежуток времени, либо при инициировании соединения со стороны локального устройства.

[29] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
3	Закрытие соединения	INFO	POLICY	Connection closed, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], bytes sent/received: %d / %d, Reason: %s где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол bytes sent/received: %d / %d – количество байт, который были отосланы и приняты под защитой этого соединения Reason: %s – причина удаления соединения, возможны следующие варианты: Loading new configuration – соединение уничтожено по причине загрузки новой конфигурации Delete payload received – от партнера пришел запрос на удаление этого соединения Time expired – истек лимит действия соединения по времени Traffic expired – истек лимит действия соединения по трафику Dead peer detected – партнер признан «мертвым» Initial contact – соединение удалено при получении нотификации INITIAL-CONTACT Cannot start DPD (no ISAKMP SA) – нет возможности инициировать DPD, партнер признается «мертвым» и соединение с ним удаляется Replaced with new one – соединение удаляется в связи с тем, что построено новое SA bundle destroyed – возникает в случае использования вложенного IPsec, когда удаляется одна из цепочек IPsec SAs, что приводит к уничтожению всей связки цепочек.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	IPsec-соединение не установилось из-за превышения количества, разрешенного лицензией	INFO	POLICY	Unable to establish connection: resources exceeded
5	Информация о лицензии Продукта	INFO	SYSTEM	Product licence: product code: %s, customer code: %s, license number: %n, license code: %s

Сообщения уровня DEBUG

Таблица 9

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Не найден сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: not found. Search template: %s
2	Найден непригодный сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: %s[30]. Subject: %s Issuer: %s SN: %s
3	Выбран сертификат партнёра	DEBUG	CERT	Use peer certificate: Subject: %s Issuer: %s SN: %s
4	Сформирован LDAP запрос {1}	DEBUG	LDAP	LDAP request: "%{1}s[31]". Где %{1}s – запрос в одном из следующих видов: “CRL by DN: <Printable_DN>” – запрос CRL производится по DN. “Certificate by DN: <Printable_DN>” – запрос сертификата производится в виде DN. “CRL by URL: <url>” – запрос CRL по URL (берется из CDP).
5	LDAP запрос {1} проигнорирован: не задан LDAP сервер	DEBUG	LDAP	LDAP request ignored: there is no LDAP server available. Query: "%{1}s".

[30] revoked | expired | not verified

[31] Во всех сообщениях LDAP запрос описывается в виде URL. В настоящее время если используются IP-адрес и порт, заданные в LSP, они в URL не указываются.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
6	Запрос на создание соединения	DEBUG	POLICY	Connection request, packet: %u.%u.%u.%u[:%u]-> %u.%u.%u.%u[:%u][, proto %u], FilteringRule: “%s” где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется FilteringRule “%s” – название фильтра, под который попал пакет
7	Ошибка инициирования создания соединения	DEBUG	POLICY	Failed to initiate connection request processing, packet: %u.%u.%u.%u[:%u]->%u.%u.%u.%u[:%u][, proto %u] где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется
8	Создание ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] established, Partner: %s:%d[32], Identity: %s, IKERule: “%”
9	Удаление ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] closed, Partner: %s:%d[33], Identity: %s, bytes sent/received: %d / %d, Exchanges passed: %d
10	Обнаружение устройства NAT	DEBUG	POLICY	NAT detected on ...[34] side, Partner: %s:%d[35]

[32] ip:port

[33] ip:port

[34] local | remote

[35] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
11	Proposals высланы партнёру	DEBUG	POLICY	(Phase I): [36] Sending IKE proposals. Rule “%s”: Auth: %s Transform #1: Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: .. (Phase II):[37] Sending IPsec proposals. Rule “%s”: Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2: Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2:
12	Партнёр прислал набор proposals	DEBUG	POLICY	(Phase I): [38] IKE proposals received. Transform #1: Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: (Phase II):[39] IPsec proposals received. Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2 Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2: Proposal #2
13	Проверка proposal для правила	DEBUG	POLICY	Check proposal #%u, Protocol %s[40], Transform #%u for Rule “%s”. Result: %s[41], attribute: %s[42]

[36] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[37] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[38] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[39] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[40] ISAKMP | AH | ESP

[41] Not matched | OK

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
14	Выбран proposal	DEBUG	POLICY	(Phase I): [43] ISAKMP proposal selected. Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s (Phase II):[44] IPsec proposal selected. Mode: %s[45], Group: %s, AH Integrity: %s, ESP Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s
15	Выбран Preshared ключ	DEBUG	POLICY	Using preshared key "%{1}s" for partner %{2}s:%{3}d, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
16	Недоступен выбранный Preshared ключ	DEBUG	POLICY	Preshared key "%{1}s" not found, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP
17	Присланный идентификатор партнера по IKE-обмену не подошел ни под одно правило ISAKMP. Предпринимается попытка идентифицировать партнера по его IP-адресу.	DEBUG	POLICY	WARNING: Unable to proceed IKE remote ID for partner %{2}s:%{3}d. Using ip-address from IKE packet instead, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
18	Не удалось подобрать правило аутентификации для данного партнера по IKE-обмену	DEBUG	POLICY	Unable to choose authentication rule for partner %{2}s:%{3}d, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
19	Информация об используемом локальном IKE-Identity	DEBUG	POLICY	[ISAKMP]: Sending identity "%s" to partner <ip:port>
20	Информация об IKE-Identity, присланным партнером	DEBUG	POLICY	[ISAKMP]: Identity "%s" is received from partner <ip:port>

[42] Authentication method | Hash | Cipher | Oakley group | Integrity | mode – только для не совпавших proposals

[43] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[44] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[45] Transport | Tunnel

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
21	Информация о сообщении (IKE-Notification), присланном партнером	DEBUG	POLICY	[ISAKMP]: Notification [%s[46]] has been received for Exchange <%u[47]>: %s[48]
22	Инициированный IKE-обмен завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Connection request FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [49] (см. Таблица 10) стек выполняемых операций (см.Таблица 11) сведения о партнере: <ip:port>, IKE-Identity [50]
23	IKE-обмен, инициированный партнером, завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Incoming connection FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [51] (см.Таблица 10) стек выполняемых операций (см.Таблица 11) сведения о партнере: <ip:port>, IKE-Identity[52]
24	Пересечение соединений по адресам от разных партнеров на одном фильтре	DEBUG	POLICY	Connection to %{1}s:%{2}d conflicts with connection to %{3}s:%{4}d, conflicting address range: %{5}s %{1}s:%{2}d – IP-адрес и порт партнера, который блокирует соединение к партнеру %{3}s:%{4}d в адресном пространстве %{5}s

[46] Согласно списку п. 3.14.1 в RFC 2408 и п. 4.6.3 в RFC 2407.

[47] Номер-идентификатор IKE-обмена.

[48] Реакция Агента на присланное сообщение: Ignore | Ignore unprotected Notification | Cancel target connection | Correct TTL for target connection | Start IPsec traffic | Target connection is already disabled | Peer is alive | Wrong sequence: Ignore | Peer is interested in my liveness: send acknowledgement | Clear all old connections

[49] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «*Unable to decode packet*», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[50] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

[51] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «Unable to decode packet», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[52] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

19.5.1. Список ошибок протокола ISAKMP

(**См**. пункты 22 и 23 Таблица 9)

Таблица 10

	Описание ошибки	Запись об ошибке в строке сообщения
1	Не удалось сформировать подпись	Unable to Form Signature
2	От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPsec-соединения на стороне партнера)	Unexpected Notification type: need CONNECTED
3	Получен компонент IKE-пакета типа 130, соответствующий компоненту для обнаружения устройства NAT, что не соответствует протоколу обмена для данного этапа	Unexpected payload found (payload type - 130, possibly NAT Discovery)
4	От партнера пришла команда дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующая протоколу обмена для данного этапа	Unexpected configuration message type
5	Потеряны внутренние данные от предыдущего пакета	Previous packet missed
6	Потеряны данные формируемого пакета	OUT packet missed
7	Потерян SA-компонент предыдущего пакета	Missing SA payload
8	Невозможно выбрать сценарий IKE-обмена для выбранного типа аутентификации	Unknown IKE-scenario for chosen Authentification method
9	Не обнаружен локальный сертификат	Local Certificate is not present
10	Не обнаружен сертификат партнера	Remote Certificate is not present
11	Не найден сертификат	Certificate not found
12	Нет доступа к публичному ключу сертификата	Cert Public Key is inaccessible
13	Не найден один из необходимых компонентов пакета	Can't find proposal
14	Потеряны данные с ключевой информацией	Encryption container missed
15	Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPsec-соединения	Bad IDcr returned
16	Потеряны данные входящего пакета	IN packet missed
17	Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPsec-соединения	Bad IDci returned

 Copyright © S-Terra CSP 2003 - 2015

	Описание ошибки	Запись об ошибке в строке сообщения
18	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать.	Invalid packet (invalid structure).

19.5.2. Список выполняемых действий по протоколу ISAKMP

(**см.** пункты 22 и 23 Таблица 9)

Таблица 11

	Описание дествия	Информация в строке сообщения
1	Шифрование сформированного IKE-пакета перед отправкой партнеру	Coding packet
2	Расшифрование IKE-пакета, присланного партнером	Decoding packet
3	Проверка предложений, на которые согласился партнер	Check replied SA
4	Проверка сертификата, присланного партнером	Check for Remote Certificate
5	Запрос локального сертификата	Check for Local Certificate
6	Проверка идентификационной информации, присланной партнером	Check incom IDs
7	Использование в качестве идентификационной информации партнера его IP-адреса	Check IDs as IP-addresses
8	Проверка используемого алгоритма хэширования	Check for Hash method
9	Синтаксический разбор пакета, присланного партнером на отдельные компоненты (payloads)	Make payload set for received packet
10	Проверка всех компонентов присланного пакета	Check received payloads
11	Проверка формируемого пакета на наличие компонентов перед отправкой партнеру. Используется только при создании пакетов Informational обменов чтобы удостовериться, что информация не была отправлена с другим пакетом.	Check for added payloads
12	Формирование подписи	Encrypt Signature
13	Выбор правила IKE согласно текущей конфигурации по идентификационной информации партнера	Choose Rule for Partner's identity
14	Создание ключевых пар текущей IKE-сессии	Generate Keys
15	Формирование ключевого материала	Generate SKEYIDs

	Описание дествия	Информация в строке сообщения
16	Выбор политики безопасности согласно текущей конфигурации на основании предложений от партнера	Compare policy
17	Формирование SPI	Set SPI
18	Проверка и принятие параметров устанавливаемого соединения, на которые согласился партнер	Accept Transform
19	Вычисление хэша для обнаружения устройства NAT	Calculate NAT Discovery payload
20	Вычисление общего ключа	Calculate Shared Key
21	Вычисление инициализационного вектора	Calculate InitVector
22	Определение метода аутентификации	Detect Authentification Method
23	Проверка локального сертификата для метода аутентификации с использованием сертификатов	Authentification uses Certificates: Check for Local Certificates
24	Проверка метода аутентификации, предложенного партнером, на соответствие текущей политике безопасности	Check Authentification Method
25	Выбор метода аутентификации	Choose Authentification Method
26	Проверка выбранной комбинации параметров устанавливаемого соединения	Get Proposal
27	Задание выбранного алгоритма шифрации для устанавливаемого соединения	Get Algorithm
28	Запрос возможных параметров устанавливаемого соединения согласно текущей конфигурации для их согласования с партнером	Get Local Policy
29	Проверка на наличие в предложении партнера параметра, устанавливающего MODP-группу	Get DH group for QM
30	Выбор используемой идентификационной информации для отправки партнеру	Get ID from Local Policy
31	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве инициатора	Get IDii from Local Policy
32	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве ответчика	Get IDir from Local Policy
33	Выбор используемой идентификационной информации для отправки партнеру при создании IPsec-соединения в качестве инициатора IKE-обмена	Get IDci from Local Policy

 Copyright © S-Terra CSP 2003 - 2015

	Описание дествия	Информация в строке сообщения
34	Выбор используемой идентификационной информации для отправки партнеру при создании IPsec-соединения в качестве ответчика IKE-обмена	Get IDcr from Local Policy
35	Инициализация ключевой информации для формирования IPsec-соединения	Initialize Encryption Container for QM
36	Формирование готового IPsec-соединения	Create contexts
37	Распознавание метода дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine IKE configuration method
38	Распознавание команды дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine ike-cfg message type
39	Распаковка параметров присланного запроса на дополнительную аутентификацию (XAuth) и формирование соответствующего графического пользовательского диалога	Analyse attributes and fill user dialog fields
40	Запуск графического пользовательского диалога дополнительной аутентификации (XAuth).	Start dialog for user extended authentication
41	Проверка наличия компонента IKE-пакета	Check payload %s[53]
42	Проверка структуры компонента IKE-пакета	Analyse payload structure %s[54]
43	Формирование компонента IKE-пакета	Form payload %s[55]
44	Заполнение блока данных указанного компонента IKE-пакета	Fill payload %s[56]
45	Проверка содержимого компонента IKE-пакета	Check %s[57]
46	Вычисление хэша – содержимого указанного компонента	Calculate %s[58]
47	Выполнение сценария инициации информационного обмена IKE согласно RFC 2409	[Informational Exchange, Initiator, Packet 1]
48	Выполнение сценария обработки пакета информационного обмена IKE согласно RFC 2409	[Informational Exchange, Responder, Packet 1]

[53] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[54] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[55] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[56] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[57] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[58] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

 Copyright © S-Terra CSP 2003 - 2015

	Описание дествия	Информация в строке сообщения
49	Выполнение шага сценария формирования 1-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packet 1]
50	Выполнение шага сценария обработки 1-го пакета IKE Main Mode согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 1,2]
51	Выполнение шага сценария начала обработки 2-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packets 2,3]
52	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Pre-Shared Key]
53	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Signature]
54	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Pre-Shared Key]
55	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Signature]
56	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Pre-Shared Key]
57	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Signature]
58	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Pre-Shared Key]
59	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Signature]
60	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Pre-Shared Key]
61	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Signature]
62	Выполнение шага сценария начала формирования 1-го пакета IKE Aggressive Mode Mode согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1]

	Описание дествия	Информация в строке сообщения
63	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Pre-Shared Key]
64	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Signature]
65	Выполнение шага сценария начала обработки 2-го пакета IKE Aggressive Mode согласно RFC 2409	[Aggressive Mode, Responder, Packets 1,2]
66	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Pre-Shared Key]
67	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Signature]
68	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Pre-Shared Key]
69	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Signature]
70	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Pre-Shared Key]
71	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Signature]
72	Выполнение шага сценария формирования 1-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 1]
73	Выполнение шага сценария обработки 1-го пакета IKE New Group Mode согласно RFC 2409 и формирование ответного пакета	[New Group Mode, Responder, Packets 1,2]
74	Выполнение шага сценария обработки 2-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 2]
75	Выполнение шага сценария формирования 1-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 1]
76	Выполнение шага сценария обработки 1-го пакета служебного обмена IKE и формирование ответного пакета	[Transaction Exchange, Responder, Packets 1,2]

	Описание дествия	Информация в строке сообщения
77	Выполнение шага сценария обработки 2-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 2]
78	Выполнение шага сценария формирования 1-го пакета IKE Quick Mode согласно RFC 2409	[Quick Mode, Initiator, Packet 1]
79	Выполнение шага сценария обработки 1-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Responder, Packets 1,2]
80	Выполнение шага сценария обработки 2-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Initiator, Packets 2,3]
81	Выполнение шага сценария обработки 3-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета (при поддержке партнером Commit Bit)	[Quick Mode, Responder, Packet 3,(4)]
82	Выполнение шага сценария обработки 4-го пакета IKE Quick Mode (при поддержке партнером Commit Bit)	[Quick Mode, Initiator, Packet 4]
83	Вычисление ключевого материала	[Make SKEYID]
84	Выбор ISAKMP либо IPsec правила	[Choose Rule]
85	Проверка присланного атрибута – компонента пакета IKE	[Check Attr]
86	Проверка присланного сертификата – компонента пакета IKE	[Check Cert]
87	Проверка присланного хэша – компонента пакета IKE	[Check HASH]
88	Проверка присланного идентификатора – компонента пакета IKE	[Check ID]
89	Проверка присланного ключа – компонента пакета IKE	[Check KE]
90	Проверка присланного NAT-детектора – компонента пакета IKE	[Check NAT-D]
91	Проверка присланного NAT Original Address – компонента пакета IKE	[Check NAT-OA]
92	Проверка присланного Nonce – компонента пакета IKE	[Check Nonce]
93	Проверка присланного сообщения – компонента пакета IKE	[Check Notif]
94	Проверка присланного запроса на сертификат – компонента пакета IKE	[Check REQ]

	Описание дествия	Информация в строке сообщения
95	Проверка присланных предложений на создание соединения – компонента пакета IKE	[Check SA]
96	Проверка присланной подписи – компонента пакета IKE	[Check SIG]
97	Проверка вендор-идентификатора – компонента пакета IKE	[Check VID]
98	Формирование атрибута – компонента пакета IKE	[Form Attr]
99	Формирование сертификата – компонента пакета IKE	[Form Cert]
100	Формирование хэша – компонента пакета IKE	[Form HASH]
101	Формирование идентификатора – компонента пакета IKE	[Form ID]
102	Формирование ключа – компонента пакета IKE	[Form KE]
103	Формирование NAT-детектора – компонента пакета IKE	[Form NAT-D]
104	Формирование NAT Original Address – компонента пакета IKE	[Form NAT-OA]
105	Формирование Nonce – компонента пакета IKE	[Form Nonce]
106	Формирование запроса на сертификат – компонента пакета IKE	[Form CertReq]
107	Формирование подписи – компонента пакета IKE	[Form SIG]
108	Формирование вендор-идентификатора – компонента пакета IKE	[Form VendorID]
109	Проверка на наличие устройства NAT	[NAT existence check]

 Copyright © S-Terra CSP 2003 - 2015

19.6. Ошибки криптографической подсистемы

Список сообщений об ошибках криптографической подсистемы, работающей в ядре ОС, при которых пользователю рекомендуется выполнить какие-либо действия, приведен в Таблица 12. При всех остальных сообщениях – обращайтесь в службу поддержки – support@s-terra.com.

Таблица 12

	Текст шаблона сообщения	Рекомендуемые пользователю действия, краткое описание
1	CP_Conf_K2U_PushPluginConf: Plugin is not properly loaded	Если есть проблемы с загрузкой LSP или прохождением трафика, обратиться в службу поддержки.
2	CP_ReOpen: bad check handle	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
3	CP_Transform: bad handle 0x%x	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
4	CPCCreateProvider failed with return code 0x%.8X!	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
5	%s: Can't get function addresses from CSP	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
6	CP_Open: can't find alg %s	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
7	Skipping unused algorithm [%s]	Не ошибка, можно игнорировать.
8	forced close: %u contexts	Не ошибка, можно игнорировать
9	drvcsp:_info()=OK	Не ошибка, можно игнорировать.
10	drvcsp: loglevel=0x1, logformat=0x39	Не ошибка, можно игнорировать.
11	drvcsp: serial= <...>	Не ошибка, можно игнорировать.

 Copyright © S-Terra CSP 2003 - 2015

20. Мониторинг

Настройка SNMP-агента производится администратором при подготовке инсталляционного пакета пользователя.

Мониторинг CSP VPN Client осуществляется по протоколу обмена SNMPv1 или SNMPv2c.

SNMP-менеджер имеет возможность запрашивать содержимое базы данных агента. Настройка SNMP-агента для выдачи статистики и база данных MIB, которую он поддерживает, описана в разделе "Выдача статистики".

SNMP-агент может посылать SNMP-менеджеру сообщение о возникшем прерывании в виде трап-сообщения. Настройка SNMP-агента для посылки трап-сообщений и список этих сообщений описаны в разделе "Trap-сообщения".

В качестве SNMP-менеджера могут быть использованы:

- программный Продукт CiscoWorks VPN Monitor, который входит в состав комплекта CiscoWorks VMS 2.2.
- бесплатная утилита NET-SNMP (http://www.net-snmp.org/), которая является простейшим SNMP-менеджером. При работе с SNMP-агентом нужно указывать версию SNMP –v 1 или – v 2c.

20.1. Выдача статистики

SNMP-менеджер инициирует запрос на значения одной или нескольких переменных, который посылает SNMP-агенту. SNMP-агент, отвечая на запрос, возвращает значения одной или нескольких переменных.

В конфигурационном файле задание настроек SNMP-агента для выдачи статистики SNMP-менеджеру осуществляется **структурой SNMPPollSettings**. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо.

База данных MIB, поддерживаемая SNMP-агентом, разделена на группы. В приведенной ниже таблице перечислены переменные из стандартной группы `system`, глобальной статистики IKE и IPsec, которые могут быть запрошены SNMP-менеджером.

Примечание 1: при принудительном перезапуске сервиса IKE-статистика сбрасывается и начинает считаться со старта Агента. IPsec-статистика считается со старта компьютера и при принудительном перезапуске сервиса не сбрасывается.

Примечание 2: в IKE-статистике при подсчете трафика учитывается только количество байт в ISAKMP-пакете. У Cisco же в IKE-статистике учитываются данные из IP-заголовка, UDP-заголовка и Ethernet-заголовка пакета.

 Copyright © S-Terra CSP 2003 - 2015

Таблица 13

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Статистика по стандартной группе System и специфичным константным значениям				
sysDescr	1.3.6.1.2.1.1.1.0	DisplayString	Текстовое описание сетевого объекта. Строка вида "CSP VPN Gate 3.11.<build>"	RFC1213-MIB
sysObjectID	1.3.6.1.2.1.1.2.0	OID	Идентификатор фирмы-производителя (внутри поддерева 1.3.6.1.4.1): 1.3.6.1.4.1.9.1.467(cisco2611XM из CISCO-PRODUCTS-MIB)	RFC1213-MIB
sysUpTime	1.3.6.1.2.1.1.3.0	TimeTicks	The time (in hundredths of a second) since the network management portion of the system was last re-initialized. Время в сотых долях секунды с момента последней загрузки системы	RFC1213-MIB
sysContact	1.3.6.1.2.1.1.4.0	DisplayString	Имя контактной персоны и способ контакта	RFC1213-MIB
sysName	1.3.6.1.2.1.1.5.0	DisplayString	Полное имя домена <hostname>.<domain-name>	RFC1213-MIB
sysLocation	1.3.6.1.2.1.1.6.0	DisplayString	Физическое местоположение агента	RFC1213-MIB
sysServices	1.3.6.1.2.1.1.7.0	int32	Значение, которое характеризует сервисы, предоставляемые узлом. Это значение есть сумма номеров уровней модели OSI в зависимоти от того, какие сервисы поддерживаются: 0x01 (физический), 0x02 (канальный), 0x04 (сетевой), 0x08 (точка-точка), 0x40 (прикладной). Например, если поддерживается IP уровень (маршрутизация) и транспортный уровень (точка-точка), то значение sysServices есть сумма 4 и 8. 78 (c2611XM)	RFC1213-MIB
chassisType	1.3.6.1.4.1.9.3.6.1.0	int32	335 (c2611XM)	OLD-CISCO-CHASSIS-MIB
cipSecMibLevel	1.3.6.1.4.1.9.9.171.1.1.1.0	int32	The level of the IPsec MIB 1	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
snmpSetSerialNo	1.3.6.1.6.3.1.1.6.1.0	int32	<An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation. Используется как значение, которое ограничивает сверху Cisco-specific значения. Фактически является неформальным обозначением конца MIB-а. Служит для предотвращения возможных коллизий при отработке GET-NEXT операций. 0	SNMPv2-MIB
ciscoImageString	1.3.6.1.4.1.9.9.25.1.1.1.2.<i>	DisplayString	<The string of this entry.> (описание таблицы – <A table provides content information describing the executing IOS image.>). Выдаются данные для агента: 1: "CW_BEGIN$-csp-vpn$" 2: "CW_IMAGE$C2600-CSP-VPN$" 3: "CW_FAMILY$C2600$" 4: "CW_FEATURE$IP\|FIREWALL 2 PLUS 3DES$" 5: "CW_VERSION$12.2(13)T5, $" 6: "CW_MEDIA$RAM$" 7: "CW_SYSDESCR$CSP VPN {Gate|Server|Client} <major>.<minor>.<build>$"" 8: "CW_MAGIC$$" 9: "CW_END$-csp-vpn$"	CISCO-IMAGE-MIB
Глобальная IKE-статистика				
cikeGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.2.1.1.0	uint32	<The number of currently active IPsec Phase-1 IKE Tunnels> Все существующие на данный момент активные ISAKMP SA.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.2.1.2.0	uint32	<The total number of previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalInOctets	1.3.6.1.4.1.9.9.171.1.2.1.3.0	uint32	<The total number of octets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество байт, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInPkts	1.3.6.1.4.1.9.9.171.1.2.1.4.0	uint32	<The total number of packets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.5.0	uint32	<The total number of packets which were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, отвергнутых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.7.0	uint32	<The total number of IPsec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве респондера.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.8.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and found to be invalid by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.9.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, которые не состоялись по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.2.1.11.0	uint32	<The total number of octets sent by all currently and previously active and IPsec Phase-1 IKE Tunnels> Количество байт, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.2.1.12.0	uint32	<The total number of packets sent by all currently and previously active and IPsec Phase-1 Tunnels> Количество ISAKMP-пакетов, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.13.0	uint32	<The total number of packets which were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов в течение всех IKE-сессий с момента старта Агента, которые были готовы к отсылке, но по каким-то причинам не были отосланы	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.15.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве инициатора.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.16.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and found to be invalid by all currently and previously active IPsec Phase-1 Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.17.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalInitTunnels	1.3.6.1.4.1.9.9.171.1.2.1.19.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated> Количество созданных ISAKMP SA в качестве инициатора (т.е. по инициативе локальной стороны).	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.20.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated and failed to activate> Количество инициированных сессий по созданию ISAKMP SA, завершившихся неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalRespTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.21.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were remotely initiated and failed to activate> Количество сессий по созданию ISAKMP SA, инициированных партнёрами, которые завершились неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalAuthFails	1.3.6.1.4.1.9.9.171.1.2.1.23.0	uint32	<The total number of authentications which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных сессий по созданию ISAKMP SA, в которых не прошла аутентификация	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalDecryptFails	1.3.6.1.4.1.9.9.171.1.2.1.24.0	uint32	<The total number of decryptions which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине ошибки расшифрования пакета.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalHashValidFails	1.3.6.1.4.1.9.9.171.1.2.1.25.0	uint32	<The total number of hash validations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных операций по проверке значения хэш-функции во всех IKE сессиях	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.2.1.26.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине отсутствия ISAKMP соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Глобальная IPsec-статистика				
cipSecGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.3.1.1.0	uint32	<The total number of currently active IPsec Phase-2 Tunnels> Количество существующих на данный момент IPsec соединений.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.3.1.2.0	uint32	<The total number of previously active IPsec Phase-2 Tunnels> Количество IPsec SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctets	1.3.6.1.4.1.9.9.171.1.3.1.3.0	uint32	<The total number of octets received by all current and previous IPsec Phase-2 Tunnels. This value is accumulated BEFORE determining whether or not the packet should be decompressed. See also cipSecGlobalInOctWraps for the number of times this counter has wrapped> Количество байт, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.5.0	uint32	<The number of times the global octets received counter (cipSecGlobalInOctets) has wrapped> Количество переполнений счетчика cipSecGlobalInOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInPkts	1.3.6.1.4.1.9.9.171.1.3.1.9.0	uint32	<The total number of packets received by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDrops	1.3.6.1.4.1.9.9.171.1.3.1.10.0	uint32	<The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing> Общее количество всех входящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения (Кроме проигнорированных по Anti-Replay).	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalInReplayDrops	1.3.6.1.4.1.9.9.171.1.3.1.11.0	uint32	<The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех входящих пакетов, отвергнутых локальным устройством посредством механизма Anti-Replay, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.13.0	uint32	<The total number of inbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных входящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecrypts	1.3.6.1.4.1.9.9.171.1.3.1.14.0	uint32	<The total number of inbound decryption's performed by all current and previous IPsec Phase-2 Tunnels> То же самое значение, что и cipSecGlobalInPkts. Общее количество входящих пакетов, которые были расшифрованы всеми IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecryptFails	1.3.6.1.4.1.9.9.171.1.3.1.15.0	uint32	<The total number of inbound decryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество входящих пакетов, которые были неудачно расшифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.3.1.16.0	uint32	<The total number of octets sent by all current and pre-vious IPsec Phase-2 Tunnels. This value is accumulated AFTER determining whether or not the packet should be compressed. See also cipSecGlobalOutOctWraps for the number of times this counter has wrapped> Количество байт, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.18.0	uint32	<The number of times the global octets sent counter (cipSecGlobalOutOctets) has wrapped> Количество переполнений счетчика cipSecGlobalOutOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.3.1.22.0	uint32	<The total number of packets sent by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutDrops	1.3.6.1.4.1.9.9.171.1.3.1.23.0	uint32	<The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех исходящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.25.0	uint32	<The total number of outbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных исходящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncrypts	1.3.6.1.4.1.9.9.171.1.3.1.26.0	uint32	<The total number of outbound encryption's performed by all current and previous IPsec Phase-2 Tunnels> Тоже самое значение, что и cipSecGlobalOutPkts. Общее количество исходящих пакетов, которые были зашифрованы всеми IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncryptFails	1.3.6.1.4.1.9.9.171.1.3.1.27.0	uint32	<The total number of outbound encryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество исходящих пакетов, которые были неудачно зашифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.3.1.29.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-2 Tunnels> Общее количество обменов, не состоявшихся по причине отсутствия IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Interfaces-статистика				
ifPhysAddress	1.3.6.1.2.1.2.2.1.6.<ifIndex>	Octet string	<The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.> MAC-адрес данного интерфейса. Индекс для данного значения берется из ipAdEntIfIndex.<ip>	RFC1213-MIB
ifIndex	1.3.6.1.2.1.2.2.1.1.<ifIndex>	int32	<A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization> ifIndex – индекс интерфейса, значение лежит в диапазоне от 1 до ifNumber (ifNumber - число сетевых интерфейсов)	RFC1213-MIB
IP - статистика				
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1.<ip>	IpAddress	<The IP address to which this entry's addressing information pertains.> Собственно сам <ip> (совпадает с индексом значения)	IP-MIB
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.<ip>	IpAddress	<The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.> Маска адреса.	IP-MIB
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.<ip>	int32	<The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.> Индексом переменной является IP-адрес устройства. Значением – индекс интерфейса (в таблице ifTable), который содержит данный адрес.	IP-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
CPU, Memory - статистика				
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 second period. This object obsoletes the busyPer object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5secRev which has the changed range of value (0..100).> Загрузка процессора за последние 5 секунд.	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 second period. This object deprecates the object cpmCPUTotal5sec and increases the value range to (0..100). This object is deprecated by cpmCPUTotalMonInterval> Загрузка процессора за последние 5 секунд. Отличается от cpmCPUTotal5sec допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4.1	uint32 (1..100)	<The overall CPU busy percentage in the last 1 minute period. This object obsoletes the avgBusy1 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal1minRev which has the changed range of value (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1minRev допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7.1	uint32 (0..100)	<The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1min допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5minRev which has the changed range of value (0..100).> Средняя загрузка процессора за последние 5 минут (в процентах).	CISCO-PROCESS-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100).> Загрузка процессора за последние 5 минут. Отличается от cpmCPUTotal5min допустимыми пределами.	CISCO-PROCESS-MIB
ciscoMemoryPoolUsed	1.3.6.1.4.1.9.9.48.1.1.1.5.1	uint32	<Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.> Рассматривается как таблица из одного элемента (с индексом 1), которая задает общее количество используемой физической памяти.	CISCO-MEMORY-POOL-MIB
ciscoMemoryPoolFree	1.3.6.1.4.1.9.9.48.1.1.1.6.1	uint32	<Indicates the number of bytes from the memory pool that are currently unused on the managed device. Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool> Общее количество свободной физической памяти.	CISCO-MEMORY-POOL-MIB

 Copyright © S-Terra CSP 2003 - 2015

20.2. Трап-сообщения

SNMP-агент посылает трап-сообщения о каких-то возникших событиях SNMP – менеджеру.

В конфигурационном файле задание настроек SNMP-агента для посылки трап - сообщений осуществляется в структурах **SNMPTrapSettings** и **TrapReceiver**. В этих структурах указывается IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

В приведенной ниже таблице перечислены реализованные трапы и переменные, которые высылаются SNMP-менеджеру, и описание трапа.

Таблица 14

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cikeSysFailure	1.3.6.1.4.1.9.9.171.2 3 1.3.6.1.4.1.9.9.171.2.0.3	cikePeerLocalAddr – адрес local peer cikePeerRemoteAddr – адрес remote peer Оба значения – табличные.	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences an internal or system capacity error.> Сигнализация о внутренней ошибке или исчерпании ресурсов при обработке IKE.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeCertCrlFailure	1.3.6.1.4.1.9.9.171.2 4 1.3.6.1.4.1.9.9.171.2.0.4	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a Certificate or a Certificate Revoke List (CRL) related error.> Ошибка, связанная с сертификатами или CRL.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeProtocolFailure	1.3.6.1.4.1.9.9.171.2 5 1.3.6.1.4.1.9.9.171.2.0.5	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a protocol related error.> Ошибка, связанная с обработкой протокола IKE: • Authentication error (в ситуациях, не попадающих под cikeCertCrlFailure) • BlackLog	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeNoSa	1.3.6.1.4.1.9.9.171.2 6 1.3.6.1.4.1.9.9.171.2.0.6	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a non-existent security association error.> Приход IKE-пакетов на несуществующий SA (Invalid cookie).	CISCO-IPSEC-FLOW-MONITOR-MIB

 Copyright © S-Terra CSP 2003 - 2015

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cipSecSetUpFailure	1.3.6.1.4.1.9.9.171.2 10 1.3.6.1.4.1.9.9.171.2.0.10	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the setup for an IPsec Phase-2 Tunnel fails.> По тем или иным причинам не удалось создать IPsec SA (при существующем IKE SA). Примечание: этот трап отсылается только при появлении ошибки во время проведения IKE-сессии и тем партнером, на котором случилась ошибка. Если создание соединения прекращено по другим причинам – остановка сервиса, перезагрузка LSP, delete payload, получение нотификации о том, что партнер по своей инициативе прекратил создание соединения, timeout и др., то локальное устройство трап не отсылает. В этом состоит отличие нашего агента от IOS, где трапы отсылаются с обоих партнеров при любой неуспешной сессии по созданию IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStart	1.3.6.1.4.1.9.9.171.7 7 1.3.6.1.4.1.9.9.171.2.0.7	cipSecTunLifeTime cipSecTunLifeSize Табличные значения.	<This notification is generated when an IPsec Phase-2 Tunnel becomes active.> Успешное создание туннеля.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStop	1.3.6.1.4.1.9.9.171.8 8 1.3.6.1.4.1.9.9.171.2.0.8	cipSecTunActiveTime Табличное значение	<This notification is generated when an IPsec Phase-2 Tunnel becomes inactive.> Уничтожение созданного туннеля (по разным причинам).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipsTooManySAs	1.3.6.1.4.1.9.10.62.2 7 1.3.6.1.4.1.9.10.62.2.0.7	cipsMaxSAs – максимальное количество IPsec SAs. Если не существует предела – 0.	<This trap is generated when a new SA is attempted to be setup while the number of currently active SAs equals the maximum configurable. The variables are: cipsMaxSAs> Отказ от создания SA по причине достигнутого максимального количества SA, указанного в лицензии. В переменной прописывается максимальное количество SA из лицензии.	CISCO-IPSEC-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
ciscoConfigManEvent	1.3.6.1.4.1.9.9.43.2 1 1.3.6.1.4.1.9.9.43.2.0.1	ccmHistoryEventCommandSource = { commandLine(1), snmp(2) } ccmHistoryEventConfigSource = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } ccmHistoryEventConfigDestination = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } Табличные значения. Индекс – целое число, начинающееся с единицы. Инкрементируется при каждой посылке трапа данного типа.	<Notification of a configuration management event as recorded in ccmHistoryEventTable.> Всегда ccmHistoryEventCommandSource=1 Несколько вариантов: 1 При вызове lsp_mgr show или cs_console show run: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=2 Примечание: аналогично реакции Cisco на команду show run 2 При успешной прогрузке LSP: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=3 Примечание: аналогично реакции Cisco на команду configure terminal. Для стартовой загрузки LSP надо задать ccmHistoryEventConfigSource = 4 3 При отгрузке LSP (по разным причинам): ccmHistoryEventConfigSource=1 ccmHistoryEventConfigDestination=3	CISCO-CONFIG-MAN-MIB

 Copyright © S-Terra CSP 2003 - 2015

21. Требования к внешним мерам безопасности

21.1. Физические меры безопасности

Помещения предприятия должны удовлетворять следующим требованиям:

- Обеспечение круглосуточной охраны корпусов предприятия;
- Обеспечение контроля внешнего периметра и внутренних помещений (видеонаблюдение);
- Обеспечение пропускного режима;
- Рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб;
- Двери должны быть прочными и оборудованы надежными механическими замками;
- Оборудование помещений системой пожарной сигнализации;
- Ведение Журнала выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника взявшего или сдавшего ключ дежурному вахтеру по зданию;
- Наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с продуктом, другой конфиденциальной информации. Для сейфа должно быть два ключа - основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат в опечатанном его личной печатью пенале в сейфе Генерального директора.

21.2. Процедурные меры безопасности

К безопасной эксплуатации продукта и обращения с СКЗИ предъявляются следующие требования:

- При приеме на работу сотрудники подписывают Обязательство о неразглашении сведений, составляющих коммерческую тайну организации
- Перечень сведений, составляющих коммерческую тайну организации, утверждается Генеральным директором;
- На предприятии должна быть разработана Инструкция по обращению с сертифицированными ФСБ/ФАПСИ шифровальными средствами (средствами криптографической защиты информации);
- Ведение Журнала учета СКЗИ, тестовых ключей на предприятии;
- Ведение Журнала учета обращения эталонных CD дисков на предприятии.

 Copyright © S-Terra CSP 2003 - 2015

21.3. Технические меры безопасности

К техническим мерам безопасности предъявляются следующие требования:

- Доступ к персональным компьютерам и средствам вычислительной техники осуществляется на основе логического имени и пароля пользователя в рамках операционных систем;
- Создание инсталляционного пакета для каждого пользователя и управление политикой безопасности пользователя осуществляется только администратором в соответствии с политикой безопасности предприятия;
- Администратор должен быть аутентифицирован и идентифицирован перед доступом к продукту с целью администрирования. Аутентификация осуществляется на основе пароля, вводимого с клавиатуры, не отображаясь на экране монитора, и выполняется операционной системой;
- Доставка контейнера с криптографическим ключом сертификата пользователя осуществляется только по доверенному каналу связи;
- Для защиты персонального компьютера с установленным продуктом от несанкционированного доступа администратору необходимо организовать систему протоколирования и аудита, и вести регулярный анализ результатов аудита с целью выявления нарушений несанкционированного доступа к ПК;
- Продукт должен инсталлироваться на ПК, работающий под управлением операционных систем, которые указаны в разделе «Требования на базовые платформы и совместимость»;
- На ПК с установленным продуктом должна быть установлена антивирусная программа для периодического тестирования ПК на отсутствие вирусов;
- Для операционной системы администратор должен периодически устанавливать штатные обновления. (патчи);
- Администратор должен периодически проверять целостность исполняемого кода Продукта и его политики безопасности.

 Copyright © S-Terra CSP 2003 - 2015

22. Приложение

Утилита make inst.exe

Сообщения об ошибках утилиты make inst

Установка СКЗИ "КриптоПро CSP 3.6/3.6R2"

Настройка СКЗИ "КриптоПро CSP"

Подключение внешних ключевых считывателей

Создание сертификата пользователя в "КриптоПро CSP 3.6/3.6R2"

- Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2"
- Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6/3.6R2"
- Установка и настройка Удостоверяющего Центра. Создание СА сертификата
- Создание ключевой пары и формирование запроса на сертификат пользователя
- Экспортирование сертификата пользователя в файл

 Copyright © S-Terra CSP 2003 - 2015

22.1. Утилита make_inst.exe

Вызов утилиты `make_inst.exe` должен происходить из каталога административного пакета. В противном случае будет выдано сообщение об ошибке. Утилита имеет обязательные опции и необязательные, которые заключены в квадратные скобки.

make_inst.exe `-o SFX_file_path -l LSP_file_path`

при использовании Preshared_Key указываются опции:

```
-kn Preshared_key_name
{-kv Preshared_key_val | -kvf file_path_Preshared_key_val}
```

при использовании сертификата указываются опции:

```
-c CA_file_path
-u USER_cert_file_path
-uc USER_cert_container_name
[-p PARTNER_cert_1_file_path [-p PARTNER_cert_2_file_path] ...]
[-skt {signature | exchange}]
[-up USER_cert_container_password] |
[-ufp file_path_USER_cert_container_password]
```

при копировании контейнера во время инсталляции на компьютере пользователя указываются опции:

```
[-cs Source_USER_cert_container_name]
[-cp Source_USER_cert_container_password] |
[-cfp file_path_Source_USER_cert_container_password]
```

при проверке соответствия сертификата и секретного ключа указываются опции:

```
[-chksecret {on | off}] (default: off)
[-uac USER_cert_container_name_ADMIN]
{[-uap USER_cert_container_password_ADMIN]|
[-uafp file_path_USER_cert_container_password_ADMIN]}
```

локальные настройки:

```
[-q {basic | normal | silent}] (default: basic)
[-d {passall | passdhcp}] (default: passall)
[-f {ddp | dropall}] (default: ddp)
[-s {emerg |alert |crit |err |warning |notice |info |debug}]
(default: notice)
[-t <SYSLOG_server_IP>] (default: 127.0.0.1)
[-y <log_facility>] (default: log_local7)
[-a "<Additional_cmd_msiexec_params>"]
[-lic <license_file_path>]
[-nilogin {on | off}] (default: off)
```

где:

-o SFX_file_path
`SFX_file_path` - имя создаваемого инсталляционного SFX-файла. Обязательная опция. Имя файла подразумевает и путь к этому файлу.
-l LSP_file_path
`LSP_file_path` - имя файла, содержащего LSP. Имеет текстовый формат. Обязательная опция.

 Copyright © S-Terra CSP 2003 - 2015

-kn Preshared_key_name
Preshared_key_name - имя предустановленного ключа. Обязательная опция, если используются Preshared ключи. Может быть задано несколько таких ключей (см. Примечание 2). Preshared ключи или сертификаты обязательно должны быть заданы. Можно задавать и то, и другое.
-kv Preshared_key_val
Preshared_key_val - Preshared ключ. Например, -kv 12345 или - kv "Test preshared key". (кавычки в ключ не входят). Может быть задано несколько таких ключей (см. Примечание 2).
-kvf file_path_Preshared_key_val
file_path_Preshared_key_val - имя файла, содержащего Preshared ключ на компьютере администратора. Если используется Preshared ключ, то обязательно должна быть задана опция -kv либо -kvf. Может быть задано несколько таких ключей (см. Примечание 2).
-c CA_file_path
CA_file_path - имя файла с CA-сертификатом на компьютере администратора. Обязательная опция, если используются сертификаты.
-u USER_cert_file_path
USER_cert_file_path - имя файла с локальным сертификатом пользователя на компьютере администратора. Обязательный параметр, если используются сертификаты.
-uc USER_cert_container_name
USER_cert_container_name - имя контейнера с секретным ключом на компьютере пользователя. Здесь же указывается и носитель информации, на котором хранится контейнер. Не больше 60 символов. Обязательная опция, если используются сертификаты. Например, "REGISTRY\\container" (См. Примечание 3 об именах контейнеров).
-p PARTNER_cert_i_file_path
PARTNER_cert_i_file_path – путь к сертификату партнера или промежуточному CA-сертификату, который будет положен в базу локальных настроек продукта при инсталляции. Можно задавать несколько таких опций (в базу сертификаты будут положены в порядке перечисления данных опций). Необязательный параметр. Рекомендуется использовать в случаях, когда присутствуют проблемы с передачей сертификатов по протоколу IKE и LDAP.
-up USER_cert_container_password
USER_cert_container_password - пароль к контейнеру. Не больше 40 символов. Параметр актуален, если не задана опция -ufp. Различается ситуация, когда отсутствует пароль (опция не задана) и когда пароль пустой (задано -up "").

 Copyright © S-Terra CSP 2003 - 2015

-ufp file_path_USER_cert_container_password

file_path_USER_cert_container_password - имя файла на компьютере администратора, содержащего пароль к контейнеру. Не больше 40 символов. Пароль читается из файла как текстовая строка. Если файл содержит несколько строк, то читается только первая строка (воспринимается как пароль).

-chksecret {on | off}

включение/выключение проверки соответствия сертификата пользователя и секретного ключа. По умолчанию – значение off. Такая проверка осуществляется на компьютере администратора и возможна только при наличии на нем контейнера с секретным ключом. Для проведения проверки указываются опции uac, uafp.

-uac USER_cert_container_name_ADMIN

USER_cert_container_name_ADMIN - имя контейнера на компьютере администратора. Эта опция используется только при включенной опции -chksecret. После проверки происходит импортирование секретного ключа из контейнера с данным именем в инсталляционный файл.

-uap USER_cert_container_password_ADMIN

USER_cert_container_password_ADMIN - пароль к контейнеру, указанному в опции -uac.

-uafp file_path_USER_cert_container_password_ADMIN

file_path_USER_cert_container_password_ADMIN - имя файла на компьютере администратора, в котором записан пароль к контейнеру, указанному в опции -uac.

-skt { exchange | signature }

задание типа секретного ключа. Данная опция игнорируется, если задана опция -chksecret on: в этом случае тип секретного ключа берется из проверяемого контейнера. Если создание ключевой пары и запроса на сертификат пользователя производились средствами MSCA и был выбран тип ключа both или exchange, то в этой опции нужно установить параметр exchange. Если же был выбран тип ключа signature, то и в этой опции нужно установить параметр signature. По умолчанию – значение signature.

Эта опция указывается, если на компьютере пользователя происходит копирование контейнера. Но задавать тип секретного ключа необязательно, так как при его отсутствии будут последовательно перебираться все типы ключей при копировании контейнера. См. подробно в разделе "Копирование контейнера при инсталляции".

-cs Source_USER_cert_container_name

при указании этой опции при инсталляции на компьютере пользователя будет производиться копирование контейнера с именем Source_container_name, размещенного на компьютере пользователя (например, дискете), в контейнер с именем USER_cert_container_name, которое указано в опции -uc. Опция -cs задается, если используется сертификат. Если опция не задана, то копирование контейнера не производится. Копирование контейнера с точки зрения пользователя описанов разделе "Копирование контейнера при инсталляции"

 Copyright © S-Terra CSP 2003 - 2015

-cp Source_USER_cert_container_password

Source_USER_cert_container_password - пароль к контейнеру с именем, указанным в опции
-cs, который будет копироваться при инсталляции. Если пароль отсутствует или пустой, то опция -cp не задается. По умолчанию – пароль пустой.

-cfp file_path_Source_USER_cert_container_password

file_path_Source_USER_cert_container_password – имя файла, в котором записан пароль к контейнеру, указанному в опции -cs.

-q {basic | normal | silent}

тип инсталляции:

- basic – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию.
- normal – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензии и другими окнами.
- silent – неинтерактивная установка без запросов. Стартует сразу после запуска EXE-файла без дополнительных запросов.

-d {passall | passdhcp}

Default Driver Policy:

- passall. – пропускать все. Вариант по умолчанию
- passdhcp – ничего не пропускать, кроме DHCP.

-f {ddp | dropall}

Logoff policy:

- ddp - Default Driver Policy. Вариант по умолчанию
- dropall – ничего не пропускать.

-s log_severity

log_severity ={EMERG|ALERT|CRIT|ERR|WARNING|NOTICE|INFO|DEBUG}

По умолчанию – NOTICE. Опция задает общий уровень важности протоколируемых событий, ее использование описано в главе "Протоколирование событий".

-t SYSLOG_server_IP

SYSLOG_server_IP - IP-адрес SYSLOG сервера, на который будут посылаться сообщения о протоколируемых событиях. По умолчанию – 127.0.0.1 (сообщения будут присылаться на локальный хост).

-y log_facility

log_facility =log_local 0-7. По умолчанию -log_local7.

 Copyright © S-Terra CSP 2003 - 2015

-a "Additional_cmd_msiexec_params"

"Additional_cmd_msiexec_params"- дополнительные параметры запуска WinInstaller. Например, альтернативная инсталляционная директория, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

Например, для протоколирования сообщений в файл C:\log_client1.txt при инсталляции CSP VPN Client нужно выставить опцию `-a /l* C:\log_client1.txt /i`.

Эту опцию рекомендуется указать, если выбирается тип инсталляции `silent`.

Можно указать время инициализации VPN сервиса (vpnsvc) для CSP VPN Client - указывается параметр `MAX_SERVICE_START_TIMEOUT` и его значение, например, `MAX_SERVICE_START_TIMEOUT=45`. Значение по умолчанию для этого параметра равно 30 секундам, максимальное значение – 600 секунд.

-lic license_file_path

`License_file_path` –- имя файла с Лицензией на CSP VPN Client на компьютере администратора. Эта опция обязательна для режимов инсталляции `basic` и `silent`. Для режима `normal` эта опция необязательна:

- если ее задать, то при установке Продукта вопросы о Лицензии задаваться не будут
- если ее не задать, то при установке Продукта появится стандартное окно для ввода Лицензии.

В текстовом файле данные Лицензии должны быть записаны в виде:

```
[license]
CustomerCode=NNNN
ProductCode=CLIENT
LicenseNumber=NNNN
LicenseCode=NNNNNNN
```

-nilogin {on | off}

Опция неинтерактивного режима логина пользователя:

- `on` – включен неинтерактивный режим логина
- `off` – выключен неинтерактивный режим логина, работает интерактивный режим.

При неинтерактивном режиме логина при входе пользователя в систему производится попытка логина пользователя в Продукт с пустым паролем (в качестве пароля используется пустая строка). При таком успешном логине в Продукт окно с запросом пароля не выводится. При неуспешном логине - Продукт ведет себя как при интерактивном логине (будет выдано окно запроса пароля).

Примечание 2:

Если задается несколько предустановленных ключей, то опции с именем ключа и самим ключом `(-kn и -kv или -kvf)` должны следовать одна за другой, т.е. опции `-kn и -kv (-kvf)`, расположенные рядом относятся к одному и тому же предустановленному ключу.

Пример: `-kn key1 -kv value1 -kn key2 -kvf file_with_value2`.
Пример неправильного задания ключей (два имени и два значения расположены подряд):
`-kn key1 -kn key2 -kv value1 -kvf value2` – НЕПРАВИЛЬНО!!!

 Copyright © S-Terra CSP 2003 - 2015

Примечание 3:

Имя контейнера имеет следующий формат

`\\.\READER\CONTAINER` или `READER\\CONTAINER` или `MEDIA\CONTAINER`,

где

`READER` – название считывателя ключевой информации

`MEDIA` – носитель ключевой информации

`CONTAINER` - имя контейнера.

Например:

`\\.\REGISTRY\cont_1 или REGISTRY\\cont_2` (для реестра)

`\\.\FAT12_A\cont_3` или `FAT12\cont_4` (для дискеты)

`SCARD\ETOKEN_PRO32_4f22aa14\CC03\0FDA` (для eToken)

Если контейнер находится на внешнем ключевом носителе, то для подключения и инсталляции ключевых считывателей смотрите в Приложении разделы "Подключение внешних ключевых считывателей", "Инсталляция внешнего считывателя и ключевого носителя информации в “КриптоПро CSP 3.6/3.6R2".

.А для указания уникального имени контейнера воспользуйтесь графическим интерфейсом и Примечанием 1.

 Copyright © S-Terra CSP 2003 - 2015

22.2. Сообщения об ошибках утилиты make_inst.exe

	Сообщение	Пояснение
1	Error: SFX file path is missing	Не задан путь к SFX-файлу
2	Error: CA file path is missing	Не задан путь к CA-сертификату
3	Error: Local certificate file path is missing	Не задан путь к локальному сертификату
4	Error: Container name is missing	Не задано имя контейнера
5	Error: LSP file path is missing	Не задан путь к LSP
6	Error: Container name too long	Имя контейнера слишком длинное
7	Error: Container password too long	Пароль контейнера слишком длинный
8	Error: Wrong install type	Неправильно задан тип инсталляции
9	Error: Wrong Default Driver Policy	Неправильно задана DDP
10	Error: Wrong Logoff Policy	Неправильно задано Logoff policy
11	Error: Wrong Log Severity	Неправильно задана Log Severity
12	Error: Wrong parameter: "…"	Неподдерживаемый параметр
13	Error: temporary directory creation failed	Не удалось создать временную директорию для работы утилиты
14	Error: Key creation failed	Не удалось создать описание контейнера ключа (наиболее вероятная причина – не удалось прочитать файл с паролем).
15	Error: installer files copy failed	Не удалось скопировать файлы инсталлятора
16	Error: CA not found	Не удалось найти файл с CA сертификатом
17	Error: Local certificate not found	Не удалось найти файл с локальным сертификатом
18	Error: LSP not found	Не удалось найти файл с LSP
19	Error: User preferences write failed	Не удалось создать пользовательские настройки
20	Error: Log settings write failed	Не удалось создать настройки лога
21	Error: SFX archive creation failed	Не удалось сформировать SFX-архив
22	Error: Preshared key value not found	Не удалось найти файл со значением Preshared ключа
23	Error: Source container is not applicable	Попытка задать исходный контейнер, когда не используются сертификаты

 Copyright © S-Terra CSP 2003 - 2015

	Сообщение	Пояснение
24	Error: Partner certificate is not applicable	Партнерский сертификат неприменим (попытка задать опцию –p при отсутствии других опций, связанных с сертификатами)
25	Error: Source and destination containers have the same name	Исходный и рабочий контейнеры имеют одинаковые имена, что не допустимо
26	Error: Certificates or Preshared key should be set	Сертификаты или Preshared ключ должны быть заданы
27	Error: Preshared key name is missing	Не задано имя Preshared ключа
28	Error: Preshared key value is missing	Не задано значение Preshared ключа
29	Error: Preshared key name or value missed	Не задано имя или значение Preshared ключа
30	Error: Preshared key names should be different	Имена Preshared ключей должны различаться
31	Error: Cannot initialize package settings	Не удается инициализировать настройки инсталляционного пакета
32	Error: License should be set for non-interactive installation	Лицензия должна быть задана для неинтерактивной инсталляции
33	Error: Product incorrectly installed or damaged	Продукт некорректно установлен или поврежден
34	Error: Container name on the administrator computer is missing	Отсутствует контейнер на администраторской машине
35	Error: Secret key type should not be set due to secret key check	Тип секретного ключа не должен выставляться, если задана проверка секретного ключа
36	Error: Container password reading from file failed	Не удалось прочитать из файла пароль на контейнер
37	Error: Source container password reading from file failed	Не удалось прочитать из файла пароль на исходный контейнер
38	Error: Container on administrator computer password reading from file failed	Не удалось прочитать из файла пароль на контейнер на машине администратора
39	Error: Secret key password reading from file failed	Не удалось прочитать из файла пароль на секретный ключ
40	Error: Cannot create SFX "<SFX_path>". Error code: <Error_code>[(<Error_description>)]	Не удалось создать SFX-архив по пути <SFX_path>. Номер системной ошибки: <Error_code>. Описание ошибки: <Error_description> (может отсутствовать). См. Примечание.
41	Error: File “<File_Path>” open failed. Error code: <Error_code>[(<Error_description>)]	Не удалось открыть файл по пути <File_path>. Номер системной ошибки: <Error_code>. Описание ошибки: <Error_description> (может отсутствовать). См. Примечание.

 Copyright © S-Terra CSP 2003 - 2015

	Сообщение	Пояснение
42	Error: File archiving failed	Произошла ошибка при упаковке файлов.
43	Error: Partner certificate '<file_path>' load failed	Не удалось загрузить партнерский сертификат <file_path> (наиболее вероятная причина – отсутствие или неправильный формат файла, заданного в опции –p)
44	Error: Partner certificate processing failed	Не удалось обработать партнерский сертификат

Примечание:

В сообщениях, в которых фигурируют номер и описание системной ошибки, существуют особенности:

номер системной ошибки – стандартный номер ошибки Windows.

не для всех системных ошибок существуют текстовые описания, поэтому часть с описанием ошибки может отсутствовать.

описание ошибки выводится языком, стандартным для текущего пользователя. Вывод осуществляется в кодировке ANSI.

Это удобно для вывода, перенаправленного в файл или обрабатываемого GUI-программой.

Однако это может вызвать проблемы при работе из окна командной строки, поскольку там по умолчанию используется OEM-кодировка. Соответственно сообщение об ошибке в окне командной строки может оказаться нечитаемым. Исправить данную ситуацию можно одним из следующих способов:

- использовать перенаправление вывода в файл.
- изменить текущую кодовую страницу для окна командной строки:
  - открыть окно командной строки, использующее шрифты True Type (по умолчанию используются точечные шрифты, для которых описываемый метод неприменим). На практике, как правило, в подобных ситуациях используется шрифт Lucida Console.
  - вызвать команду chcp, в качестве аргумента которой прописать номер кодировки ANSI для используемого языка. Например в случае русского языка надо задать команду:
  - `chcp` 1251
  - после этого в текущем окне командной строки сообщения об ошибке утилиты make_inst будут показываться в читаемом виде.

22.3. Установка СКЗИ "КриптоПро CSP 3.6/3.6R2"

При выполнении процедуры инсталляции СКЗИ "КриптоПро CSP 3.6/3.6R2" выбирайте:

вид установки – Выборочная

компоненты, которые необходимо установить:

Криптопровайдер уровня ядра ОС.

22.4. Настройка СКЗИ "КриптоПро CSP"

В случае использования в Продукте CSP VPN Client аутентификации пользователей на основе сертификатов, необходимо провести некоторые настройки в СКЗИ "КриптоПро CSP".

Для хранения секретного ключа сертификата пользователя используется контейнер, который может быть защищен паролем. Контейнер размещается:

- либо на внешнем ключевом носителе, который должен находиться только у пользователя
- либо на локальном ключевом носителе (Реестр) на компьютере пользователя.

СКЗИ "КриптоПро CSP" умеет считывать секретный ключ из контейнера как на внешнем ключевом носителе так и на локальном ключевом носителе.

Также настраивается и ДСЧ – выбирается биологический или аппаратный ДСЧ, описан в разделе «Настройка ДСЧ».

22.4.1. Локальный ключевой считыватель

Если контейнер с секретным ключом сертификата пользователя надо разместить в Реестре, то его нужно инсталлировать как считыватель. Такая инсталляция описана в Приложении в разделе “Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2".

22.4.2. Внешний ключевой считыватель и носитель информации

Если контейнер будет расположен на внешнем ключевом носителе, то сначала нужно подключить к компьютеру считыватель ключевой информации, а затем инсталлировать его. Подключение внешних считывателей ключевой информации описано в разделе "Подключение внешних ключевых считывателей".

После установки "КриптоПро CSP 3.6/3.6R2" сразу же инсталлированы – Все считыватели смарт-карт и Все съемные диски, а остальные считыватели нужно инсталлировать. Для eToken и дисковода инсталляция считывателя уже выполнена.

Для некоторых внешних считывателей еще нужно выполнить Инсталляцию носителей. После установки "КриптоПро CSP 3.6/3.6R2" сразу же инсталлированы несколько типов носителей для eToken, остальные носители информации требуют инсталляции.

Процедура инсталляции внешних считывателей и носителей описана в разделе “Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6/3.6R2".

 Copyright © S-Terra CSP 2003 - 2015

22.5. Подключение внешних ключевых считывателей

Подключите внешний ключевой считыватель к компьютеру, следуя прилагаемой инструкции (Не следует подключать eToken до установки драйверов).

Установите все необходимые файлы и драйверы для работы внешнего считывателя, прилагаемые к нему.

В состав дистрибутива СКЗИ "КриптоПро CSP 3.6/3.6R2" не входят драйвера, обеспечивающие взаимодействие внешних ключевых считывателей с "КриптоПро CSP 3.6/3.6R2".

Для этого с Web-страницы http://www.cryptopro.ru/cryptopro/products/csp/readers.htm компании Крипто-ПРО загрузите и установите модуль поддержки внешнего считывателя для СКЗИ "КриптоПро CSP".

 Copyright © S-Terra CSP 2003 - 2015

22.6. Создание сертификата пользователя в “КриптоПро CSP 3.6/3.6R2”

22.6.1. Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2"

Для инсталляции локального ключевого считывателя Реестр надо выполнить следующие действия:

Шаг 1: запустите КриптоПро CSP: Пуск –Настройка – Панель управления – КриптоПро CSP.

В ОС Windows 7 в появившемся окне КриптоПро CSP во вкладке **Общие** выберите предложение «Запустить с правами администратора»

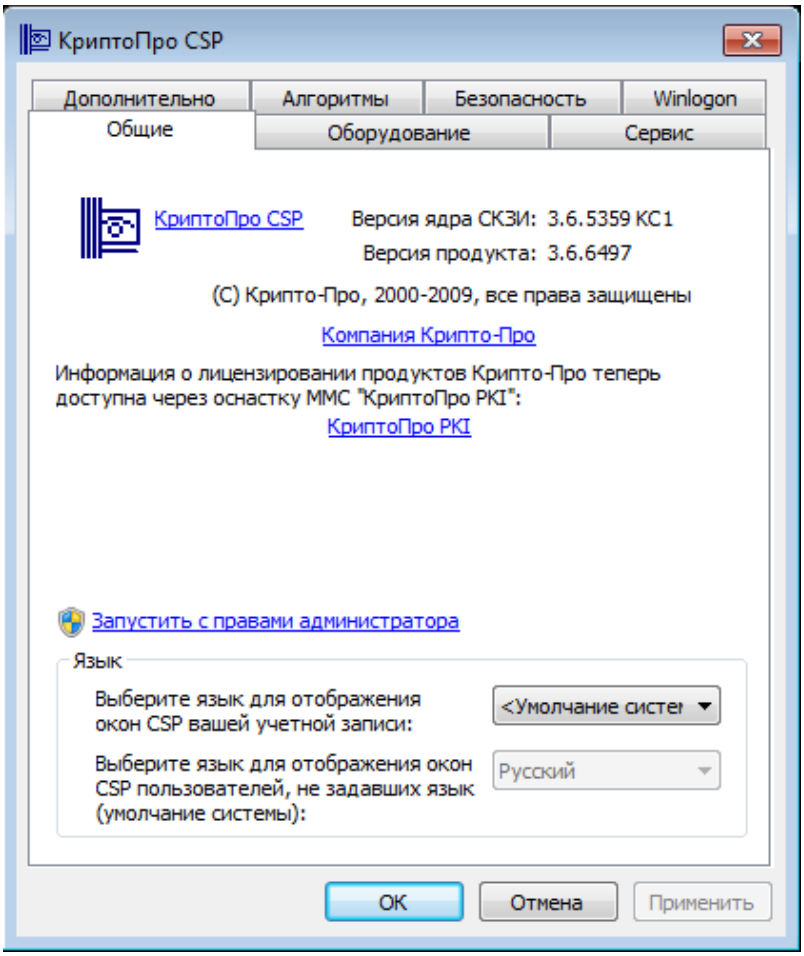


Рисунок 110

Шаг 2: в появившемся окне Свойства войдите во вкладку **Оборудование** и нажмите кнопку Настроить считыватели...:

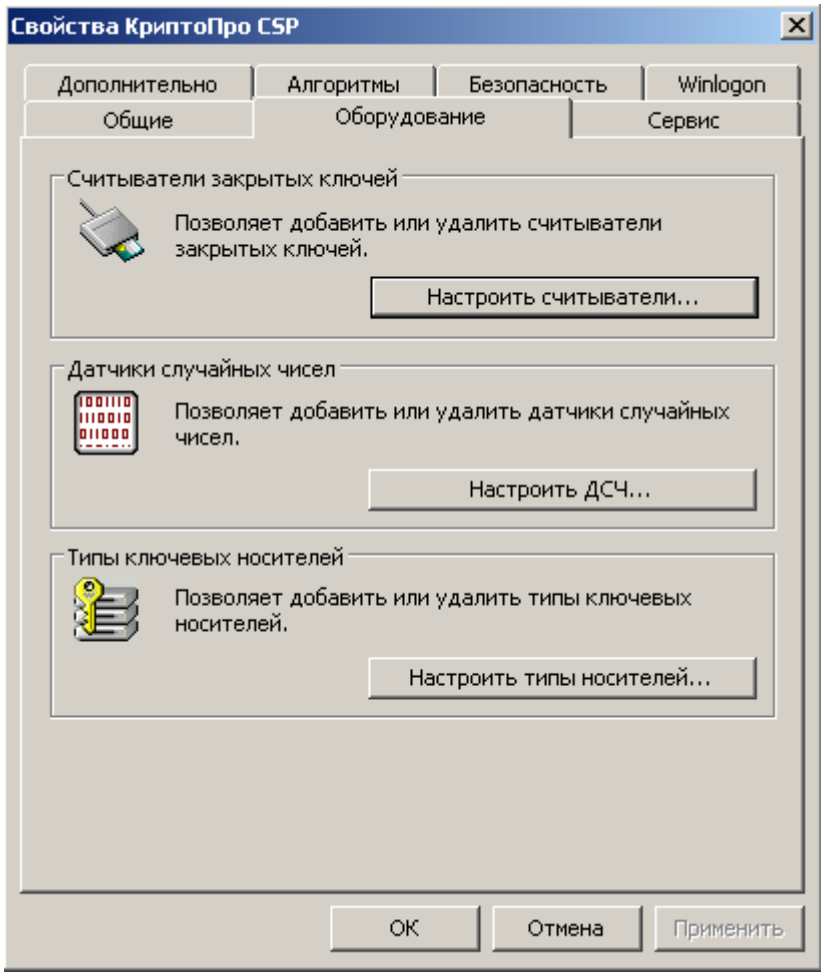


Рисунок 111

 Copyright © S-Terra CSP 2003 - 2015

Шаг 3: нажмите кнопку `Добавить...`, чтобы добавить новый ключевой считыватель:

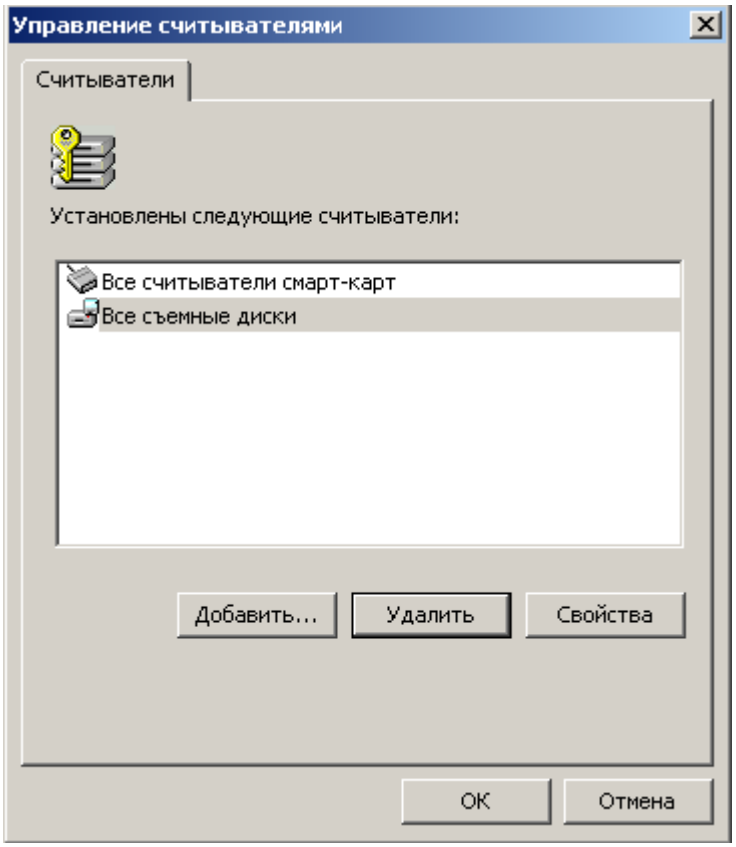


Рисунок 112

Шаг 4: в окне визарда нажмите кнопку `Далее`:

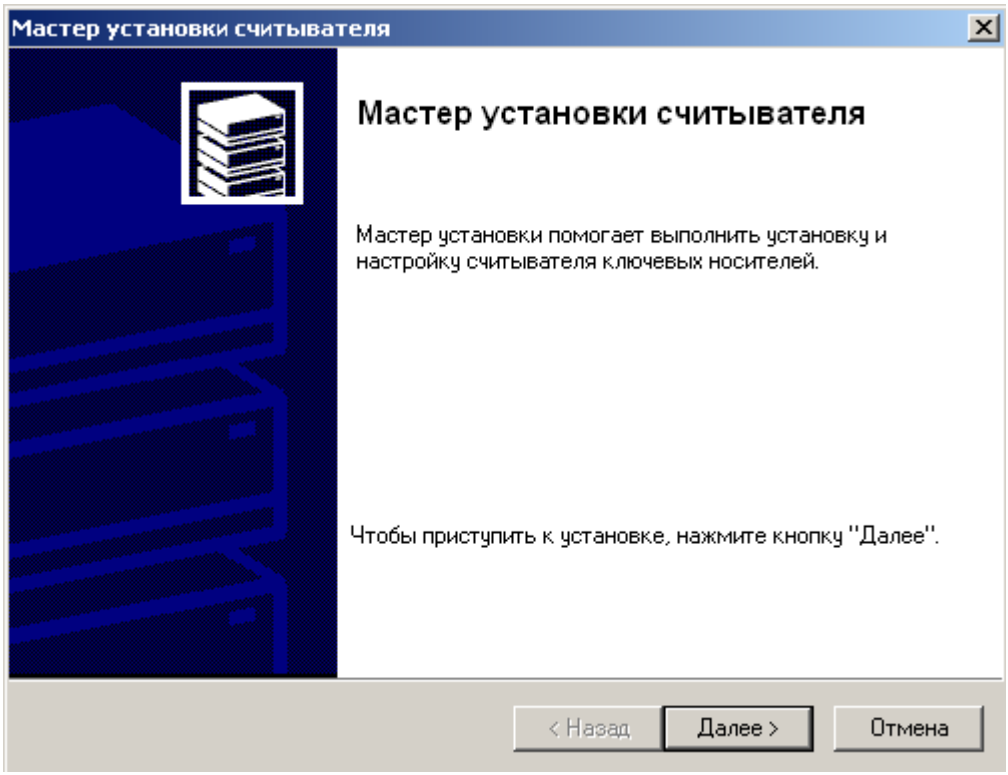


Рисунок 113

 Copyright © S-Terra CSP 2003 - 2015

Шаг 5: из представленного списка выберите считыватель "Реестр" и нажмите кнопку `Далее`:

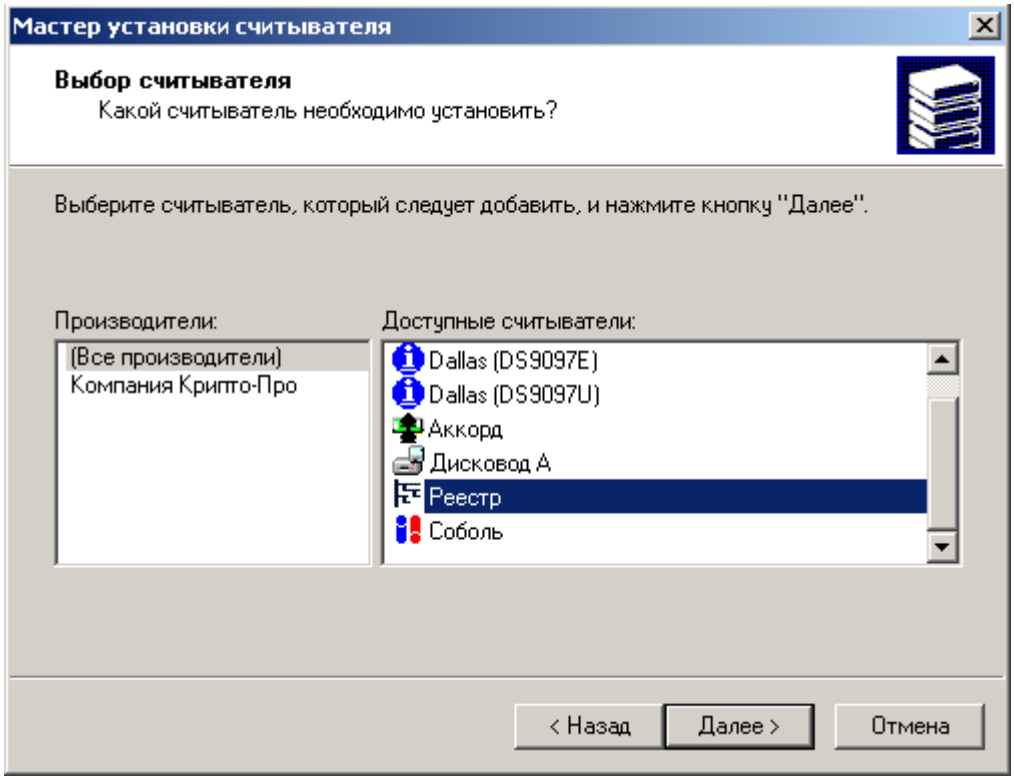


Рисунок 114

Шаг 6: считывателю Реестр можно присвоить имя и нажать кнопку `Далее`:

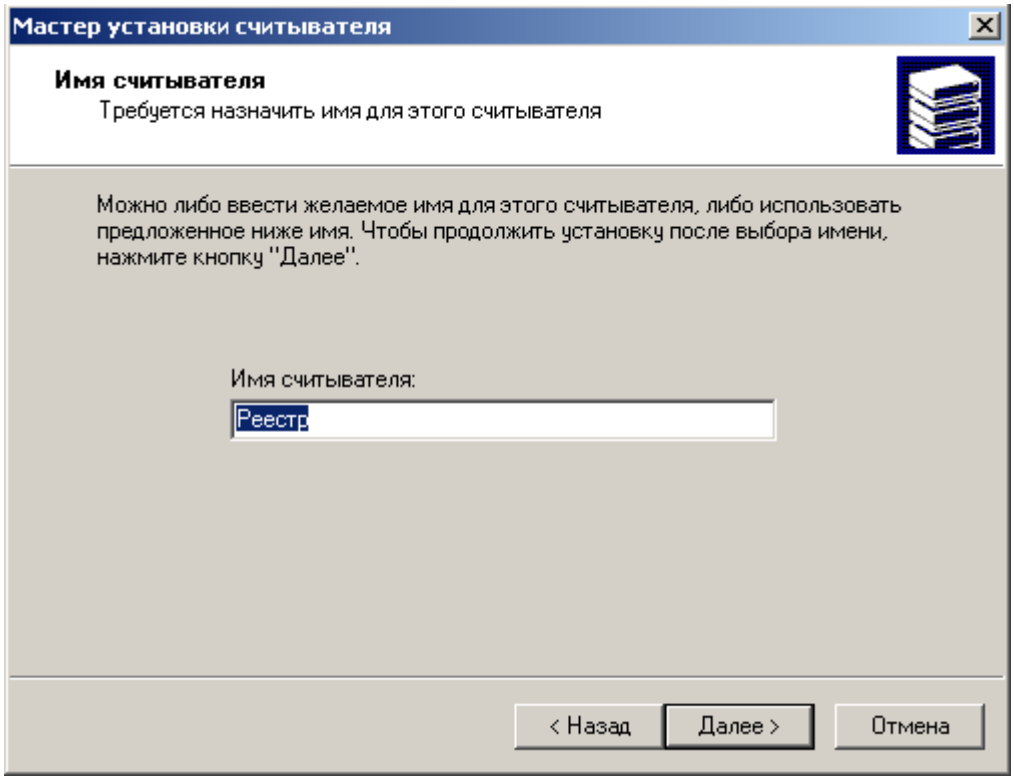


Рисунок 115

 Copyright © S-Terra CSP 2003 - 2015

Шаг 7: инсталляция считывателя Реестр завершена, нажмите `Готово`:

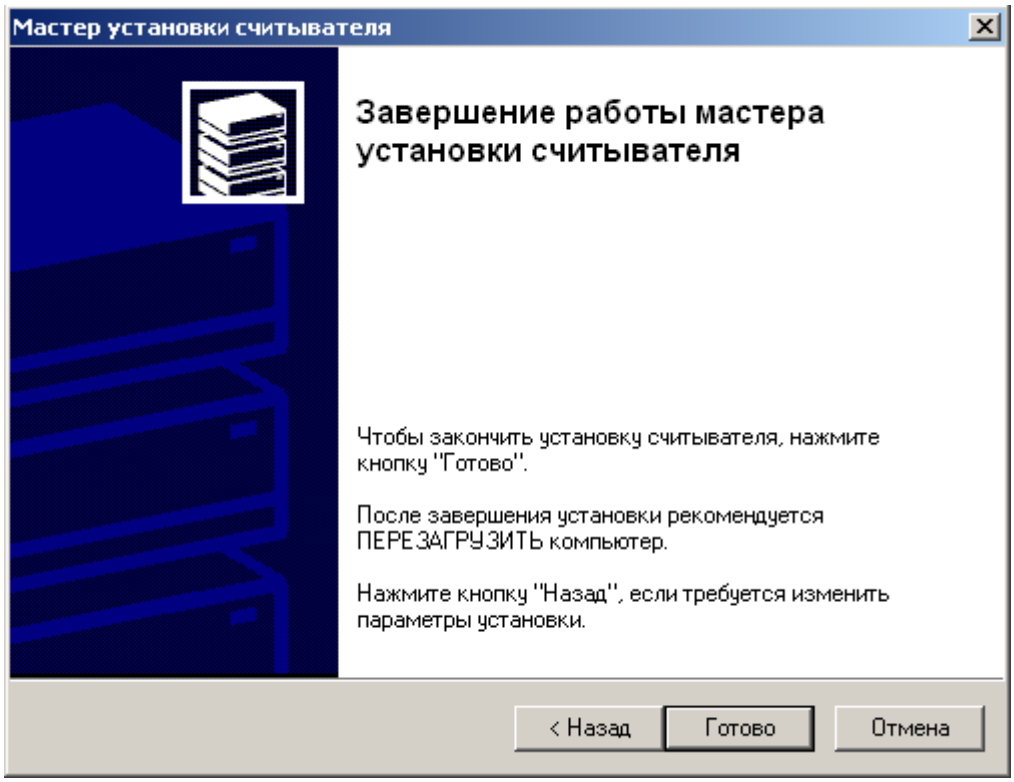


Рисунок 116

Шаг 8: считыватель Реестр добавлен в список инсталлированных считывателей, нажмите `OK`:

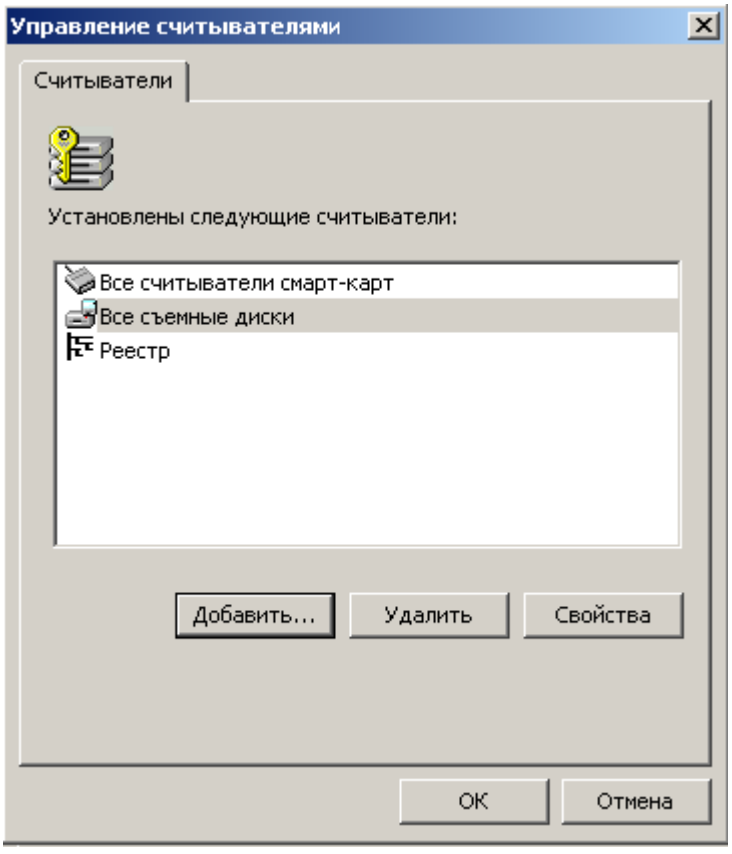


Рисунок 117

Шаг 9: перезагрузите компьютер.

 Copyright © S-Terra CSP 2003 - 2015

22.6.2. Инсталляция внешнего считывателя и ключевого носителя информации в "КриптоПро CSP 3.6/3.6R2"

Инсталляция некоторых внешних считывателей уже выполнена. Для остальных считывателей инсталляция выполняется так же как и для Реестра, описанная в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2".

Для некоторых считывателей необходимо еще выполнить инсталляцию носителей. Для Rutoken и eToken Pro такая инсталляция уже выполнена.

Шаг 1: Инсталляция других носителей производится при выборе предложения Настроить типы носителей... в окне Свойства КриптоПро CSP во вкладке Оборудование (Рисунок 118).

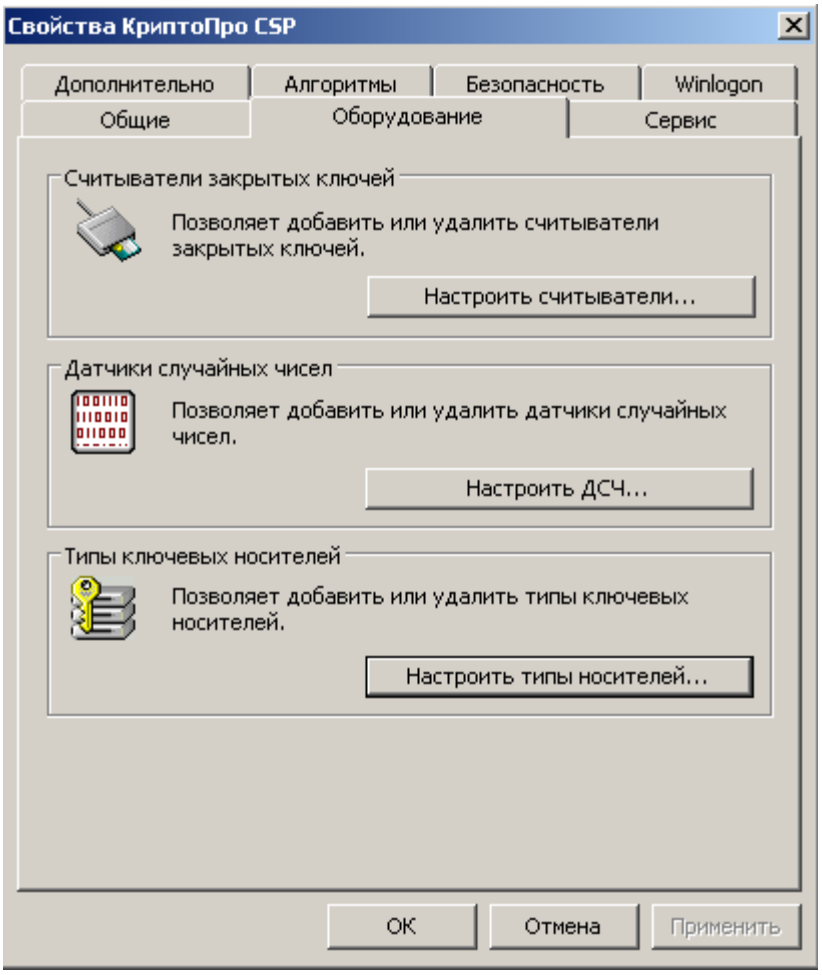


Рисунок 118

 Copyright © S-Terra CSP 2003 - 2015

Шаг 2: вкладка Ключевые носители показывает инсталлированные ключевые носители. Для добавления носителя нажмите кнопку `Добавить...`

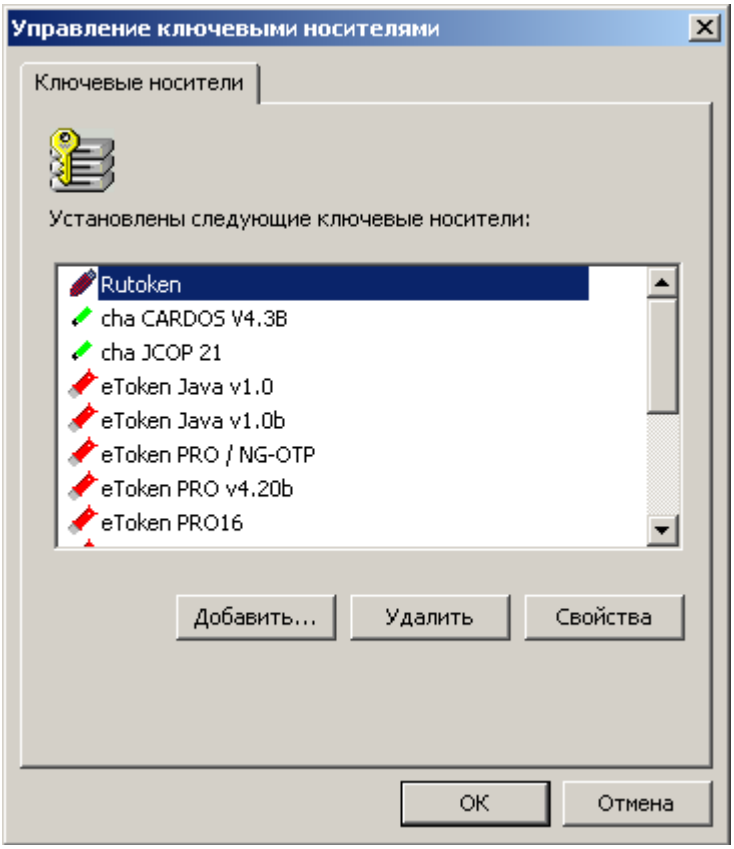


Рисунок 119

Далее следуйте указаниям Мастера установки ключевого носителя.

По завершению инсталляция внешнего ключевого носителя и считывателя полностью выполнена.

 Copyright © S-Terra CSP 2003 - 2015

22.6.3. Настройка ДСЧ

Для защиты ПК от несанкционированного доступа в режиме КС1 используется биологический ДСЧ, в режиме защиты КС2 – используется ПАК «Соболь» или «Аккорд-АМДЗ».

Шаг 1: во вкладке Оборудование нажмите кнопку `Настроить ДСЧ...`:

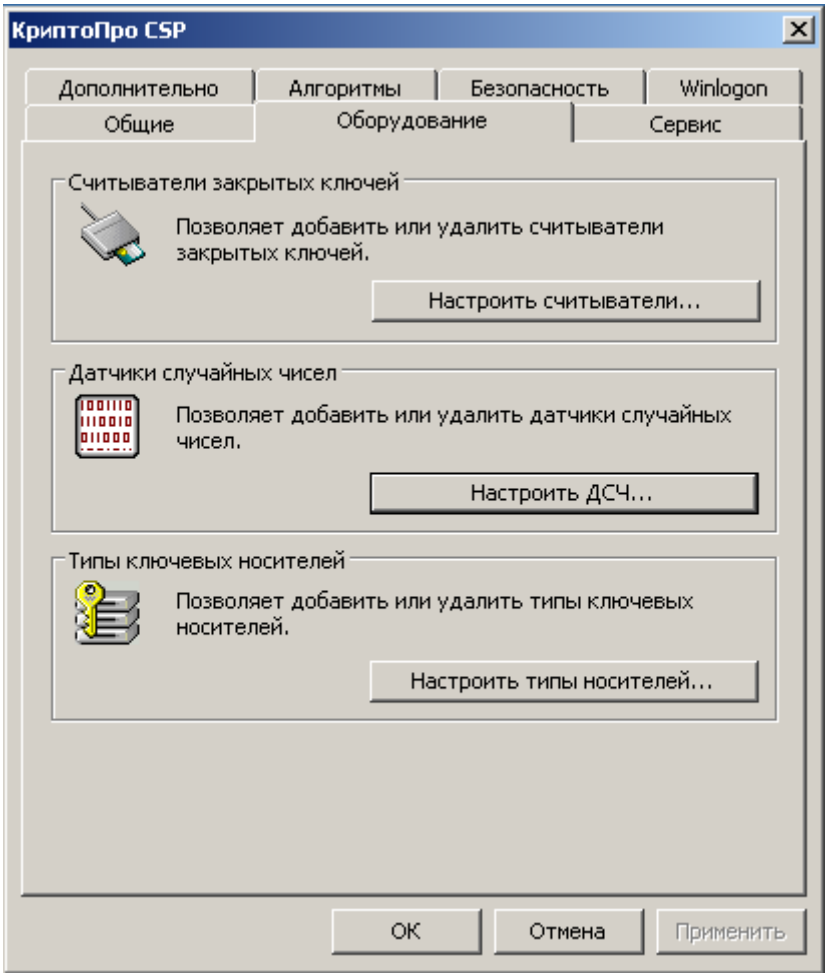


Рисунок 120

Шаг 2: если используется режим защиты КС1, то в открывшемся окне должен быть установлен только «Биологический ДСЧ» (Рисунок 121). Нажмите кнопку `OK`.

 Copyright © S-Terra CSP 2003 - 2015

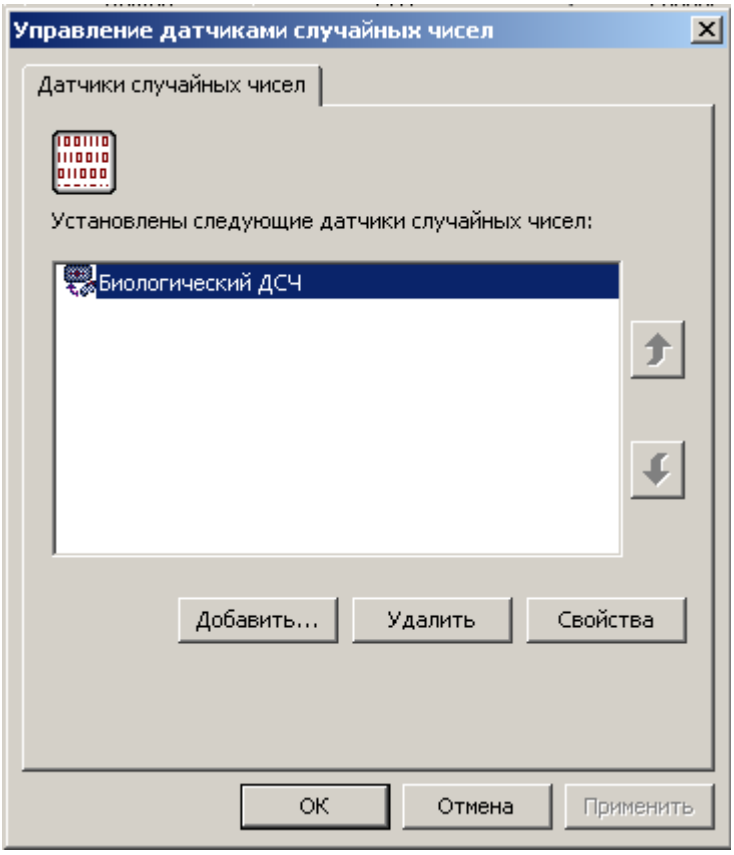


Рисунок 121

Шаг 3: для режима защиты КС2 добавьте аппаратный ДСЧ, нажав кнопку `Добавить…`.

Шаг 4: открывается Мастер установки ДСЧ, нажмите кнопку `Далее`.

Шаг 5: в окне выбора ДСЧ выберите ДСЧ – либо Аккорд либо Соболь, и нажмите `Далее`

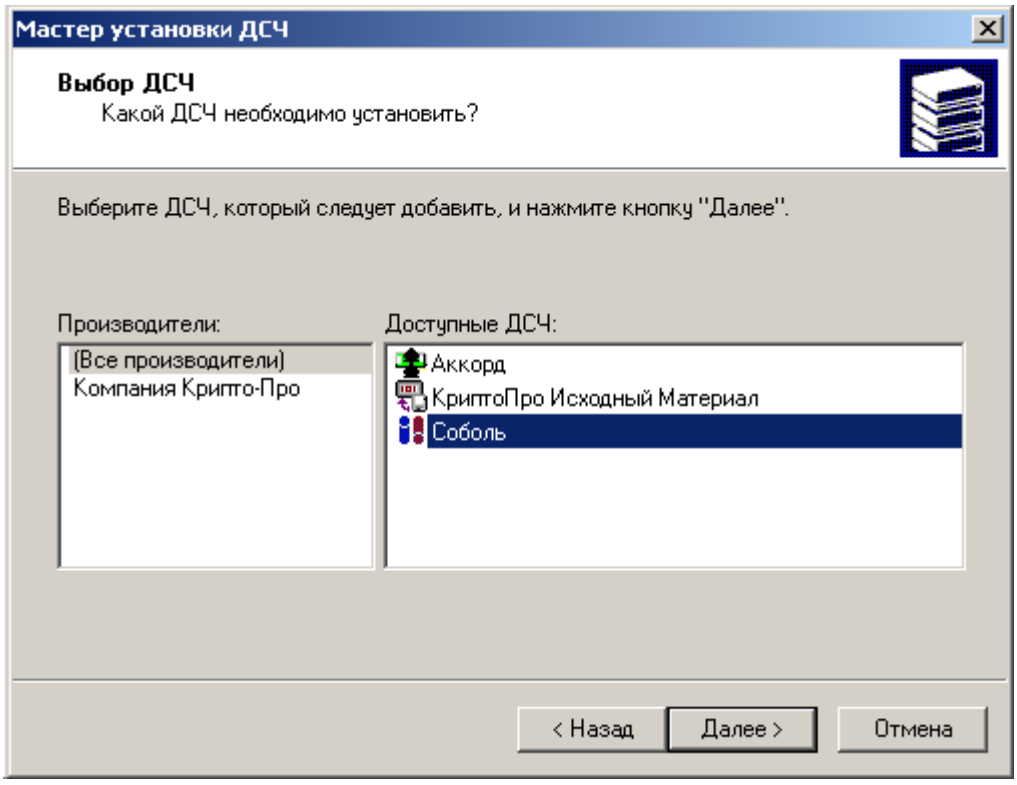


Рисунок 122

 Copyright © S-Terra CSP 2003 - 2015

Шаг 6: установленный аппаратный ДСЧ переместите в верхнюю строчку, Биологический ДСЧ можно удалить или оставить, нажмите кнопку `OK`.

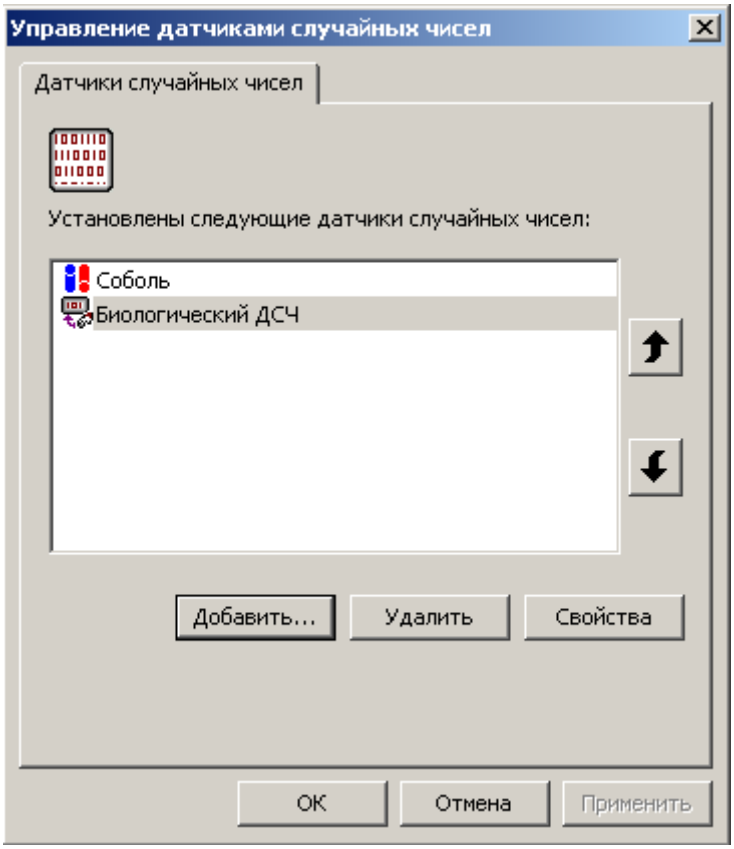


Рисунок 123

22.6.4. Установка и настройка Удостоверяющего Центра. Создание CA сертификата

Перед созданием ключевой пары и запроса на сертификат пользователя опишем как создать Удостоверяющий Центр (центр сертификации – CA) средствами MS, который будет издавать сертификат пользователю. Если Вам известен Сертификационный Центр, который по Вашему запросу будет издавать сертификат пользователя, то перейдите к следующему разделу – созданию ключевой пары, в противном случае – создайте свой Удостоверяющий Центр.

На отдельном компьютере установите ОС Windows Server 2008 R2 и СКЗИ «КриптоПро CSP 3.6/3.6R2».. Для инсталляции Удостоверяющего Центра Microsoft Certification Authority выполните следующее:

Инсталлируйте ключевой считыватель Реестр для хранения контейнера с секретным ключом CA сертификата, как описано в разделе “Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2".

Для инсталляции Удостоверяющего Центра Microsoft Certification Authority запустите `Server Manager` (`Start-Administrative Tools-Server Manager`) и войдите в раздел `Roles`. Выберите `Add Roles` и инсталлируйте `Web Server (IIS)`.

Затем, выполните инсталляцию `Active Directory Certificate Services` (Рисунок 124), которую опишем подробнее.

 Copyright © S-Terra CSP 2003 - 2015

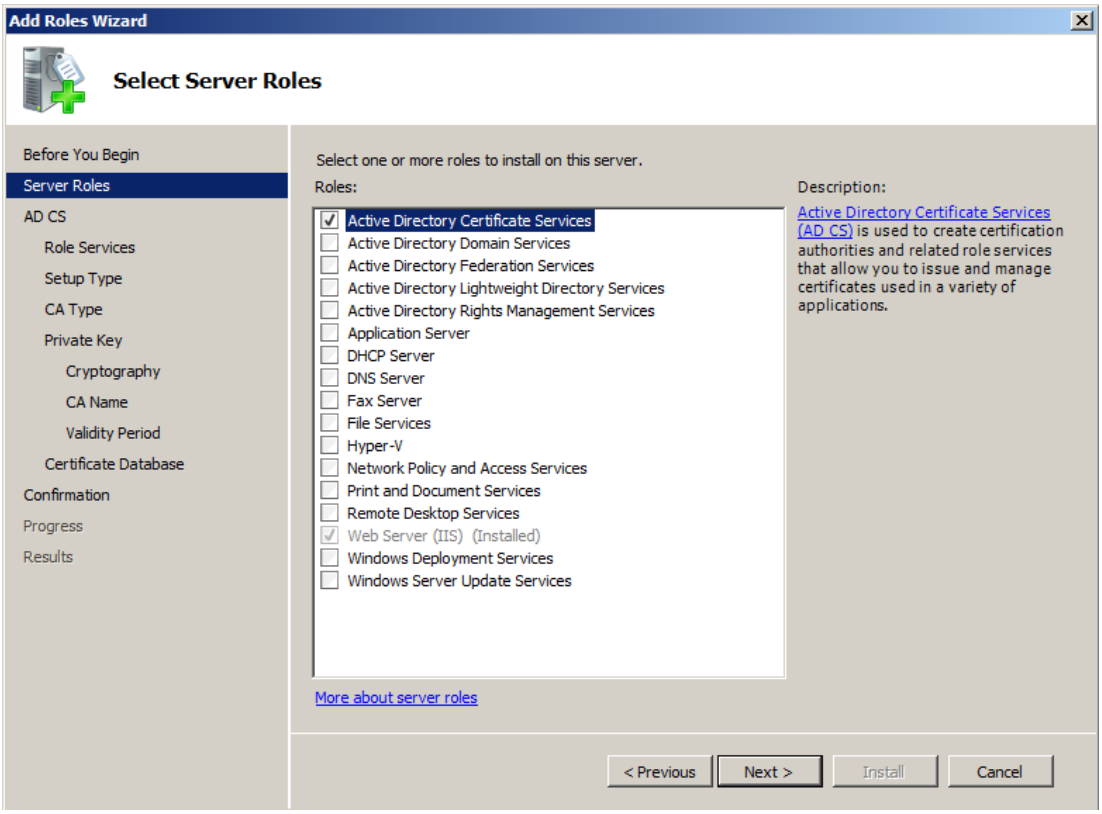


Рисунок 124

Шаг 1: установите флажки `Certification Authority` и `Certification Authority Web Enrollment` и нажмите `Next`.

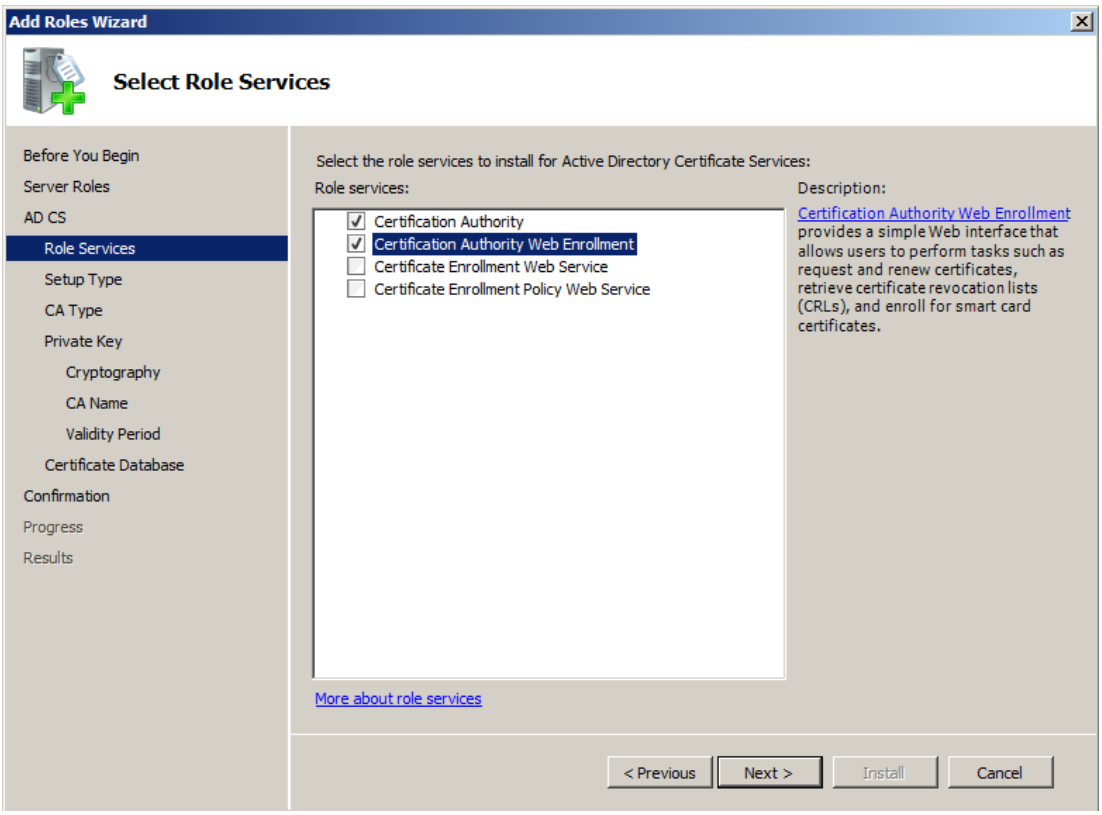


Рисунок 125

Шаг 2: переключатель должен стоять в положении `Standalone`, нажмите `Next`.

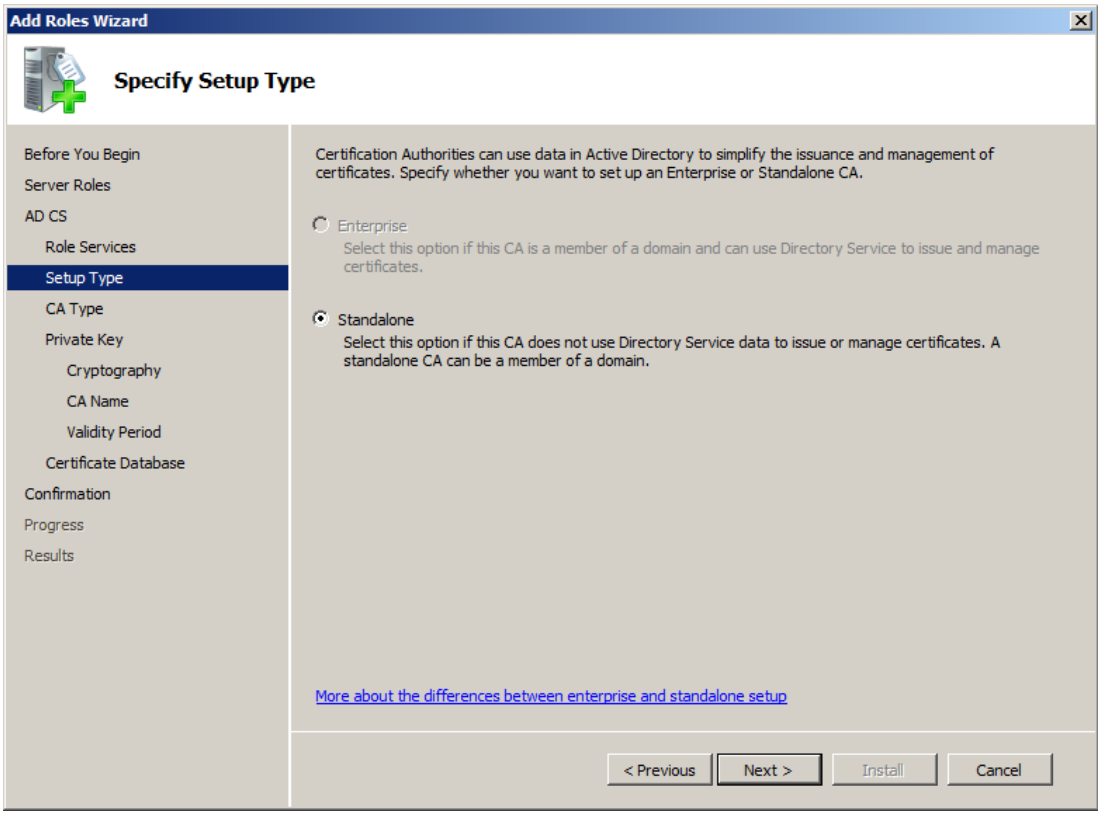


Рисунок 126

Шаг 3: поставьте переключатель в положение `Roote CA` и нажмите `Next`..

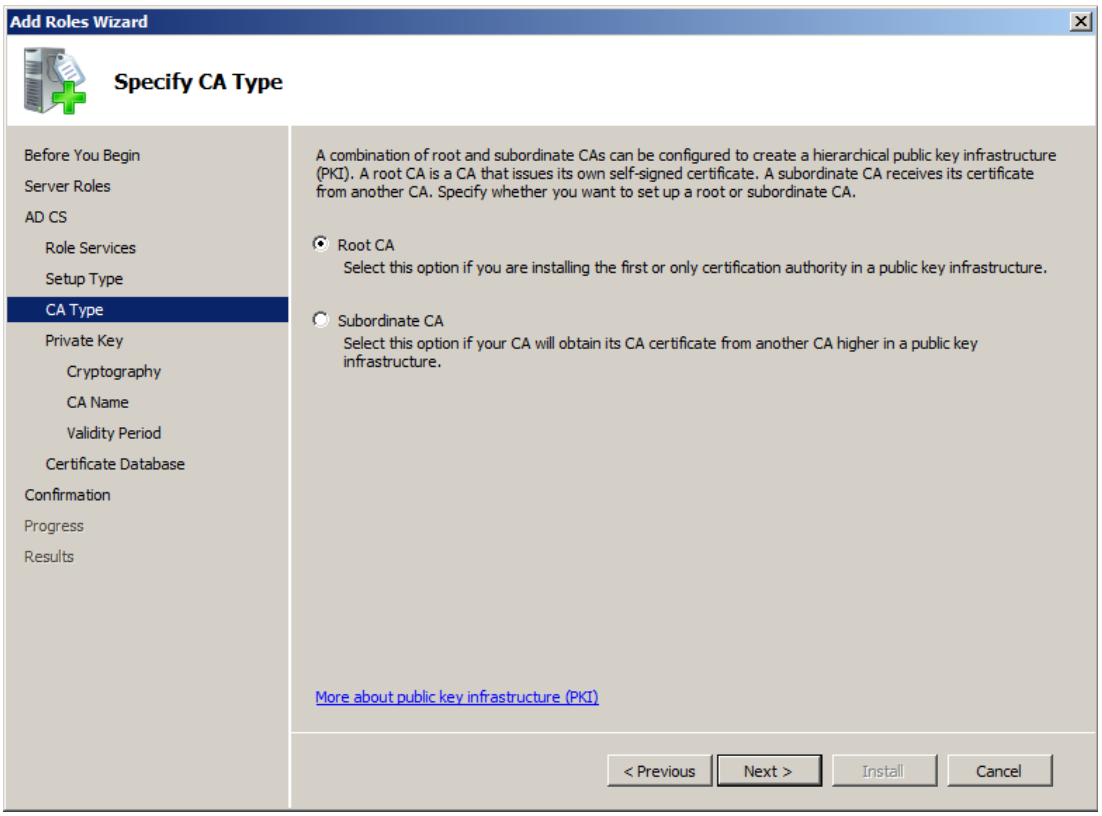


Рисунок 127

 Copyright © S-Terra CSP 2003 - 2015

Шаг 4: поставьте переключатель в положение `Create a new private key`.

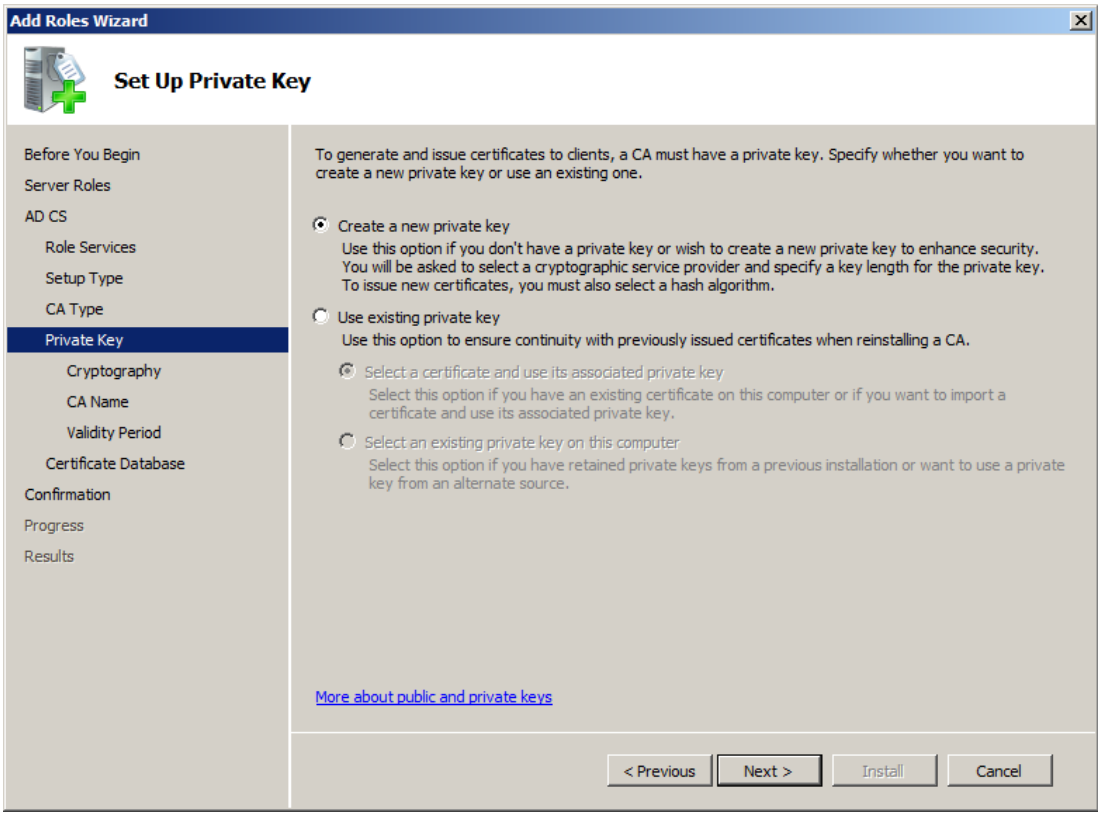


Рисунок 128

Шаг 5: в качестве криптопровайдера выберите `Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider` и установите флажок `Allow administrator interaction when the private key is accessed by the CA`.

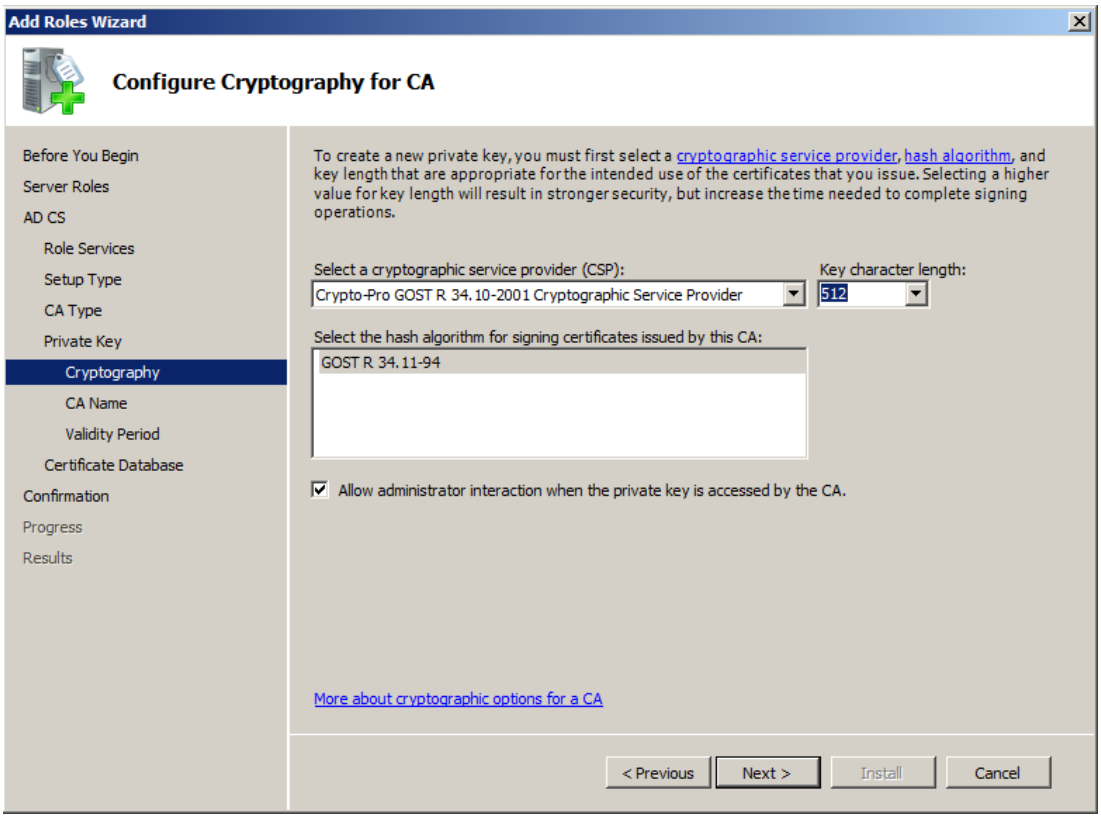


Рисунок 129

Шаг 6: заполните поля для CA сертификата и нажмите `Next` (Рисунок 130):

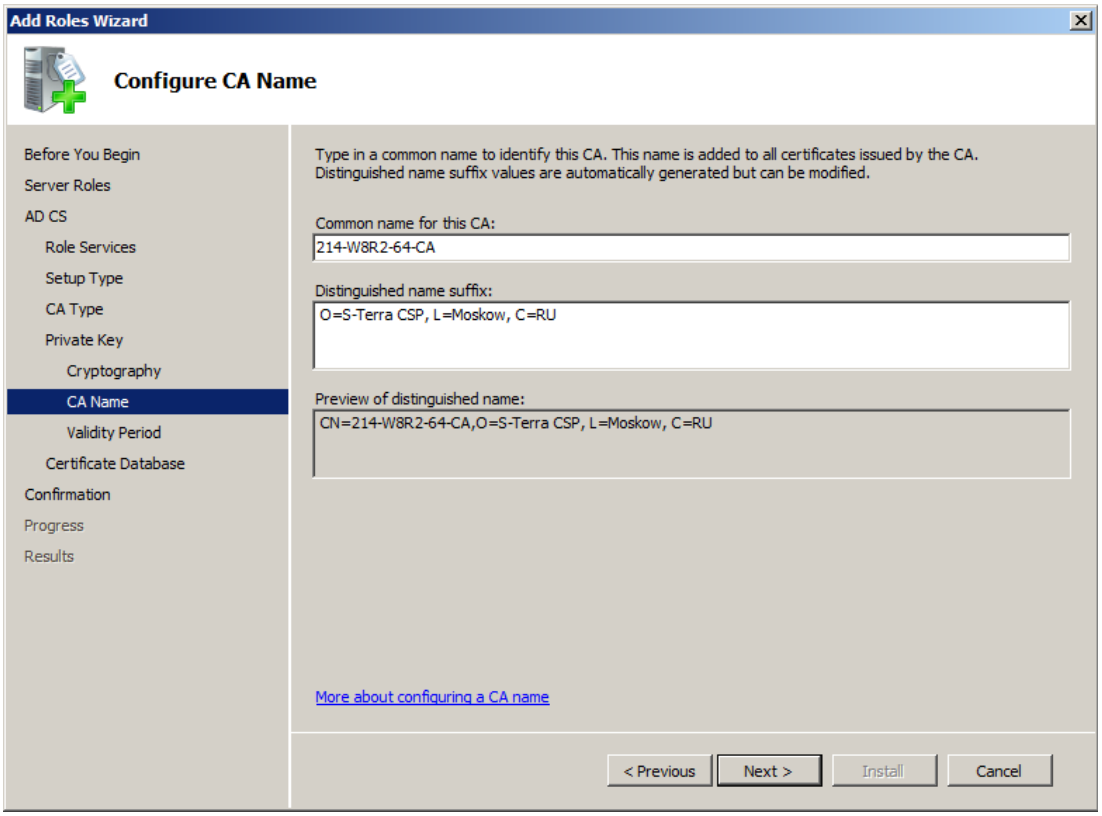


Рисунок 130

Шаг 7: укажите период действия для сертификата, нажмите `Next`.

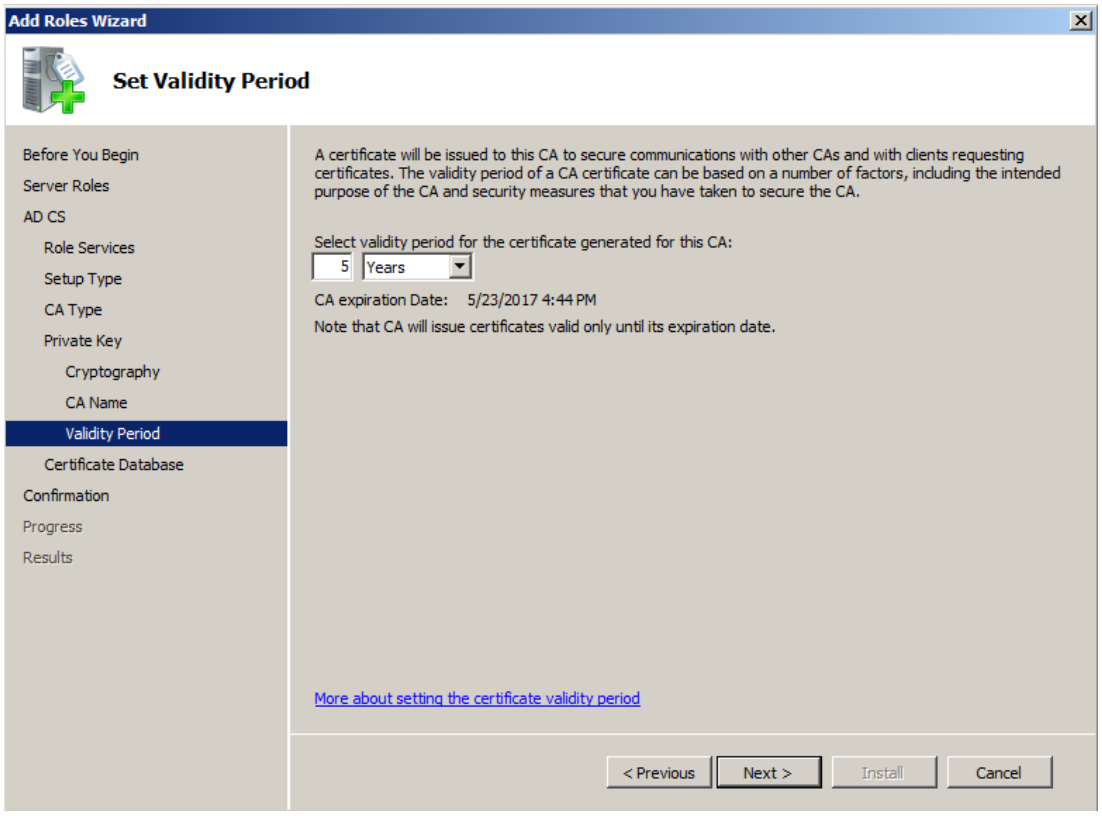


Рисунок 131

Шаг 8: в окне с указанием о размещении хранилища оставьте значения по умолчанию и нажмите `Next`.

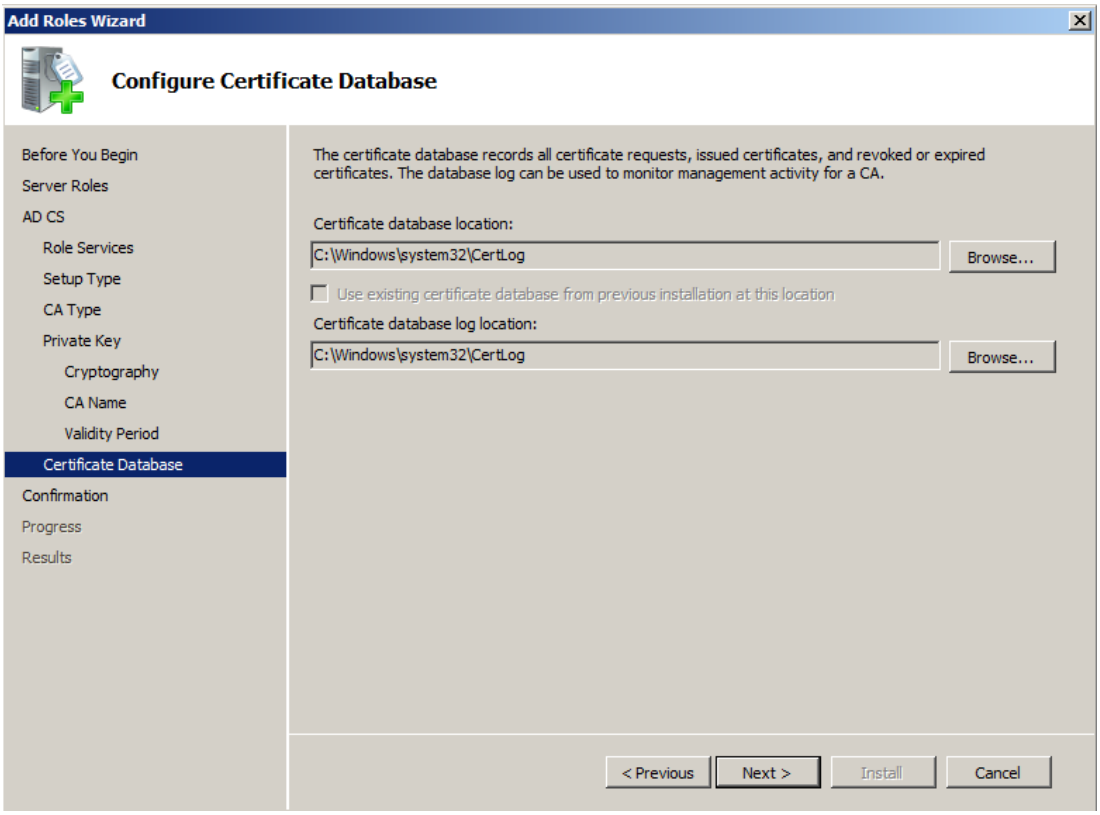


Рисунок 132

Шаг 9: нажмите `Install`.

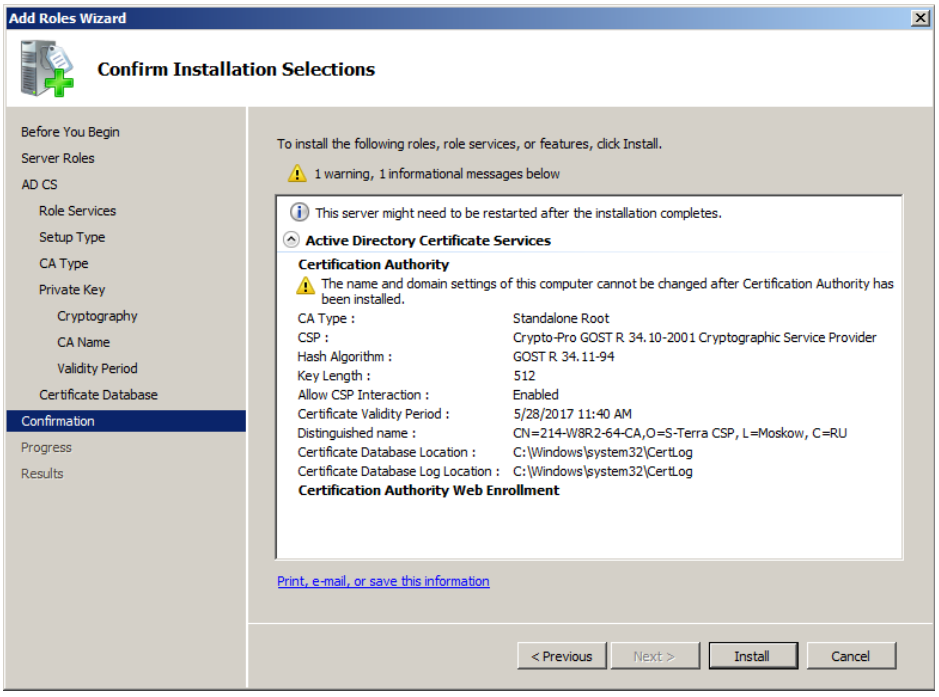


Рисунок 133

Шаг 10: выберите ключевой носитель `Registry`, куда будет записан контейнер с секретным ключом для CA сертификата.

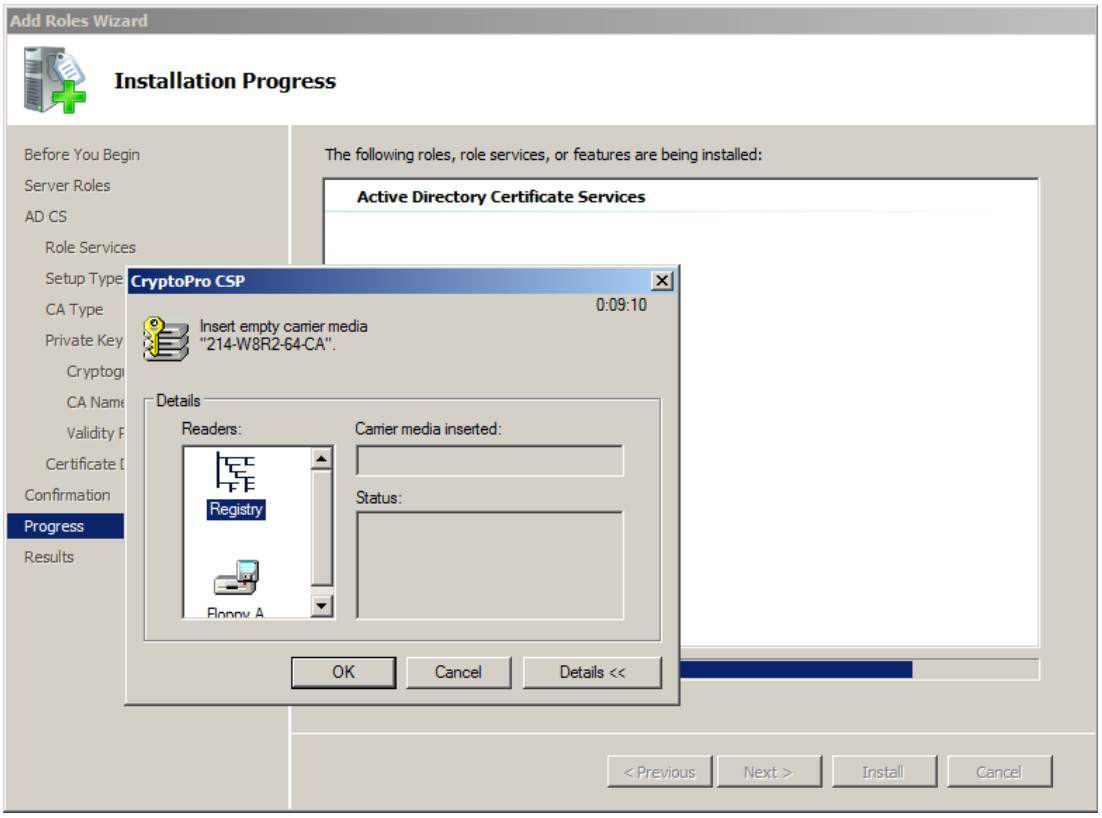


Рисунок 134

Шаг 11: подвигайте мышкой или понажимайте клавиши, пока происходит создание ключевой пары.

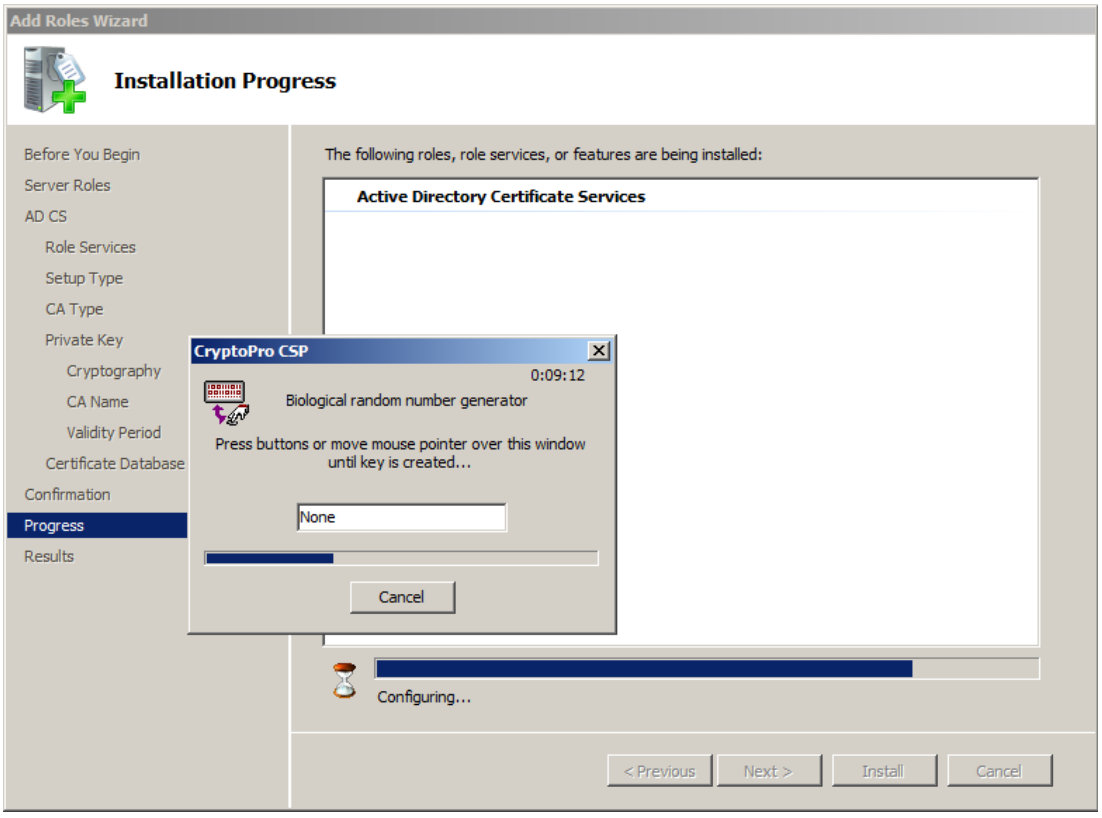


Рисунок 135

 Copyright © S-Terra CSP 2003 - 2015

Шаг12: задайте пароль к созданному контейнеру.

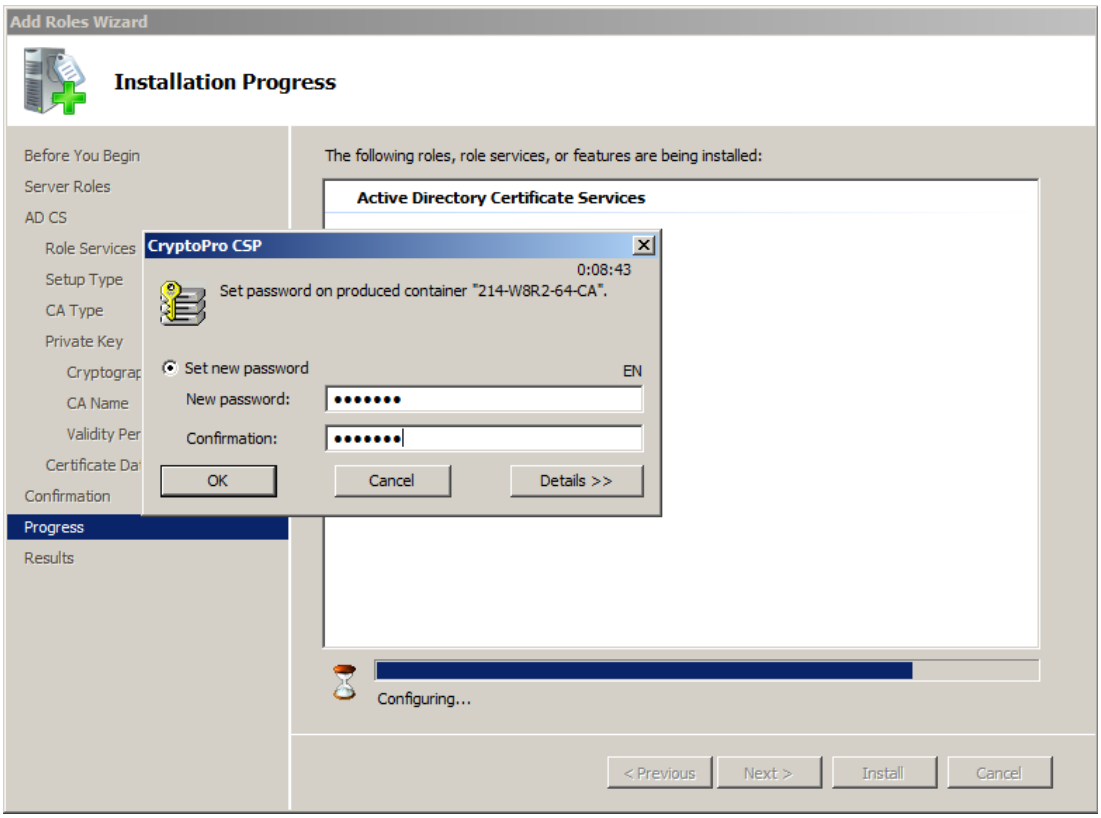


Рисунок 136

Шаг13: укажите пароль к созданному контейнеру

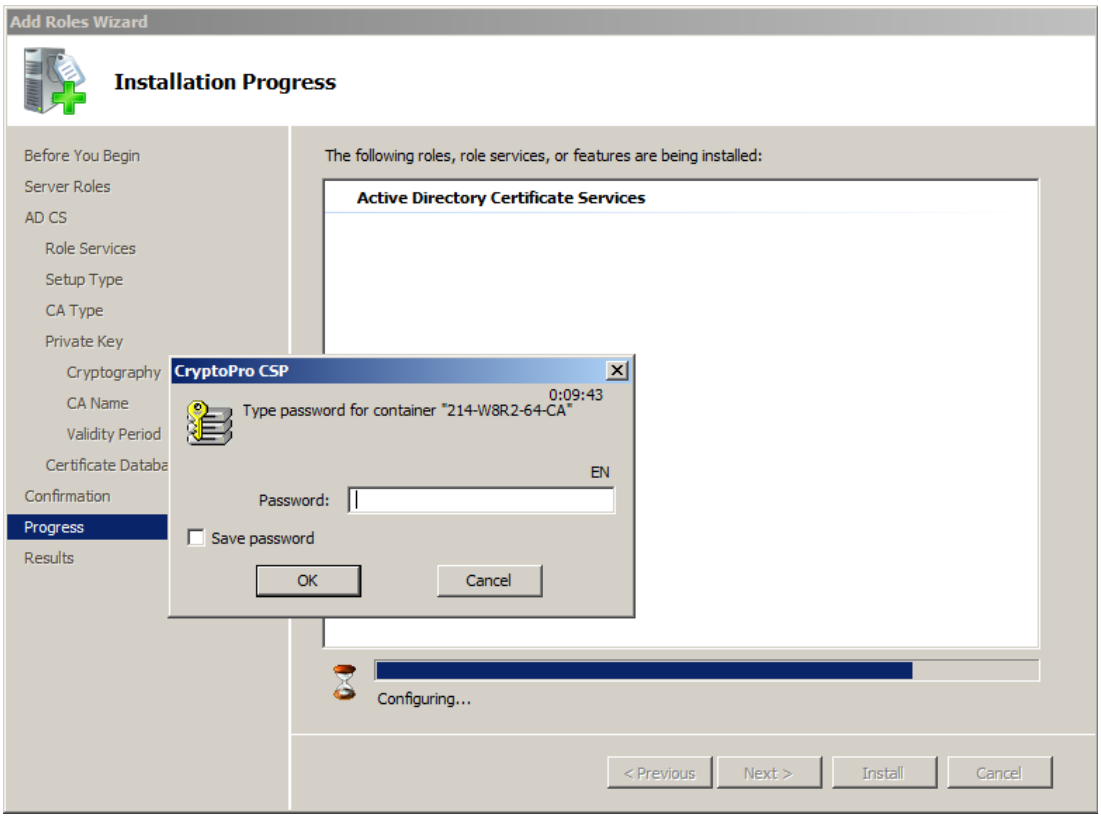


Рисунок 137

Шаг14: инсталляция Удостоверяющего Центра завершена, нажмите `Close`.

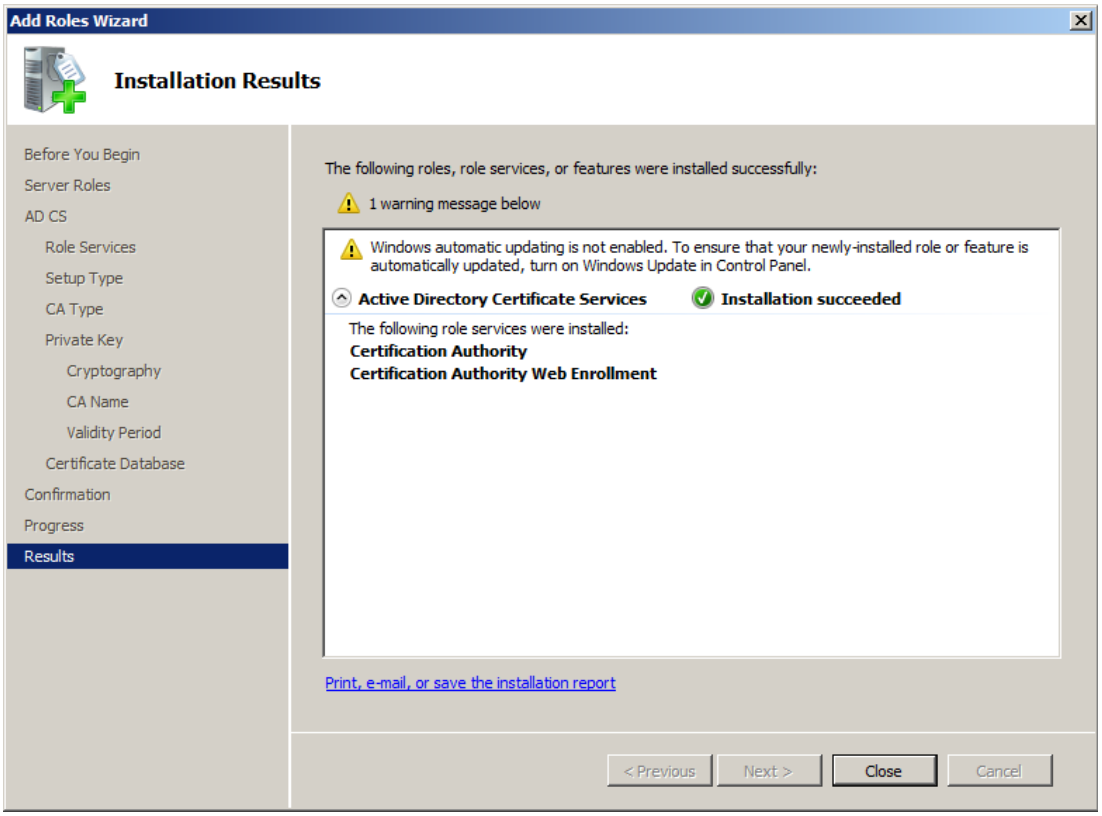


Рисунок 138

Шаг15: для автоматического создания подписываемых сертификатов по запросу проведите некоторые настройки Удостоверяющего Центра. Вызовите `Certificate Authority (Start- Administrative Tools-Certification Authority)`, выделите центр CA и нажмите `Properties`. В окне `Properties` войдите во вкладку `Policy Module` и нажмите кнопку `Properties`...(Рисунок 139).

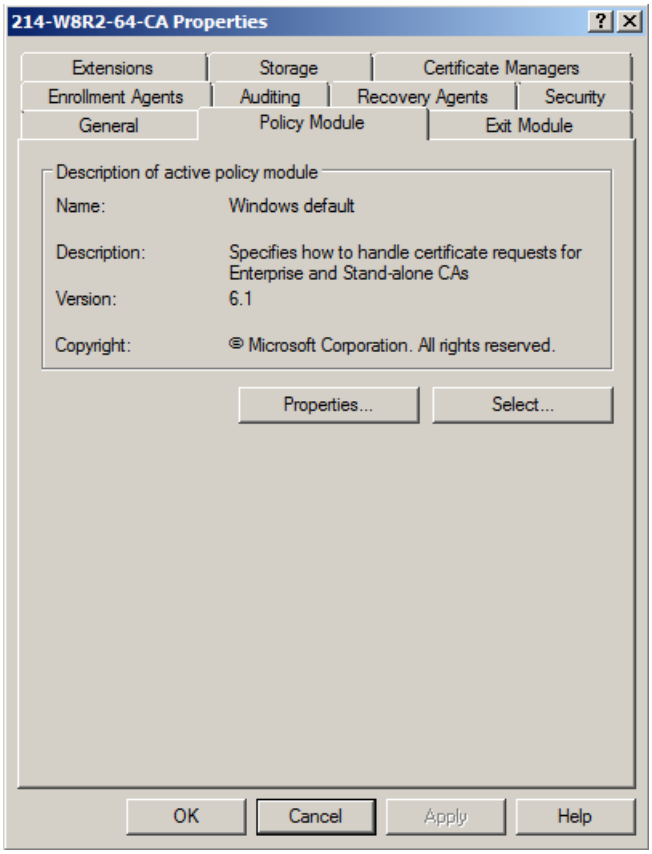


Рисунок 139

Шаг16: в появившемся окне `Properties` (Рисунок 140) установите переключатель в положение `Follow the settings …` (автоматически издавать сертификат по запросу) и нажмите `OK`::

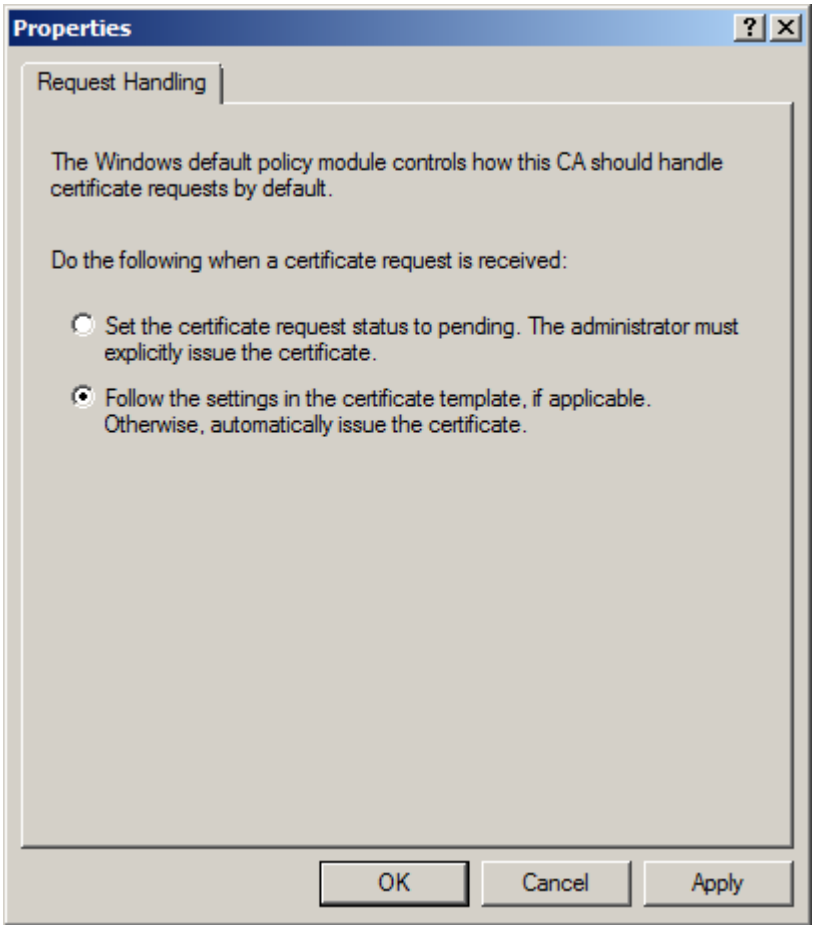


Рисунок 140

Шаг17: в окне `Windows default` выдается предупреждение о необходимости перезапуска сертификатного сервиса:

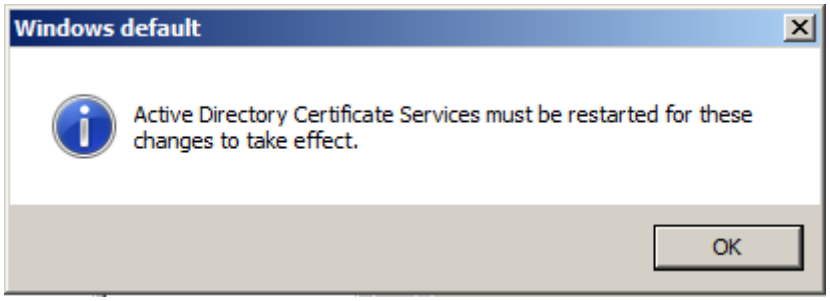


Рисунок 141

 Copyright © S-Terra CSP 2003 - 2015

Шаг18: в окне `Certificate Authority` (Рисунок 142) выберите предложение меню `Action`, в выпадающем меню предложение `All Tasks`, а в следующем выпадающем меню – предложение `Stop Service`. После остановки сервиса выберите предложение `Start Service`.

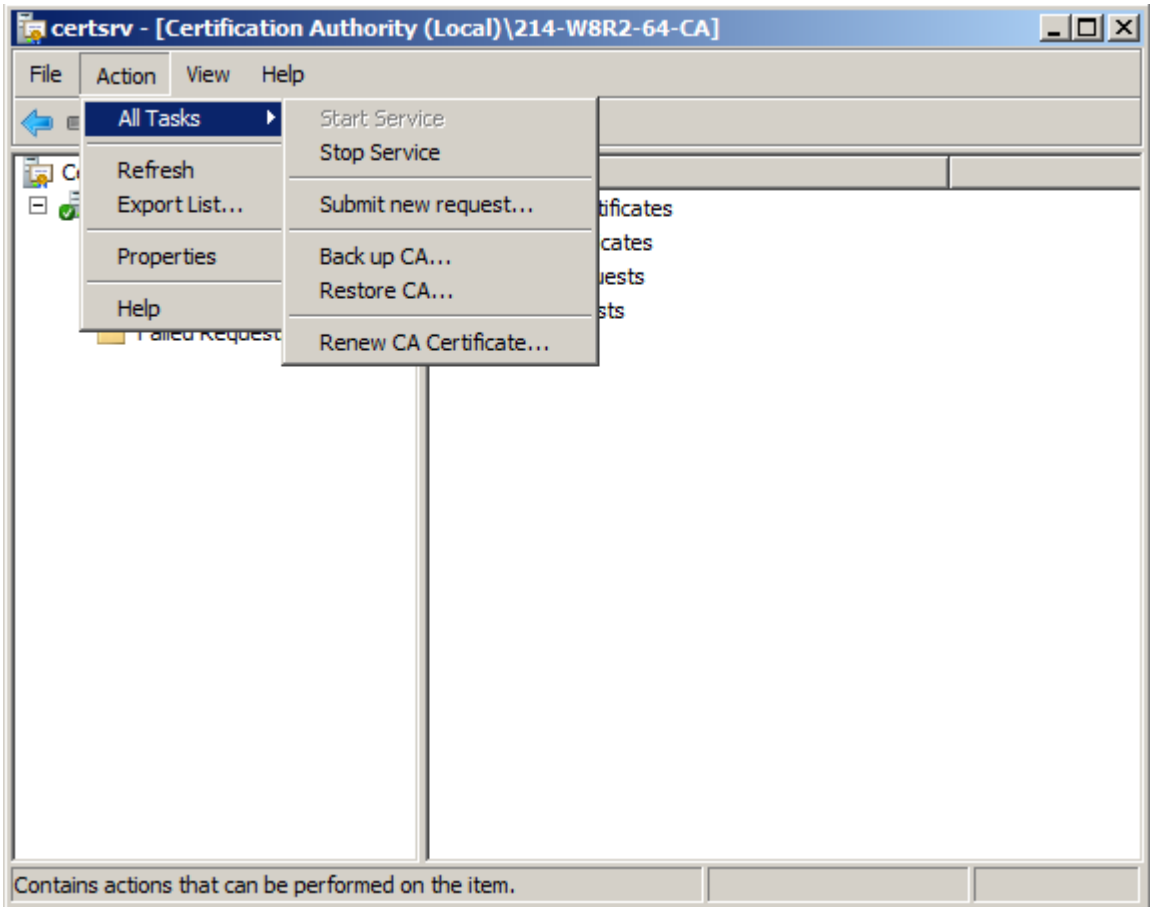


Рисунок 142

На этом создание Удостоверяющего Центра и его СА сертификата закончено.

Примечание:

Если была установлена версия 3.6/3.6R2 СКЗИ “КриптоПро CSP”, то для возможности дальнейшего выбора криптопровайдера “КриптоПро CSP” в окне создания запроса на сертификат, выполните следующее:

в файле `System32\certsrv\certsgcl.inc` измените значение константы `ConstnMaxProvType` с 25 на 99. В стандартном скрипте перечислено только 25 типов криптопровайдера.

 Copyright © S-Terra CSP 2003 - 2015

22.6.5. Экспортирование CA сертификата в файл

Шаг 1: для экспортирования CA сертификата в файл, войдите сначала в `Certificate Authority (Start- Administrative Tools-Certification Authority)`, выделите центр CA и нажмите `Properties`:

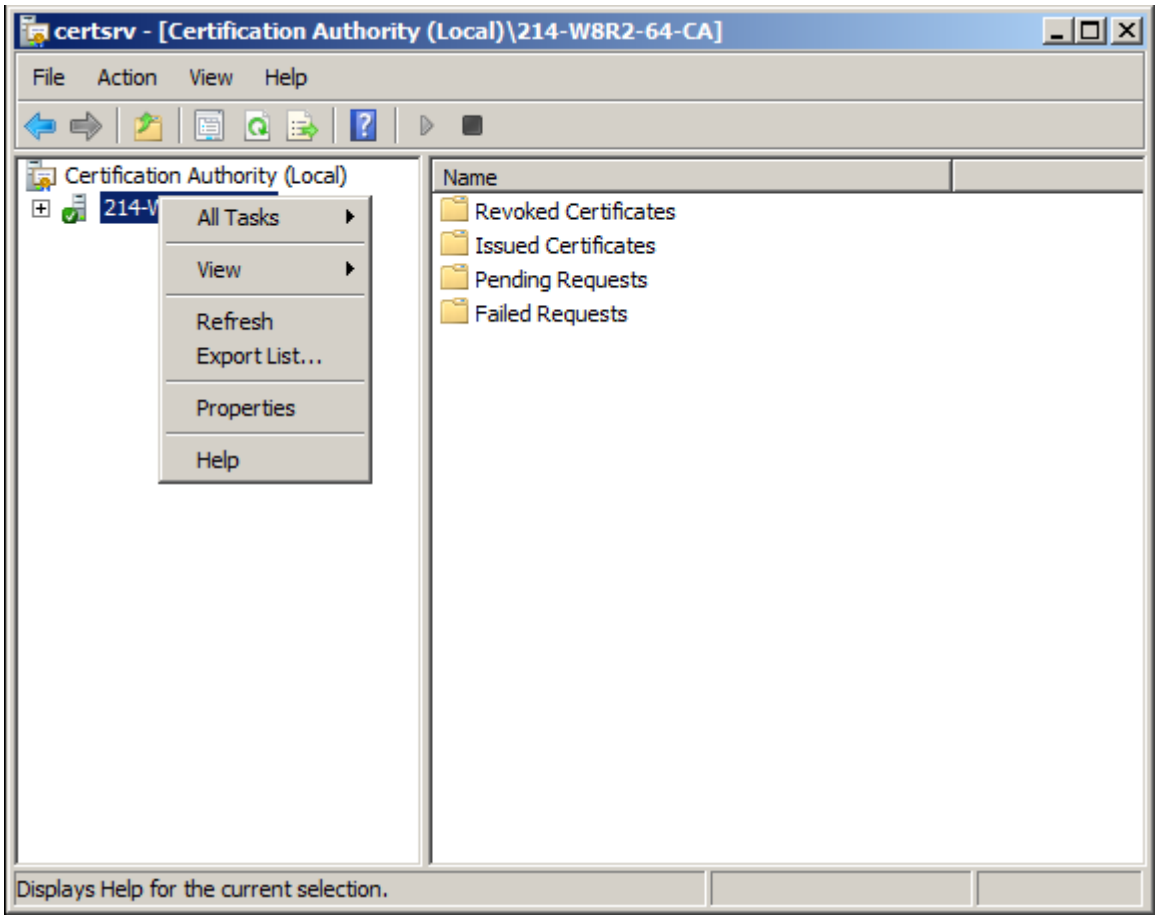


Рисунок 143

Шаг 2: далее во вкладке `General` нажмите кнопку `View Certificate`. В появившемся окне `Certificate` выберите вкладку `Details` (Рисунок 144), в выпадающем меню `Show` выберите предложение All, чтобы увидеть все поля сертификата. Нажмите кнопку `Copy to File`.

 Copyright © S-Terra CSP 2003 - 2015

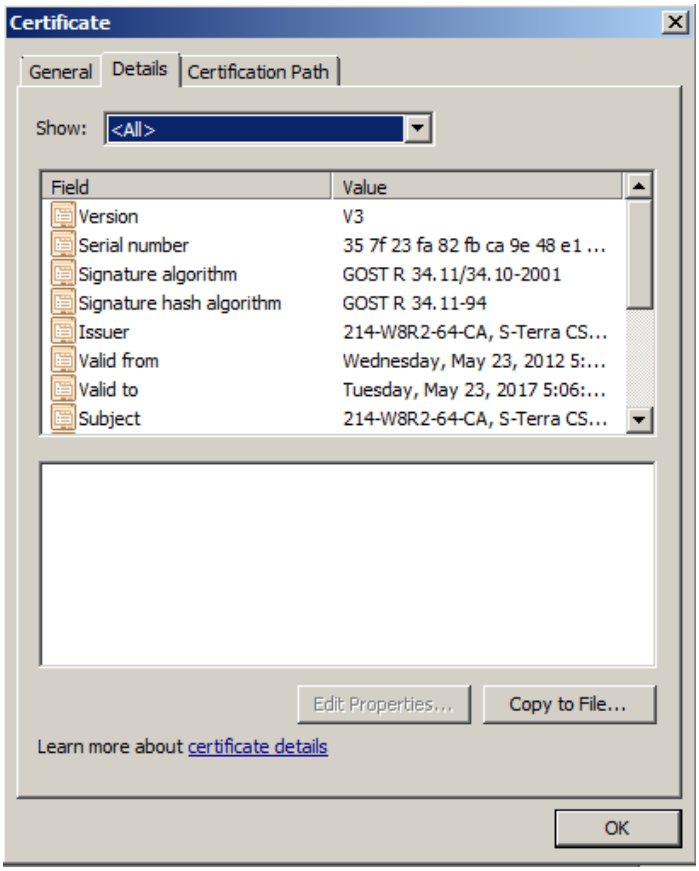


Рисунок 144

Шаг 3: в окне визарда экспортирования сертификата нажмите `Next`:



Рисунок 145

 Copyright © S-Terra CSP 2003 - 2015

Шаг 4: далее в окне визарда `Certificate Export` выберите формат, в котором должен быть экспортирован сертификат.

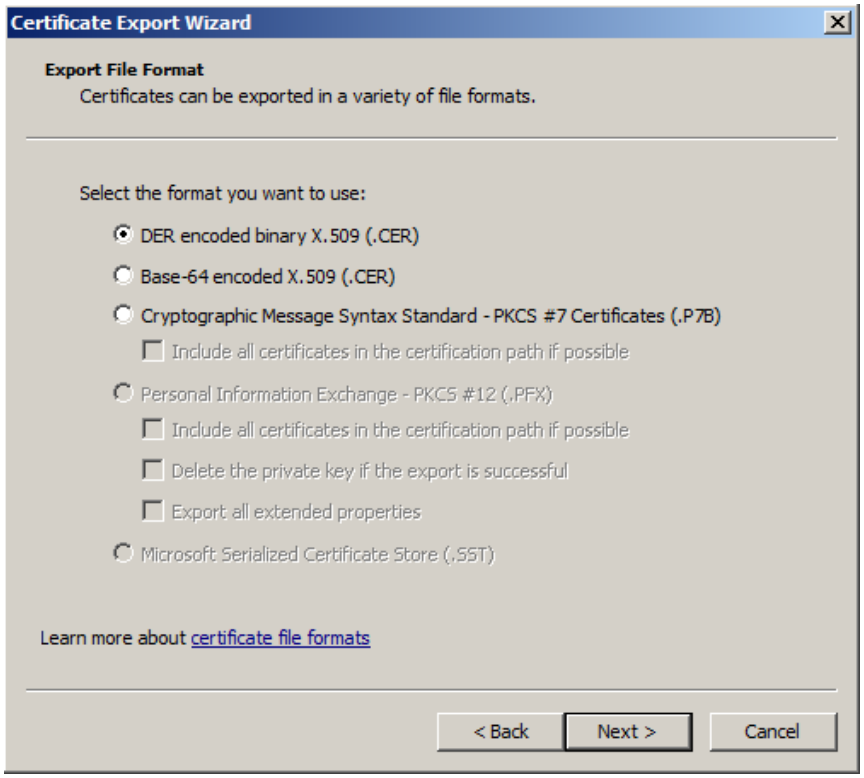


Рисунок 146

Шаг 5: укажите имя файла, в который будет экспортирован сертификат.

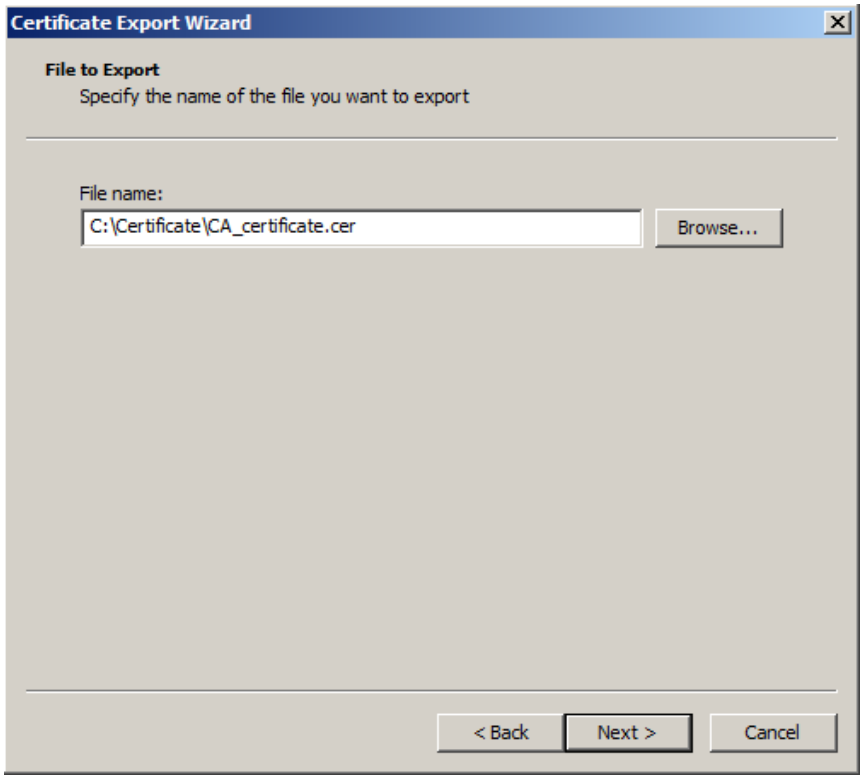


Рисунок 147

 Copyright © S-Terra CSP 2003 - 2015

Шаг 6: экспортирование CA сертификата в файл завершено, нажмите `Finish`.



Рисунок 148

22.6.6. Создание ключевой пары и формирование запроса на сертификат пользователя

Для создания ключевой пары и формирования запроса на сертификат пользователя можно использовать средства Microsoft Windows. Опишем этот процесс на отдельном компьютере пользователя..

Шаг 1: установите программный Продукт СКЗИ "КриптоПро CSP 3.6/3.6R2". Установка этого Продукта описана в разделе "Установка СКЗИ "КриптоПро CSP 3.6/3.6R2".

Шаг 2: инсталлируйте ключевой носитель, на котором будет размещен контейнер с секретным ключом пользователя, например, Реестр, используя СКЗИ "КриптоПро CSP 3.6/3.6R2". Эта инсталляция описана в разделе "Инсталляция ключевого считывателя Реестр в "КриптоПро CSP 3.6/3.6R2".

Шаг 3: запустите Microsoft Internet Explorer. В поле Address укажите адрес сервера Удостоверяющего Центра и запустите утилиту `certsrv` (Certificate Service), например, `http://10.0.6.214/certsrv/`.

Полагаем, что на сервере уже установлен Продукт СКЗИ "КриптоПро CSP 3.6/3.6R2".

Шаг 4: в появившемся окне высвечивается имя удостоверяющего центра – в нашем случае 214-W8R2-64-CA. Для формирования запроса на создание сертификата пользователя выберите предложение "`Request a certificate`" (Рисунок 149):

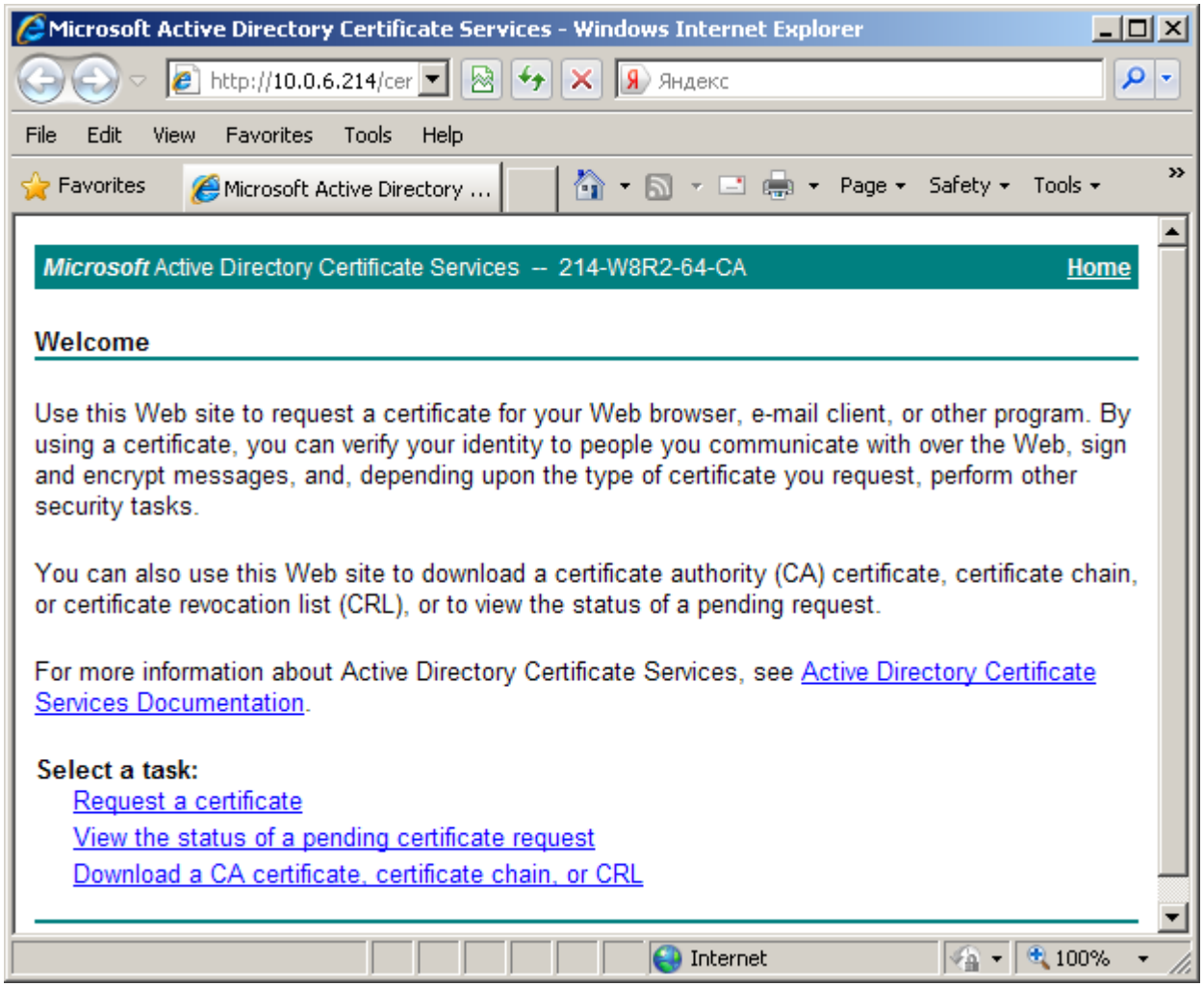


Рисунок 149

Шаг 5: выберите расширенный запрос на сертификат – предложение "`advanced certificate request`" (Рисунок 150):

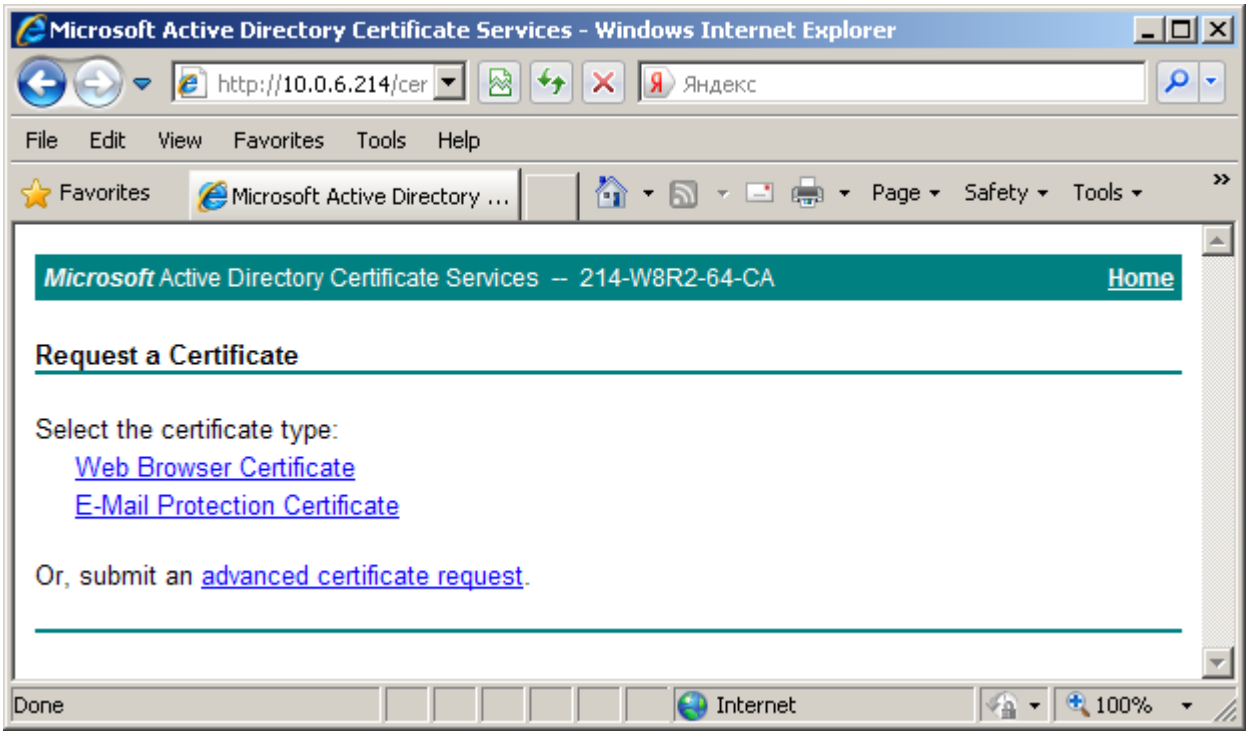


Рисунок 150

Шаг 6: для получения формы для формирования запроса на сертификат выберите предложение "`Create and submit a request to this CA`" (Рисунок 151):

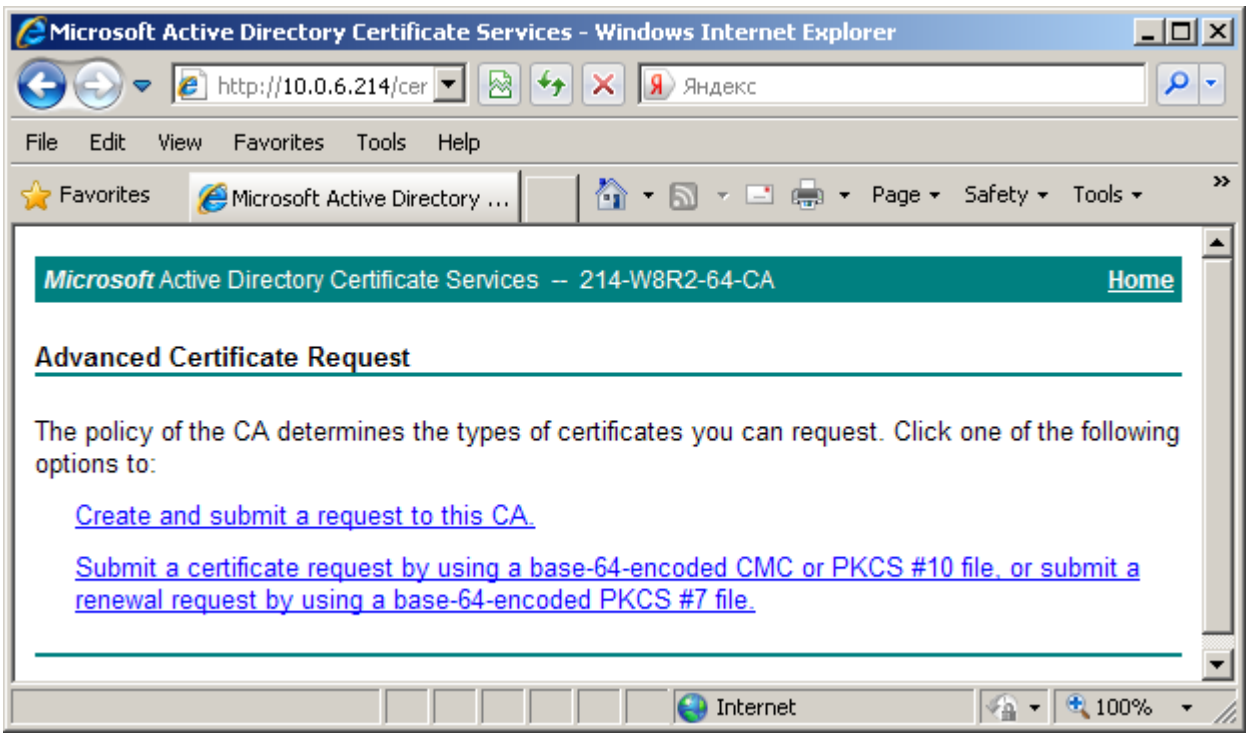


Рисунок 151

Шаг 7: заполните форму расширенного запроса, показанную ниже (Рисунок 152). Дадим некоторые пояснения для ее заполнения:

- в разделе **Identifying Information** (Информация о Владельце Сертификата) внесите данные о владельце сертификата. Во всех полях этого раздела разрешается использовать не только латинские, но и русские буквы, кроме поля Country/Region, оно всегда содержит значение RU.
  Примечание: если при создании запроса на сертификат при заполнении полей сертификата используются русские буквы, необходимо, чтобы они были введены в формате UTF-8
- в разделе **Type of Certificate Needed** (Тип требуемого сертификата) из выпадающего списка выберите предложение Client Authentication Certificate
- в разделе **Key Options** (Опции ключей) задаются параметры создаваемой ключевой пары и размещение секретного ключа. Рекомендуется выбрать следующие опции:
  - поставьте переключатель в положение `Create new key set` (Создать установки для нового секретного ключа)
  - `CSP` (Тип Криптопровайдера) – из выпадающего списка выберите Crypto-Pro GOST R 34.10-2001 KC1 CSP
  - `Key Usage` (Использование ключей) – выбор типа ключа – Signature (для подписи), Exchange (для обмена), Both (для подписи и обмена) – поставьте переключатель в положение Both
  - `Key Size` (Размер ключа) – при выборе алгоритма GOST R 34.10-2001 длина ключа всегда 512
  - поставьте переключатель в положение `User specified key container name`, чтобы задать имя контейнера с секретным ключом
  - в поле `Container name` (Имя контейнера) введите имя контейнера, в котором будет размещен секретный ключ без указания ключевого носителя, выбрать ключевой носитель будет предложено далее. В имени контейнера разрешается использовать латинские буквы и цифры
  - `Mark keys as exportable` – поставьте флажок, чтобы можно было скопировать контейнер с секретным ключом с одного ключевого носителя на другой, а также во время создания инсталляционного файла провести проверку соответствия сертификата пользователя и секретного ключа
  - `Enable strong private key protection` – этот флажок не выставляем
- в разделе **Additional Options** (Дополнительные опции):
  - `Hash Algorithm` – выбрать GOST R34.11-94
  - далее установок никаких делать не нужно.

По этому образцу заполните форму запроса и нажмите кнопку `Submit` (послать запрос):

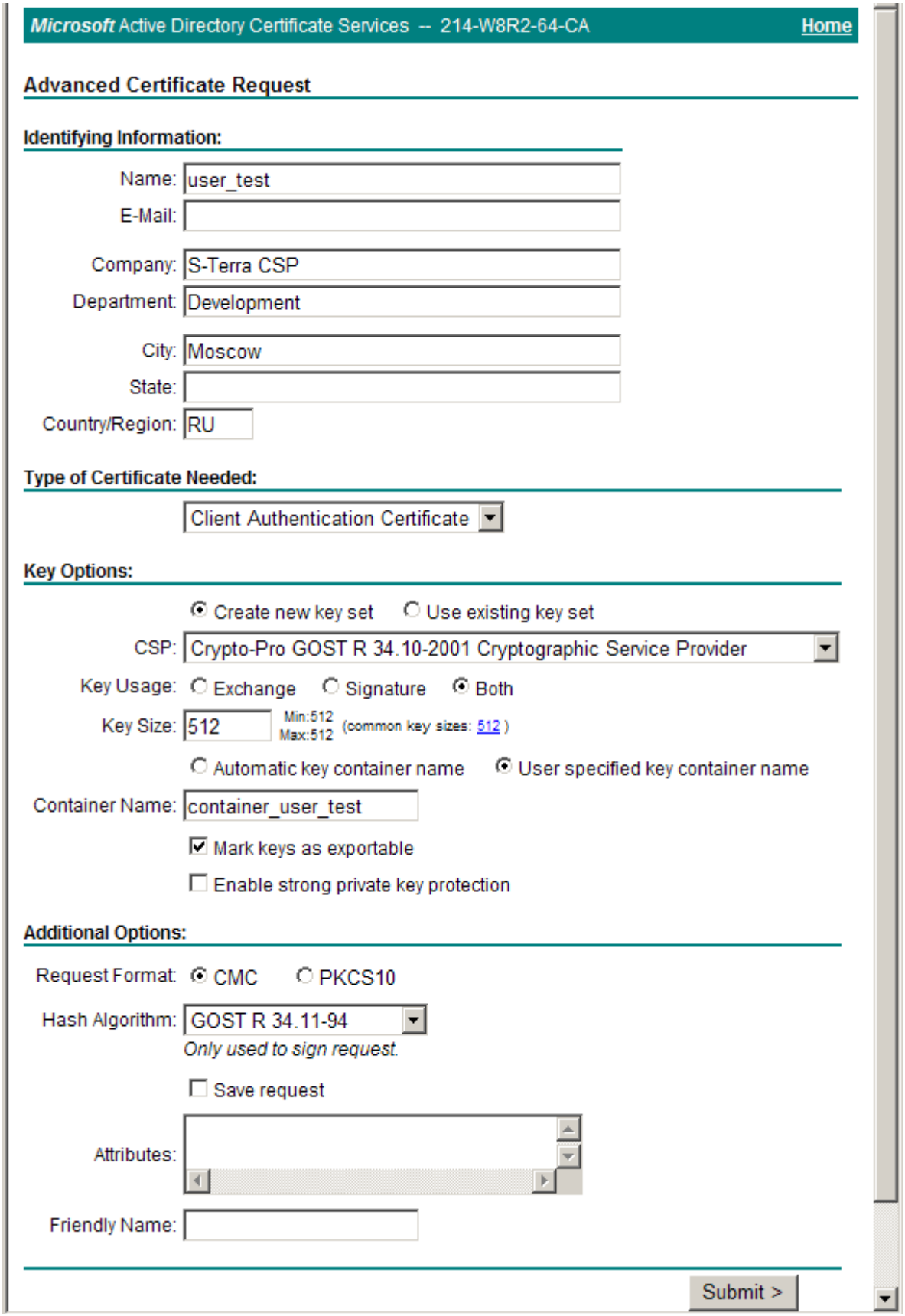

Microsoft Active Directory Certificate Services -- 214-W8R2-64-CA
Home
Advanced Certificate Request
Identifying Information:
Name: user_test
E-Mail:
Company: S-Terra CSP
Department: Development
City: Moscow
State:
Country/Region: RU
Type of Certificate Needed:
Client Authentication Certificate
Key Options:
Create new key set
Use existing key set
CSP: Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider
Key Usage: Exchange Signature Both
Key Size: 512 Min:512 Max:512 (common key sizes: 512)
Automatic key container name
User specified key container name
Container Name: container_user_test
Mark keys as exportable
Enable strong private key protection
Additional Options:
Request Format: CMC PKCS10
Hash Algorithm: GOST R 34.11-94
Only used to sign request.
Save request
Attributes:
Friendly Name:
Submit >

Рисунок 152

Шаг 8: появляется предупреждение (Рисунок 153), нажмите кнопку `Yes`, чтобы продолжить:

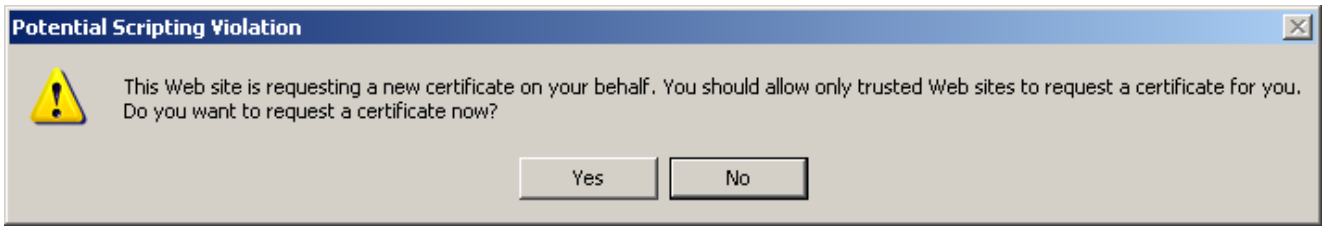


Рисунок 153

Шаг 9: выберите ключевой носитель, в котором будет размещен контейнер с секретным ключом, например, Реестр, и нажмите `OK`. В целях безопасности контейнер с секретным ключом лучше размещать на внешнем носителе (eToken), который будет храниться только у пользователя.

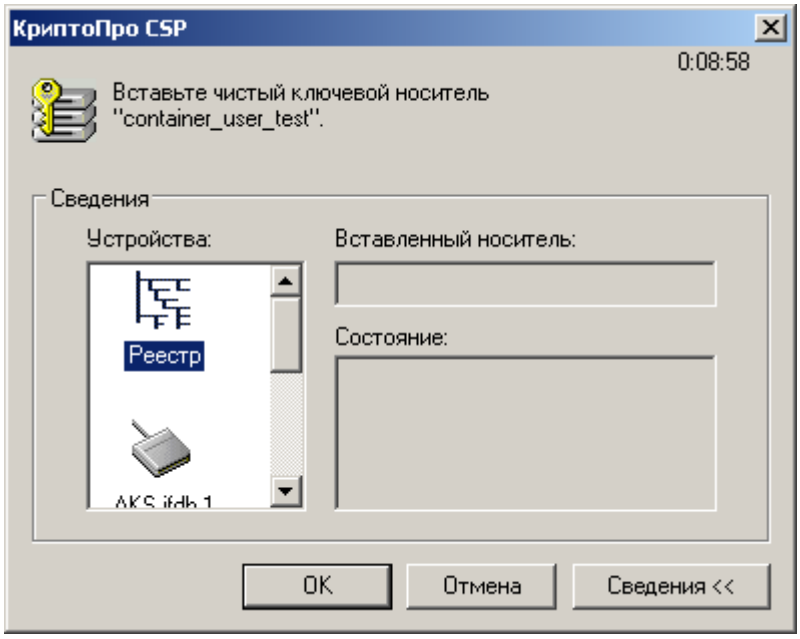


Рисунок 154

Шаг 10: для создания ключевой пары в режиме КС1 появляется окно для биологической инициализации ДСЧ – нажмите любые клавиши или подвигайте мышкой: В режиме КС2 такое окно не появляется.:

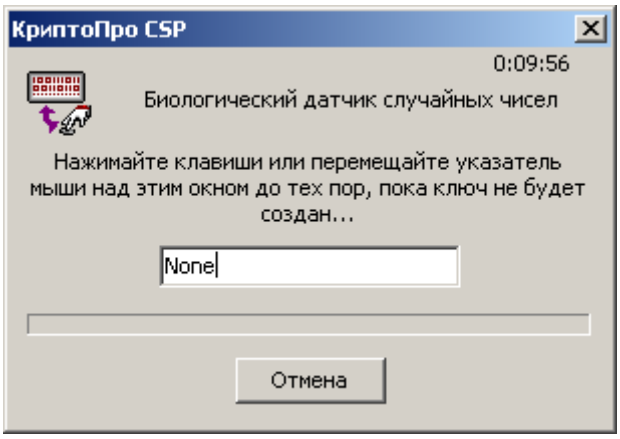


Рисунок 155

 Copyright © S-Terra CSP 2003 - 2015

Шаг 11: задайте пароль на контейнер с секретным ключом и нажмите ОК:

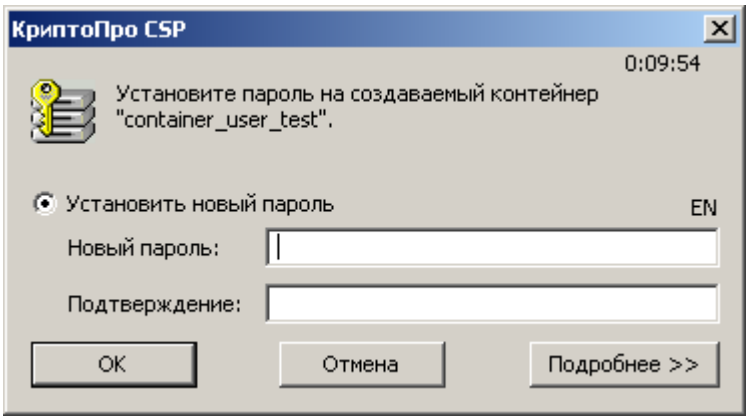


Рисунок 156

Таким образом, ключевая пара – открытый и секретный ключи созданы. Секретный ключ размещен в контейнере в ключевом носителе Реестр на компьютере пользователя и защищен паролем. А на основе открытого ключа Удостоверяющий Центр создаст сертификат пользователя.

Удостоверяющий Центр сразу создал сертификат пользователя и прислал об этом уведомление. При выборе предложения `Install this certificate` сертификат пользователя будет получен из Удостоверяющего Центра и размещен в контейнере с секретным ключом, в нашем примере – в Реестре.

Шаг 12: Удостоверяющий Центр сразу издал сертификат пользователя и прислал об этом уведомление (Рисунок 157). Выберите предложение "`Install this certificate`", чтобы получить сертификат пользователя из Удостоверяющего Центра и разместить его в контейнере с секретным ключом.

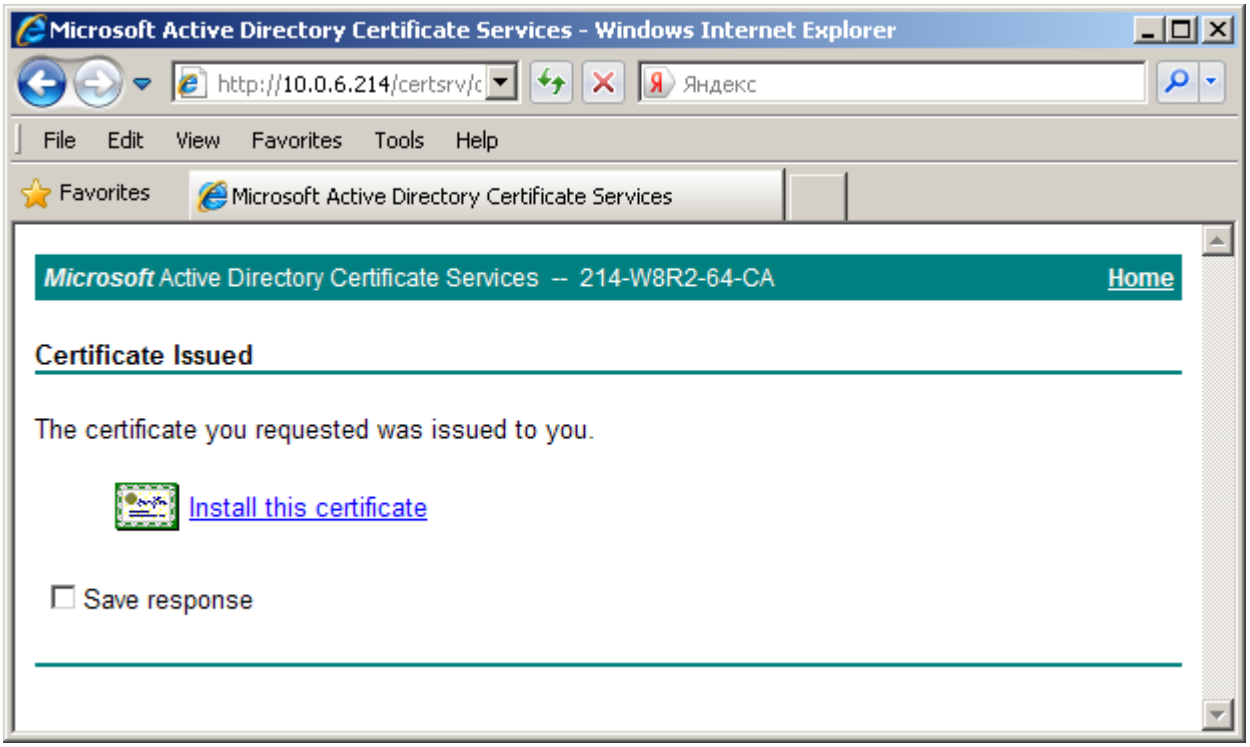


Рисунок 157

 Copyright © S-Terra CSP 2003 - 2015

Шаг 13: появляется предупреждение (Рисунок 158), нажмите кнопку Yes, чтобы продолжить:

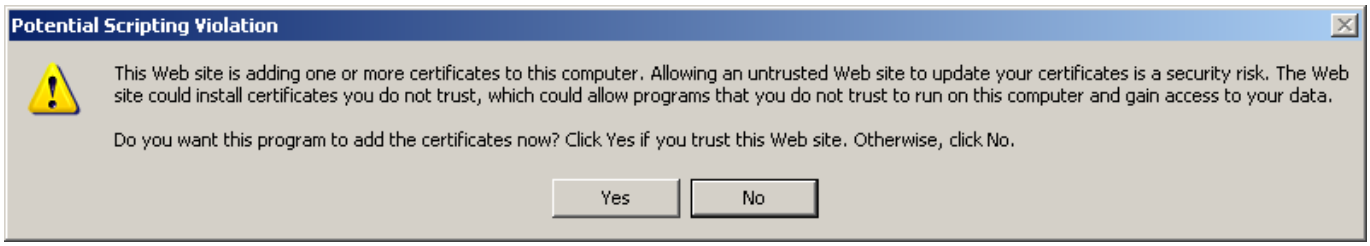


Рисунок 158

Шаг 14: еще раз введите пароль на контейнер с секретным ключом и нажмите ОК (Рисунок 159):

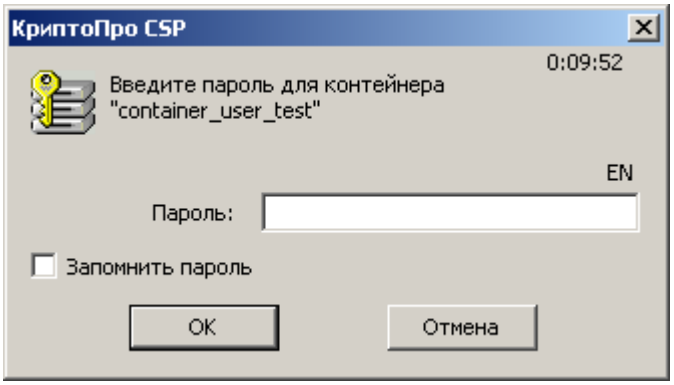


Рисунок 159

Выдается сообщение, что сертификат пользователя успешно размещен в контейнере с секретным ключом (Рисунок 160).

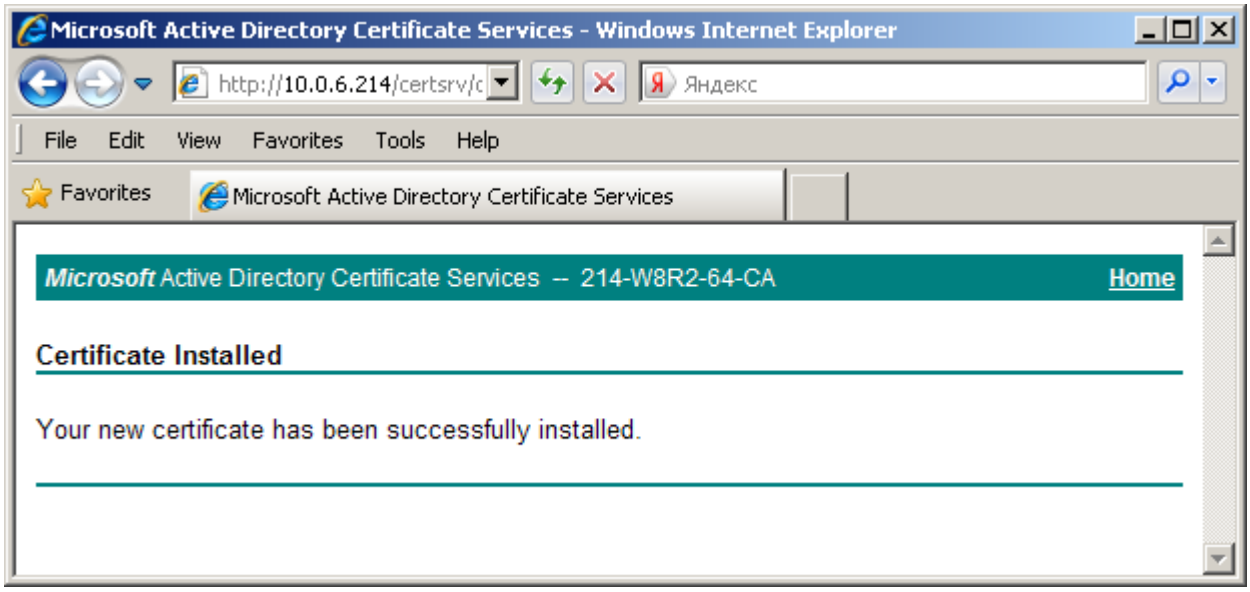


Рисунок 160

Сертификат пользователя можно получить из Удостоверяющего Центра и другими путями, но описанный здесь наиболее удобен.

В контексте безопасности компьютера, пользователь не может запрашивать сертификат компьютера через интернет с использованием обозревателя Internet Explorer. Поэтому, чтобы получить контейнер с сертификатом для компьютера, необходимо скопировать контейнер с локальным сертификатом, который был

получен из Удостоверяющего центра в контейнер компьютера. Эти действия выполняются при помощи продукта «КриптоПро CSP» и описаны ниже.

Копирование контейнера

Для копирования контейнера с локальным сертификатом пользователя в контейнер компьютера выполните следующие действия:

Шаг 1: запустите продукт "КриптоПро CSP".

Шаг 2: войдите во вкладку Сервис и нажмите кнопку Скопировать контейнер…

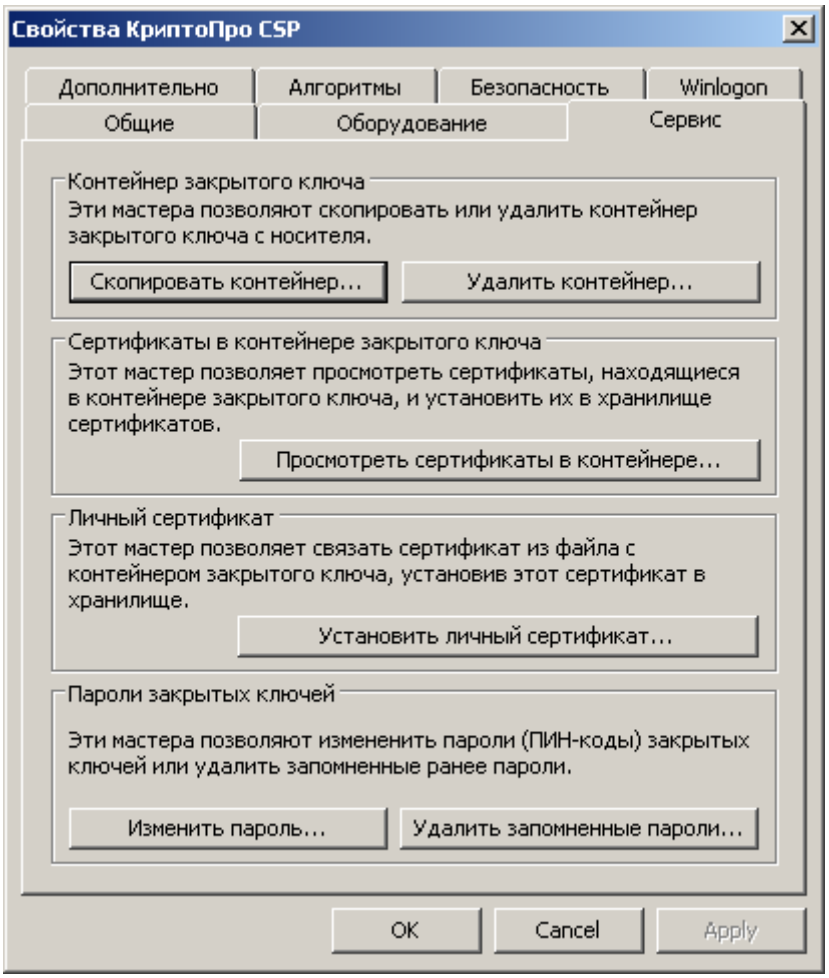


Рисунок 161

Шаг 3: в следующем окне для указания контейнера поставьте переключатель в положение `ключевой контейнер Пользователя` и нажмите кнопку `Обзор…`

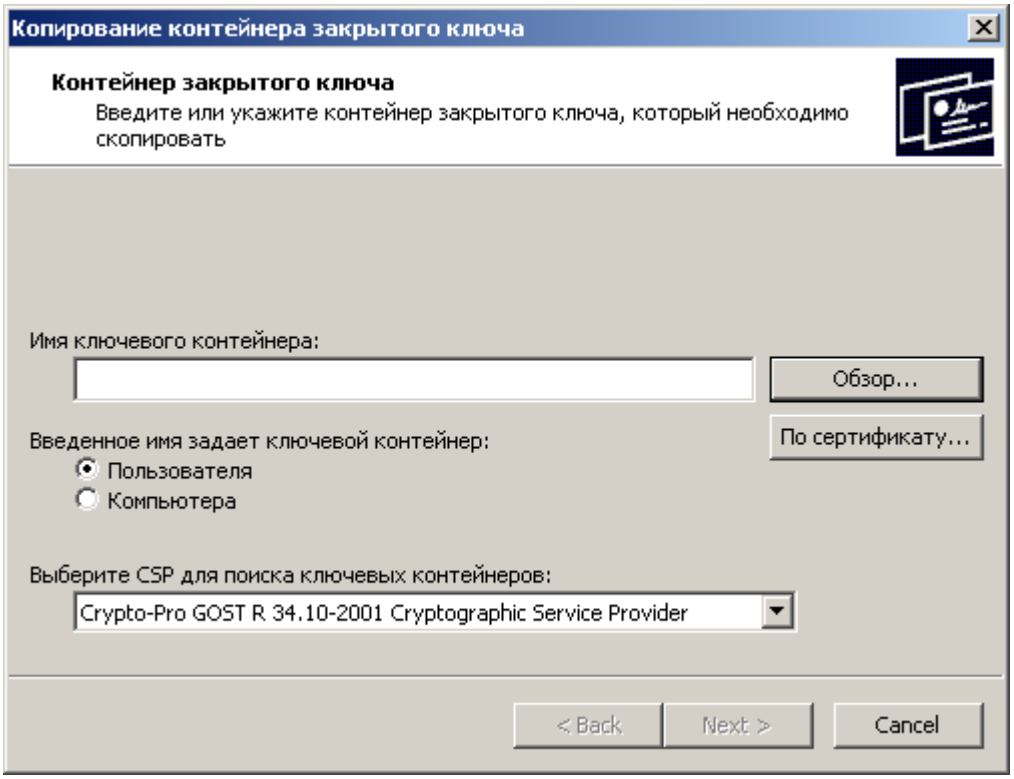


Рисунок 162

Шаг 4: поставьте переключатель в положение `Уникальные имена` и выберите контейнер с локальным сертификатом, который был получен из Удостоверяющего центра.

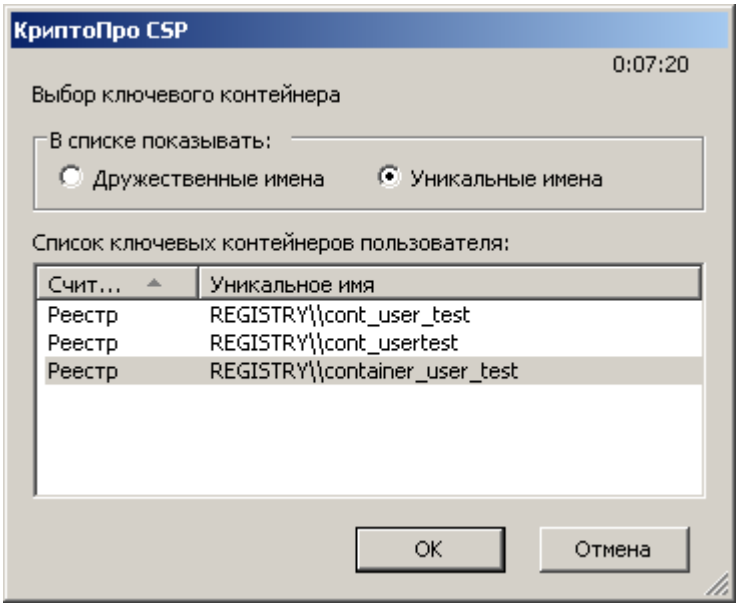


Рисунок 163

 Copyright © S-Terra CSP 2003 - 2015

Шаг 5: поставьте переключатель в положение `ключевой контейнер Пользователя` и нажмите `Next`.

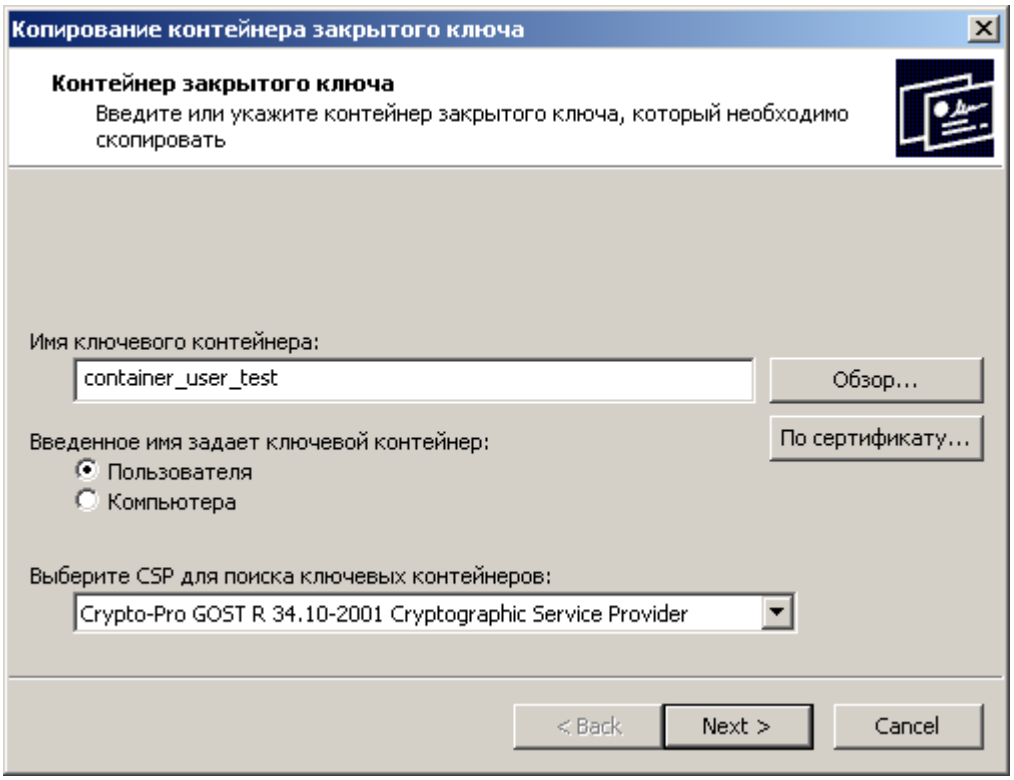


Рисунок 164

Шаг 6: задайте имя ключевого контейнера, на который будет выполняться копирование, поставьте переключатель в положение `Ключевой контейнер Компьютера` и нажмите кнопку `Finish`.

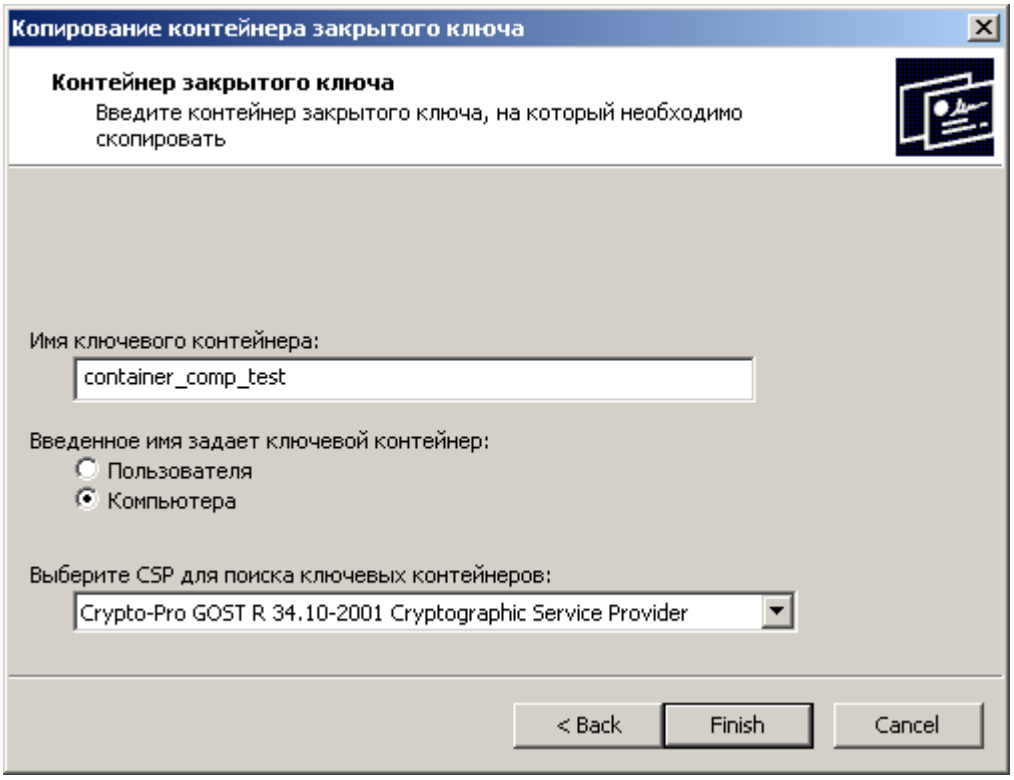


Рисунок 165

 Copyright © S-Terra CSP 2003 - 2015

Шаг 7: выберите ключевой носитель, например Реестр, для размещения контейнера с секретным ключом и нажмите OK.

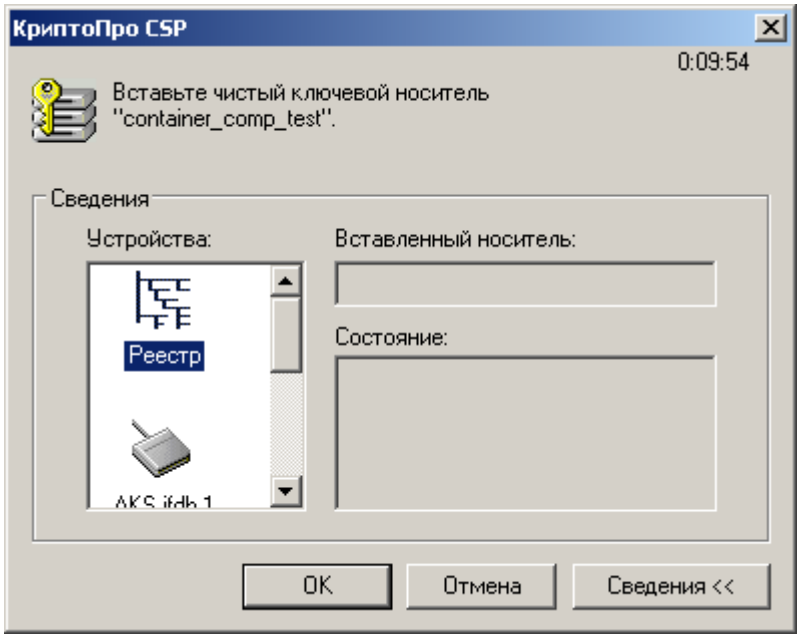


Рисунок 166

Шаг 8: установите пароль на создаваемый контейнер и нажмите OK.

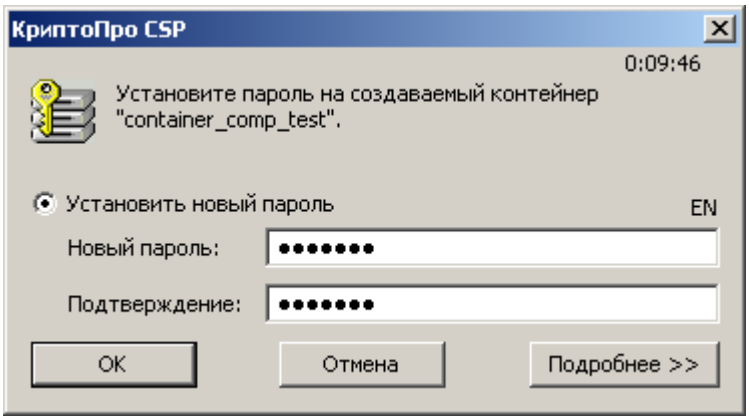


Рисунок 167

Для создания инсталляционного файла пользователя требуется экспортировать сертификат пользователя из контейнера в файл, поэтому перейдите к следующему разделу.

 Copyright © S-Terra CSP 2003 - 2015

22.6.7. Экспортирование сертификата пользователя в файл

На компьютере пользователя в ключевом носителе Реестр находится контейнер, , который содержит сертификат пользователя и секретный ключ этого сертификата. Для экспортирования сертификата в файл выполните следующие действия:

Шаг 1: запустите продукт "КриптоПро CSP 3.6/3.6R2" – `Пуск – Настройка – Панель управления – КриптоПро CSP`

Шаг 2: войдите во вкладку Сервис и нажмите кнопку `Просмотреть сертификаты в контейнере…`

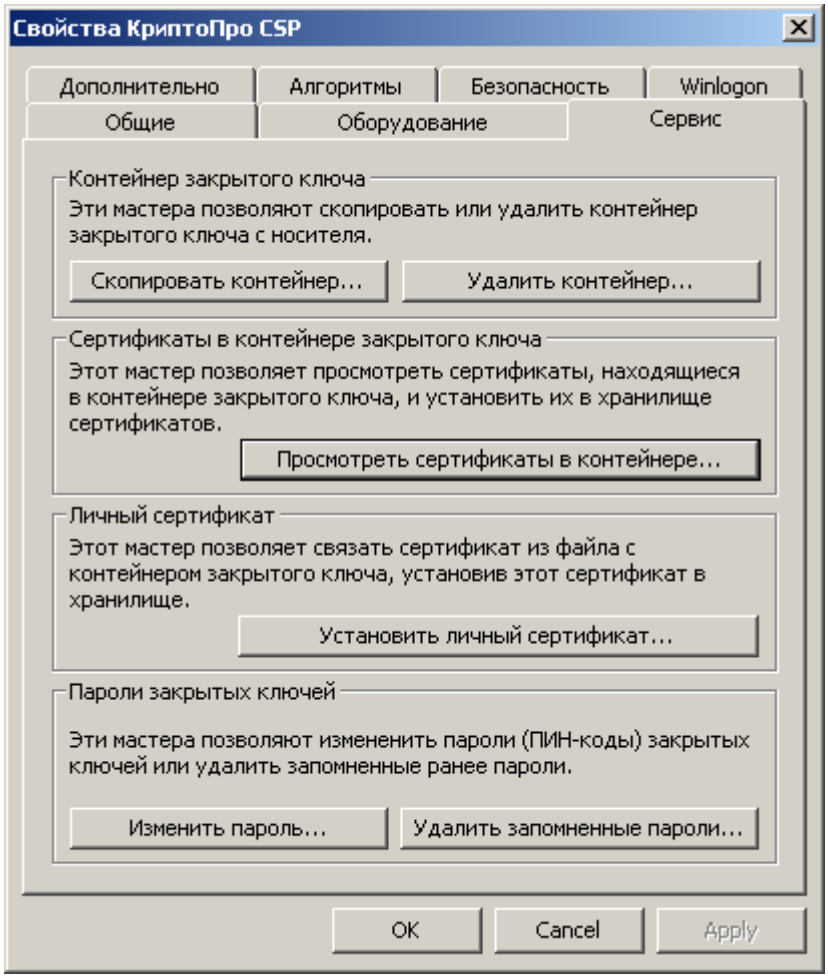


Рисунок 168

 Copyright © S-Terra CSP 2003 - 2015

Шаг 3: для указания контейнера поставьте переключатель в положение `Компьютера` и нажмите кнопку `Обзор`…

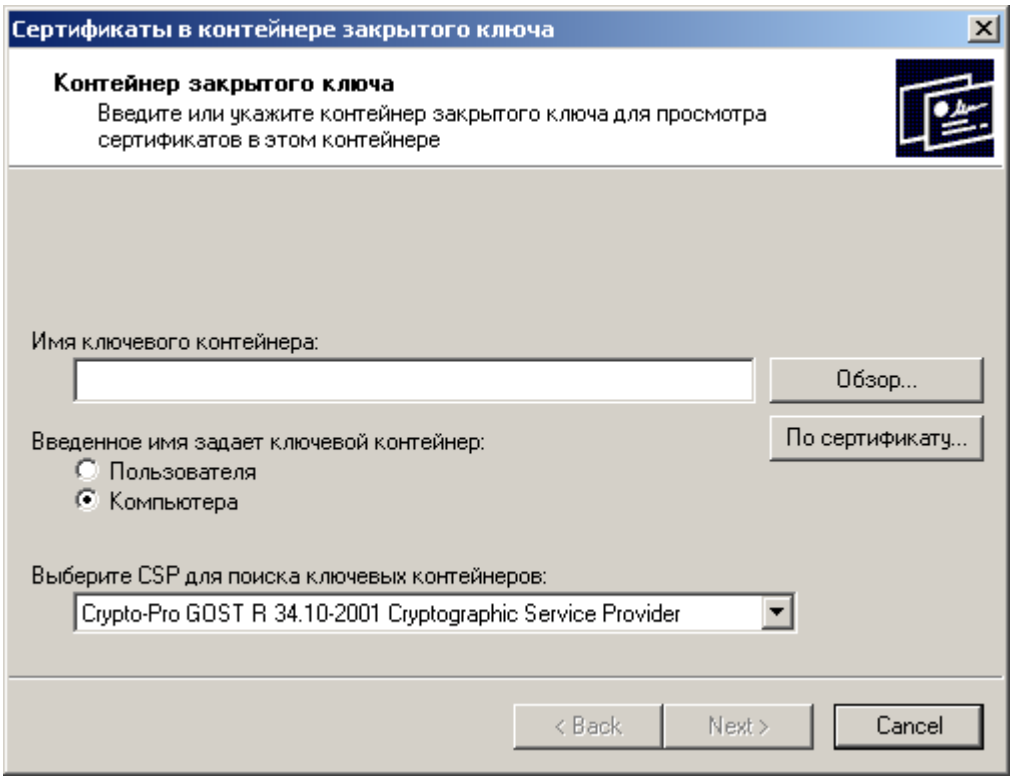


Рисунок 169

Шаг 4: в окне со списком контейнеров, размещенных в Реестре, поставьте переключатель в положение Уникальные имена и выберите контейнер, в котором лежит секретный ключ и сертификат пользователя (Рисунок 170). Нажмите кнопку `OK`:

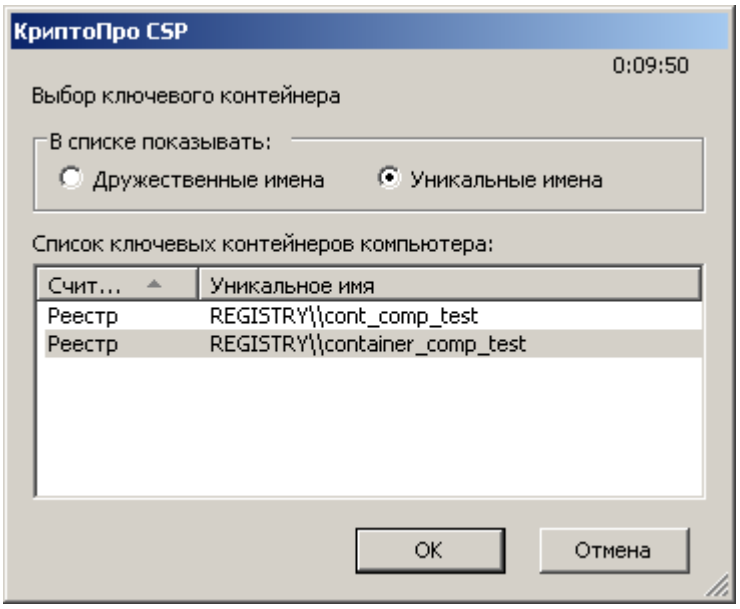


Рисунок 170

 Copyright © S-Terra CSP 2003 - 2015

Шаг 5: выбор контейнера произведен, нажмите кнопку `Next`:

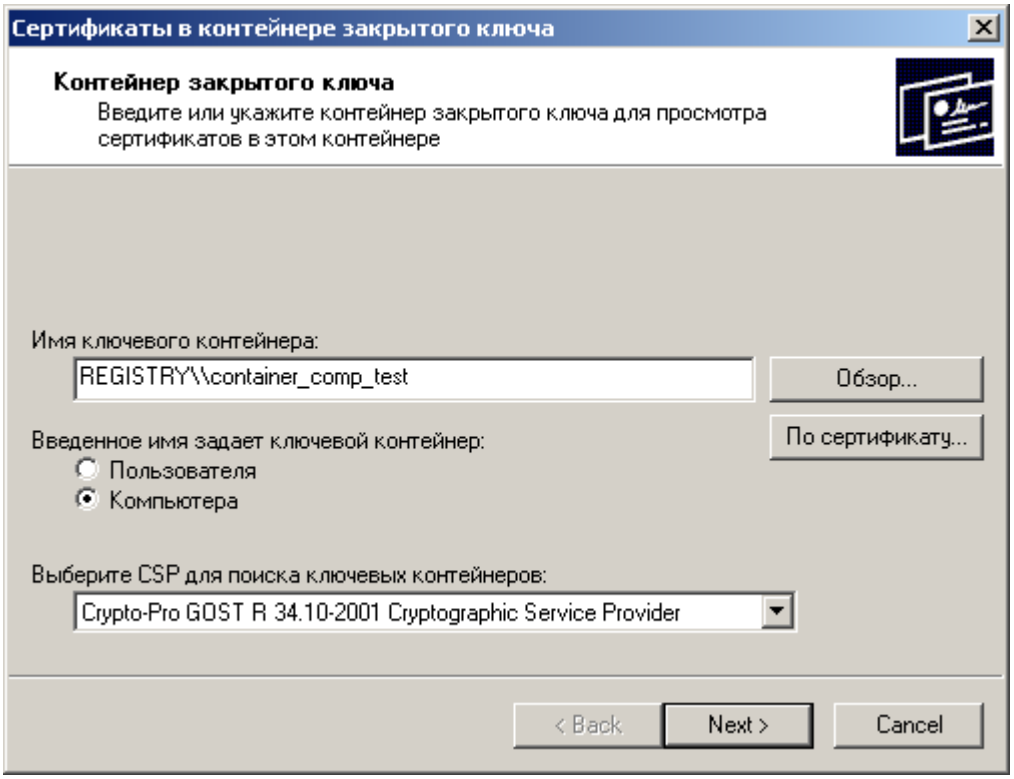


Рисунок 171

Шаг 6: следующее окно показывает поля сертификата пользователя, нажмите кнопку `Свойства`:

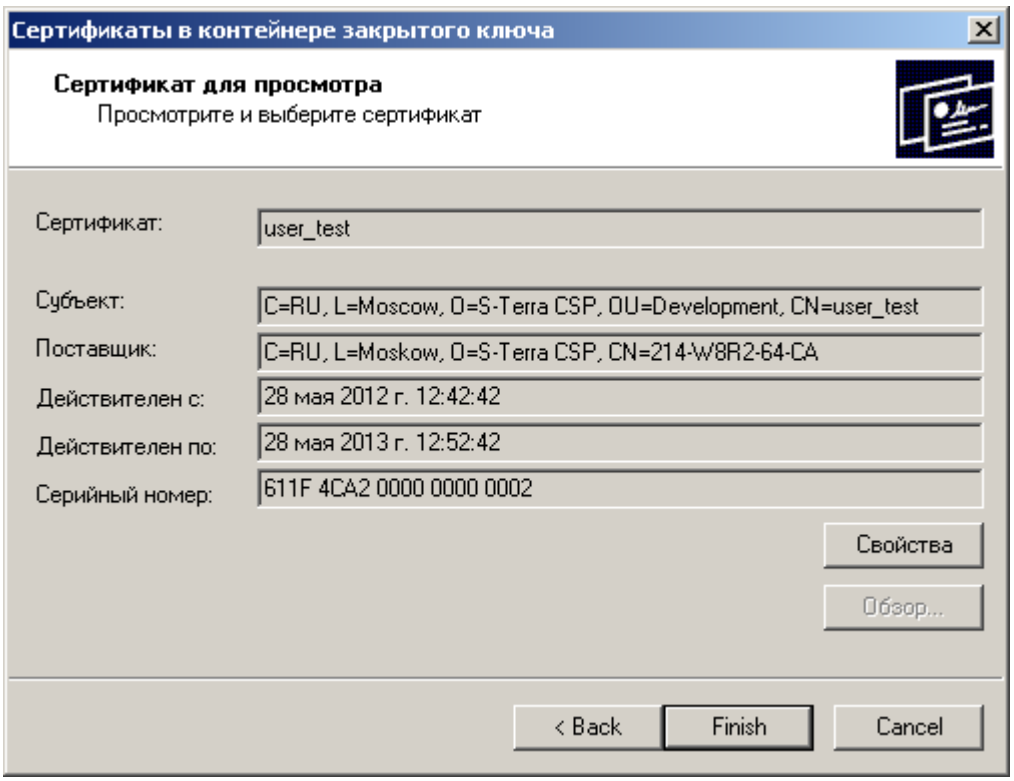


Рисунок 172

Шаг 7: выберите вкладку Detail и нажмите кнопку `Copy to File…`

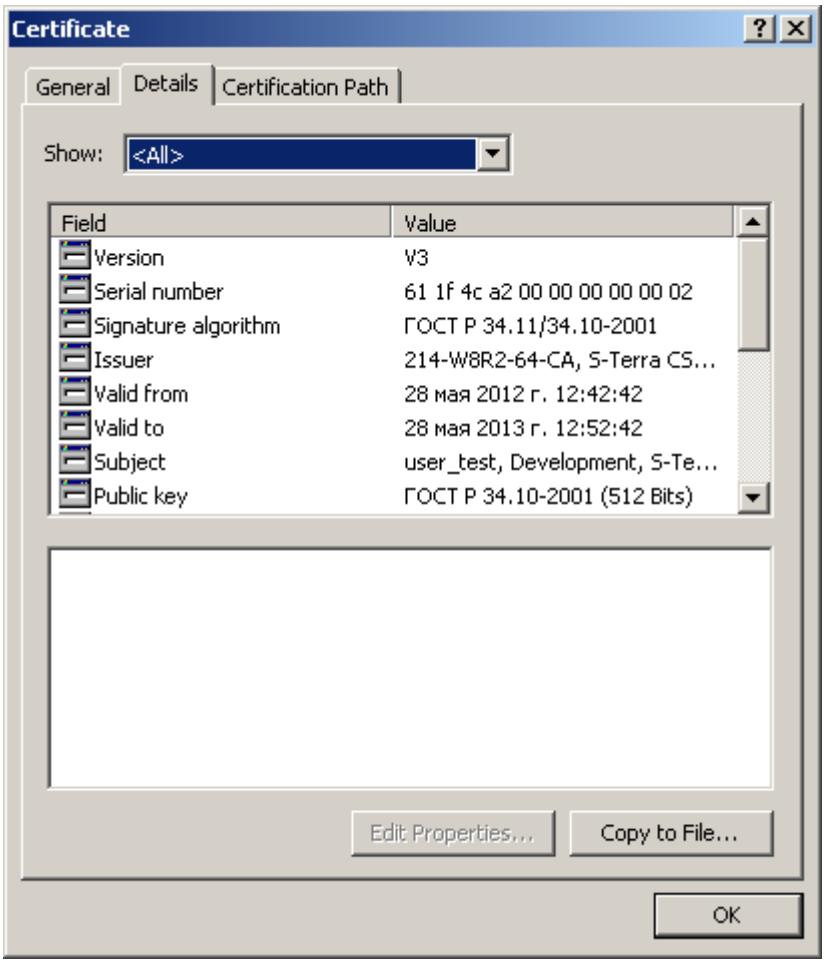


Рисунок 173

Шаг 8: в окне визарда нажмите кнопку `Next`:



Рисунок 174

 Copyright © S-Terra CSP 2003 - 2015

Шаг 9: установите переключатель во второе положение, чтобы экспортировать в файл только сертификат без секретногс ключа и нажмите `Next`:

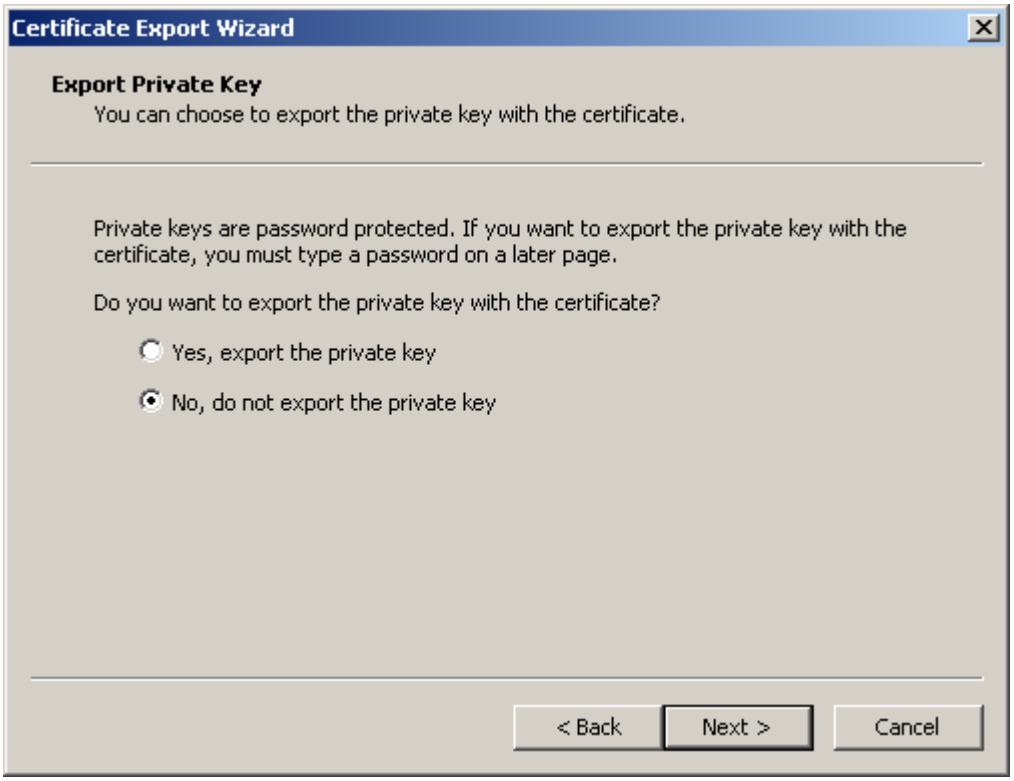


Рисунок 175

Шаг 10: выберите формат файла сертификата – `DER encoded binary X.509 (.CER) и нажмите Next`:

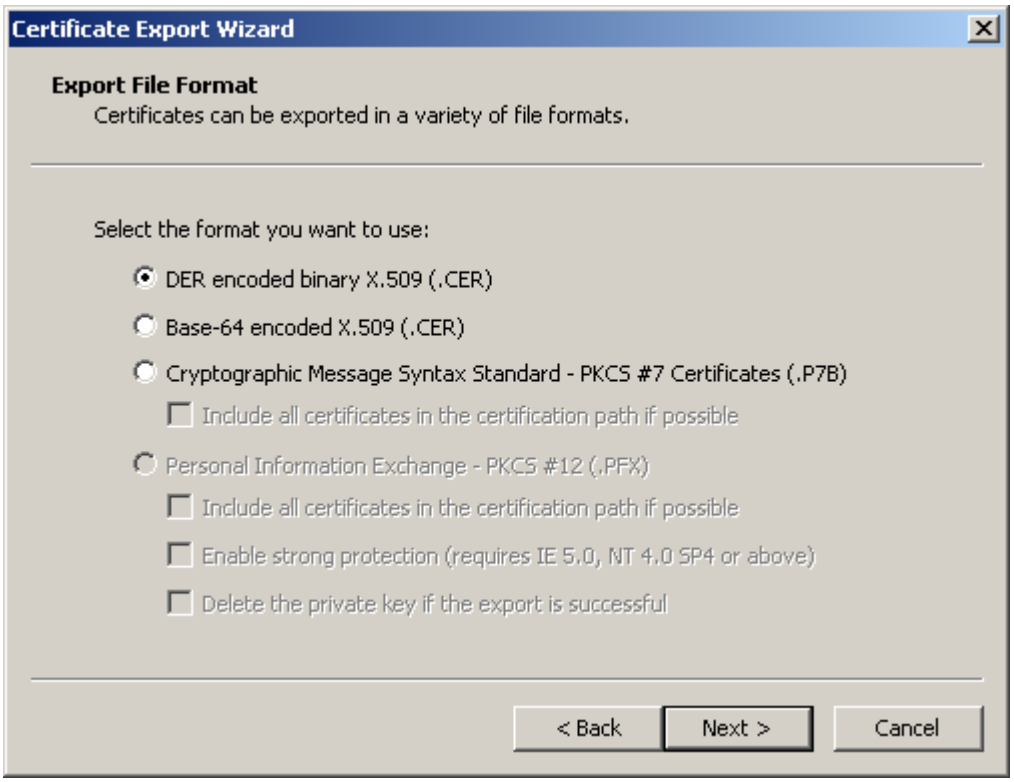


Рисунок 176

 Copyright © S-Terra CSP 2003 - 2015

Шаг 11: укажите имя файла, в который экспортируется сертификат, и нажмите `Next`:

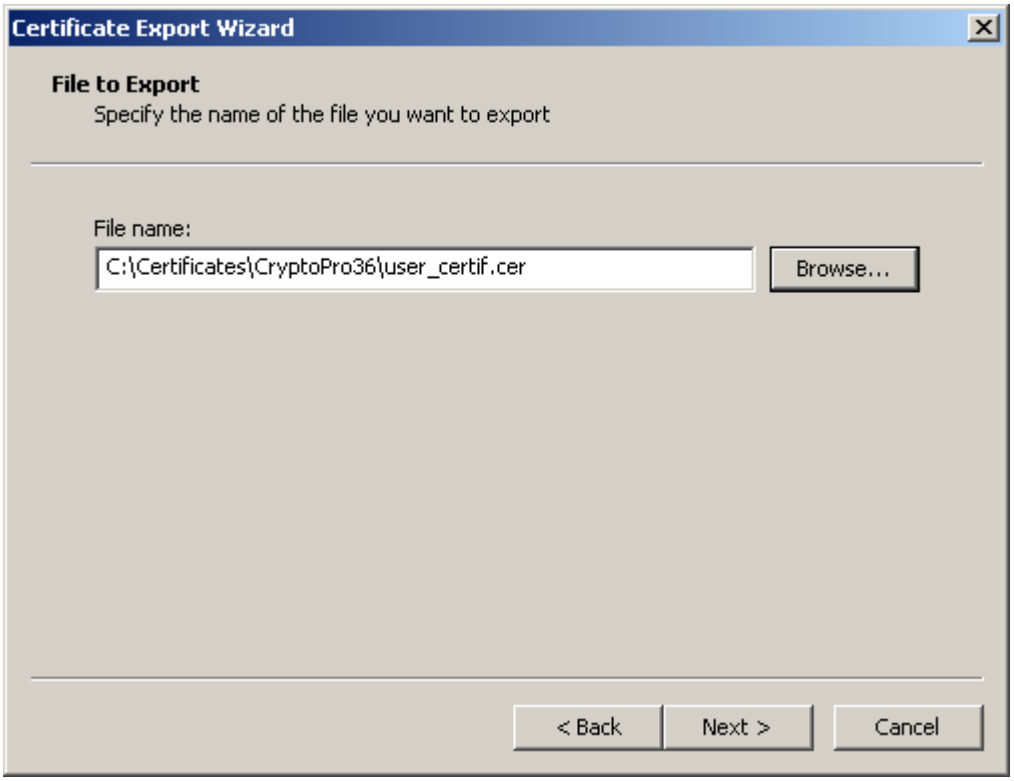


Рисунок 177

Шаг 12: экспортирование сертификата пользователя в файл закончено, нажмите `Finish`.



Рисунок 178

На этом создание сертификата пользователя и CA сертификата закончено, они оба экспортированы в файлы.

 Copyright © S-Terra CSP 2003 - 2015