127 018, Москва, Улица Образцова, 38
Телефон: (495) 780 4820
Факс: (495) 780 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТО ПРО

Средство Сетевой Аутентификации

КриптоПро Winlogon

Описание и сценарии использования

ЖТЯИ.00032-01 90 01

Листов 11

2005 г.

© ООО "Крипто-Про", 2000-2005. Все права защищены.

Авторские права на средство сетевой аутентификации КриптоПро Winlogon и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Свидетельство об официальной регистрации программ для ЭВМ № 2001610275 от 14 марта 2001 года.

Документ входит в комплект поставки программного обеспечения КриптоПро Winlogon, и на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "Крипто-Про" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

1. Аннотация

Настоящий документ содержит описание и варианты использования средства сетевой аутентификации КриптоПро Winlogon.

КриптоПро Winlogon предназначен для аутентификации пользователей в домене Microsoft Windows с использованием Enterprise CA, КриптоПро УЦ или других совместимых центров сертификации.

2. Аутентификация по протоколу Kerberos в Microsoft® Windows®

В операционной системе Microsoft® Windows® 2000/XP/2003 аутентификация пользователей в домене производится по умолчанию с помощью протокола Kerberos. Использование этого стандарта создает надежную основу для взаимодействия между различными платформами и при этом значительно повышает безопасность сетевой аутентификации.

В Windows 2000/XP/2003 применяется протокол Kerberos версии 5, дополненный расширениями, связанными с инфраструктурой открытых ключей. Безопасность системы обеспечивает клиент Kerberos с помощью интерфейса Security Support Provider Interface. Первоначальная проверка пользователя производится в рамках процесса Winlogon, которая обеспечивает единую регистрацию пользователей в системе. Центр распределения ключей Key Distribution Center (KDC) Kerberos интегрирован с другими службами безопасности Windows 2000/2003, установленными на контроллере домена. Учетные записи безопасности хранятся в базе данных службы каталогов Active Directory.

Существует расширение протокола Kerberos версии 5, предложенное IETF. Это расширение под названием PKINIT позволяет использовать сертификат открытого ключа вместо пароля в процессе начальной аутентификации. Расширение PKINIT в Windows является основой для доступа с помощью смарт-карты.

КриптоПро Winlogon добавляет в PKINIT поддержку российских криптографических алгоритмов.

Несколько упрощая, можно сказать, что процесс аутентификации по протоколу Kerberos работает по принципу проверки и передачи учетных данных между клиентами и серверами. Вот как это происходит. Когда пользователь входит в домен Windows 2000/2003, операционная система находит сервер Active Directory и службу аутентификации Kerberos и передает ей учетные данные клиента. Для этого формируется запрос в специальном формате, часть которого зашифровывается с помощью ключа, полученного из введенного пользователем пароля.

Служба KDC (Key Distribution Center) Kerberos, называемая службой распространения ключей после проверки данных клиента, необходимых для подтверждения подлинности, выдает пользователю билет TGT (Ticket-Granting Ticket). Этот билет затем используется для идентификации клиента, когда он запрашивает последующие билеты Kerberos для получения доступа к сетевым ресурсам. Хотя это сложный процесс, участие пользователя заключается лишь во введении пароля при входе.

На приведенном ниже рис. 1 показано взаимоотношения между клиентом, центром KDC и сервером ресурсов, использующими протокол аутентификации Kerberos.

Рис. 1. Процесс аутентификации по протоколу Kerberos

Аутентификация с помощью смарт-карты

При регистрации с помощью смарт-карт используется пара, состоящая из личного и открытого ключей, которая хранится в памяти смарт-карты. Расширение протокола Kerberos, определяющее порядок применения открытых ключей при обмене по подпротоколу AS Exchange, предусматривает следующий порядок использования такой пары.

Открытая ее часть служит для шифрования сеансового ключа пользователя службой KDC, а личная – для расшифрования этого ключа клиентом.

Регистрация начинается с того, что пользователь вставляет свою смарт-карту в специальное считывающее устройство, подключенное к компьютеру. При соответствующей конфигурации Windows это равносильно сигналу SAS, то есть, одновременному нажатию клавиш CTRL+ALT+DEL. В ответ Winlogon направляет на настольную систему, динамически подключаемую библиотеку MSGINA, которая выводит на экран стандартное диалоговое окно регистрации. Правда, теперь пользователю нужно ввести только один параметр – персональный идентификационный номер PIN (Personal Identification Number).

Kerberos SSP клиентского компьютера направляет в службу KDC сообщение KRB_AS_REQ – первоначальный запрос на аутентификацию. В поле данных предварительной аутентификации этого запроса включается сертификат открытого ключа пользователя. KDC проверяет подлинность сертификата и извлекает из него открытый ключ, которым шифрует ключ сеанса регистрации. После этого он включает этот ключ вместе с билетом TGT в сообщение KRB_AS_REP и направляет его клиенту. Расшифровать сеансовый ключ сможет только тот клиент, у которого есть секретная половина криптографической пары, функции которой на этом заканчиваются. Вся дальнейшая связь между клиентом и службой KDC поддерживается на основе сеансового ключа. Никаких других отклонений от стандартного процесса регистрации и вхождения в сеть не требуется.

По умолчанию поставщик Kerberos, работающий на клиентском компьютере, в качестве данных предварительной аутентификации направляет в службу KDC зашифрованную метку времени. На системах же, конфигурация которых предусматривает регистрацию с применением смарт-карты, роль данных предварительной аутентификации отводится сертификату открытого ключа.

2.2. Поддерживаемые КриптоПро Winlogon ключевые носители

КриптоПро Winlogon Клиент поддерживает следующие типы смарт-карт:

- российские интеллектуальные карты (РИК1, Оскар) с использованием считывателей смарт-карт, поддерживающий протокол PS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126 и др.);
- электронный ключ с интерфейсом USB;

КриптоПро Winlogon KDC для хранения секретного ключа KDC может использовать любой ключевой носитель, поддерживаемый КриптоПро CSP.

3. Сценарии использования КриптоПро Winlogon в программном обеспечении Microsoft

3.1. Использование КриптоПро Winlogon для интерактивной регистрации в домене Microsoft Windows 2003 Server

Использование КриптоПро Winlogon для интерактивной регистрации пользователей в домене Microsoft Windows обеспечивает аутентификацию пользователей на российских криптографических алгоритмах ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94.

При успешном прохождении процесса регистрации пользователь вместе с билетом TGT получает данные авторизации. Аутентифицированный и авторизованный пользователь получает доступ к разрешенным сервисам и серверам домена. Например, для доступа к локальному компьютеру домена, общим папкам других пользователей, серверу MS Exchange, ISA серверу без дополнительной аутентификации.

Возможная конфигурация изображена на рисунке 2.

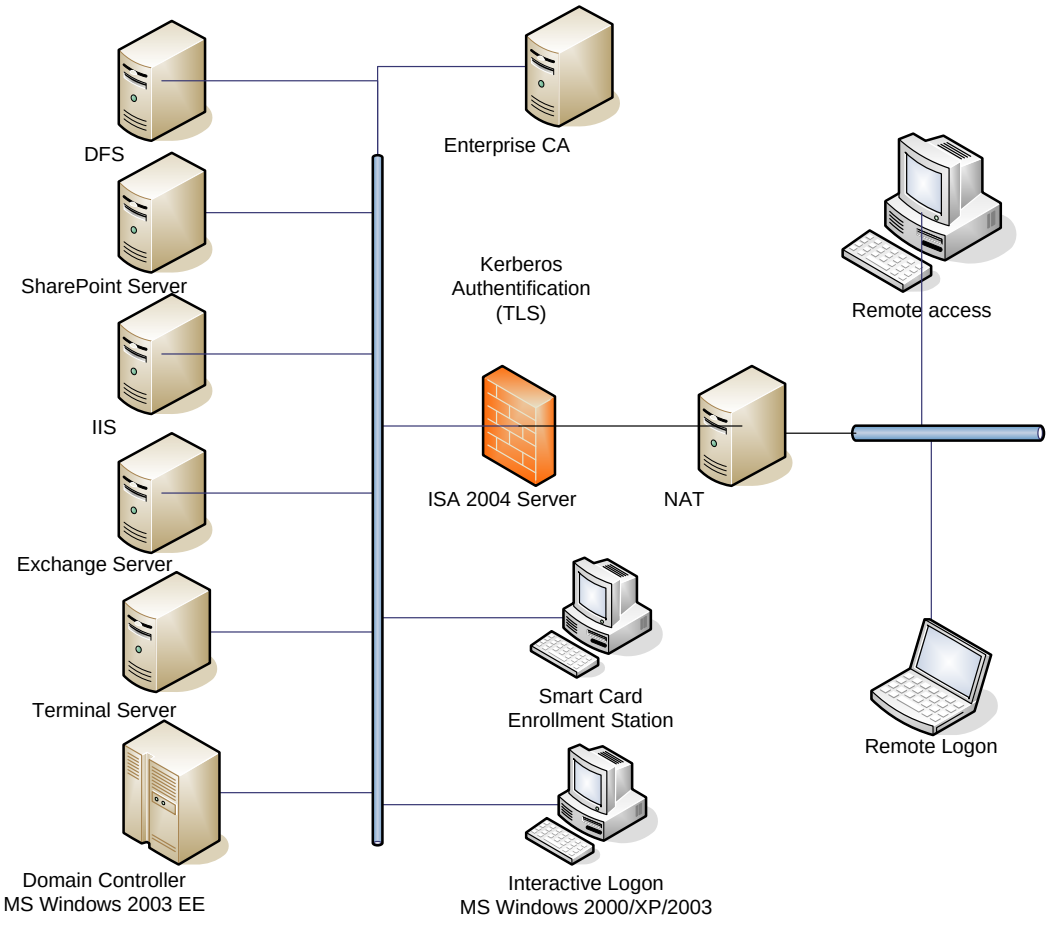
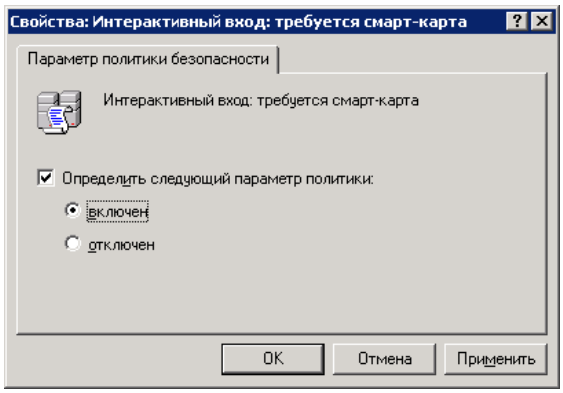


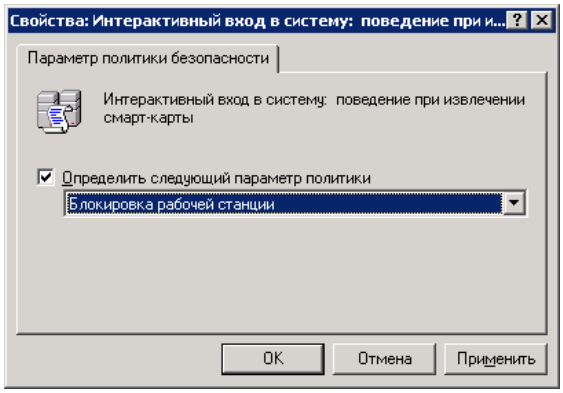
Рис. 2. Возможная конфигурация защищенного домена

3.1.1.Настройка контроллера домена

Настройка контроллера домена описана в документе «Установка и развертывание КриптоПро Winlogon».

Дополнительно можно установить или запретить вход в домен по паролю, установив параметр доменной политики «Интерактивный вход: требуется смарт-карта» и действие при извлечении смарт-карты: «Интерактивный вход: поведение при извлечении смарт-карты».





3.1.2.Настройка Центра Сертификации

Настройка центра сертификации (Enterprise CA) описана в документе «Установка и развертывание КриптоПро Winlogon».

Дополнительно необходимо обеспечить требуемую периодичность выпуска и публикации CRL, а также доступность CRL клиентам. CRL должен быть доступен **без аутентификации** в домене.

При отзыве сертификатов пользователя и публикации соответствующего CRL пользователь не сможет аутентифицироваться в домене по ранее выданной смарт-карте.

Примечание. Для использования шаблонов сертификатов для MS Enterprise CA, в которых жестко заданы криптопровайдеры и размеры ключей, совместно с криптопровайдерами КриптоПро необходимо редактирование Active Directory. Это можно сделать либо вручную (например, с помощью ADSI Edit – входит в Support Tools), либо с помощью скрипта, например, такого:

```
Dim oRoot,strConfigurationRoot, oDCTemplate

Set oRoot = GetObject("LDAP://RootDSE")

strConfigurationRoot = oRoot.Get("configurationNamingContext")

Set oRoot = GetObject("LDAP://" & strConfigurationRoot)

Set oDCTemplate = oRoot.GetObject ("pKICertificateTemplate", "CN=User, CN=Certificate Templates, CN=Public Key Services, CN=Services")

oDCTemplate.PKIDefaultCSPs = " "

oDCTemplate.SetInfo
```

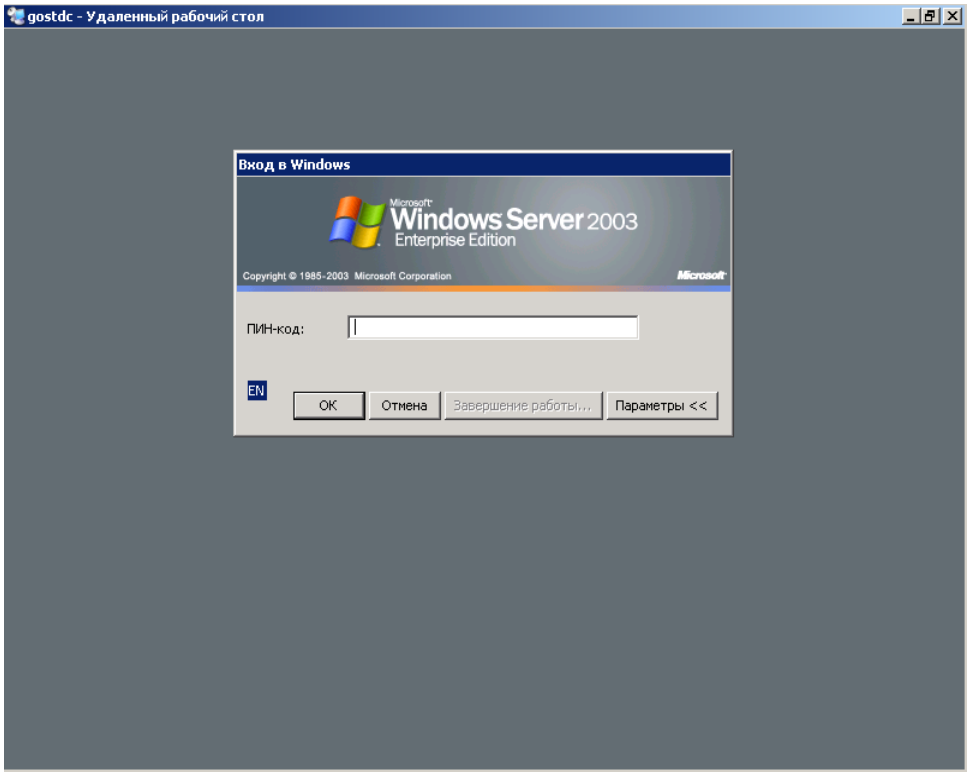
Для выполнения необходимы права администратора домена.

Также можно воспользоваться утилитой Template Editor, устанавливаемой при инсталляции КриптоПро Winlogon на контроллер

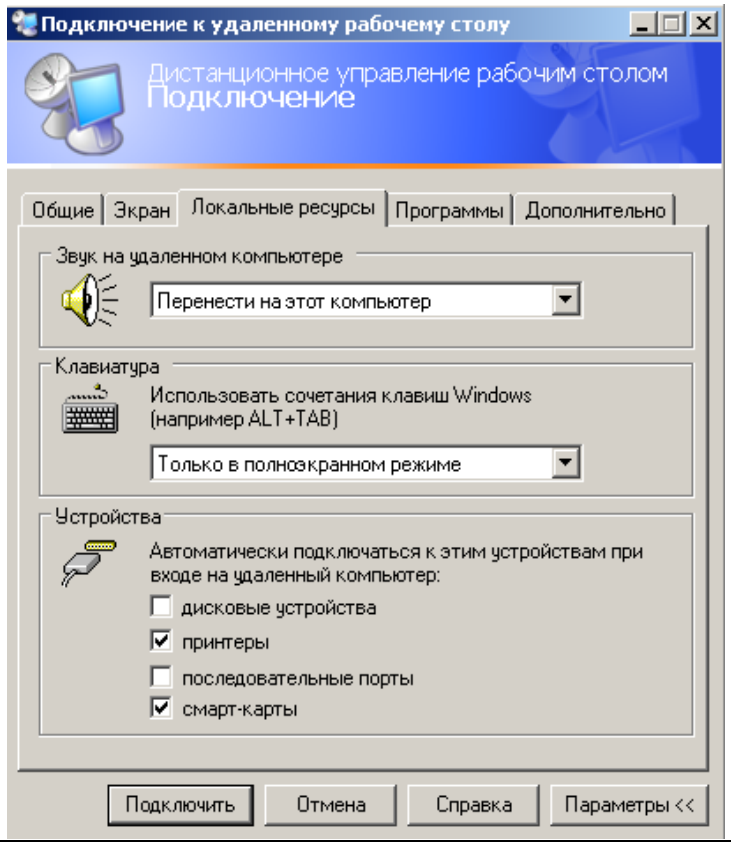
домена и доступной из меню Пуск->Программы->Крипто-Про.

3.1.3.Настройка сервера терминалов

Сервер терминалов, входящий в домен, не требует дополнительной настройки. Клиенты сервера терминалов смогут аутентифицироваться на нем при наличии соответствующего ПО (например, клиент Remote Desktop, входящий в поставку Windows XP/2003).



Для этого в свойствах клиента необходимо задействовать подключение к смарт-картам клиентской машины.



Также на сервере терминалов должен быть установлен КриптоПро Winlogon и в КриптоПро CSP добавлена поддержка клиентских считывателей и смарт-карт.

Примечание. Для корректной работы сервера терминалов необходимо использовать вариант исполнения КриптоПро CSP КС1.

Примечание. Сервер терминалов Microsoft Windows 2003 Service Pack 1 поддерживает подключение терминальных клиентов с использование протокола TLS

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/BookofSP1/2284b19b-30a6-42b5-9bd1-ff301f7248b0.mspx

http://support.microsoft.com/default.aspx?scid=kb;en-us;895433

При этом ключ сервера должен быть создан (установлен) криптопровайдером Crypto-Pro SmartCard CSP

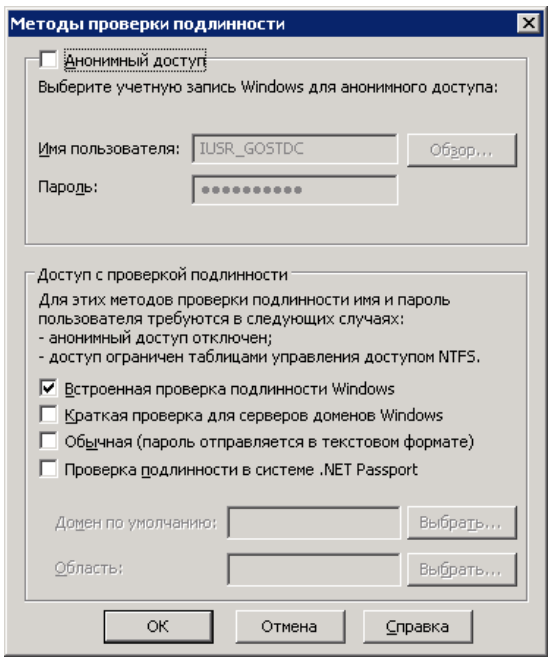
3.1.4.Настройка станции выпуска смарт-карт.

Настройка станции выпуска смарт-карт описана в документе «Установка и развертывание КриптоПро Winlogon».

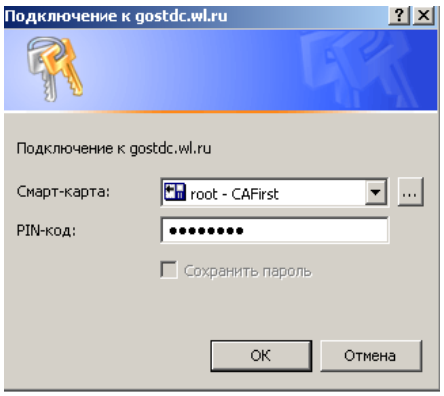
Дополнительно можно установить параметры безопасности шаблонов сертификатов, чтобы смарт-карты могли выпускать только определенные пользователи или группы.

3.1.5.Настройка Веб-сервера

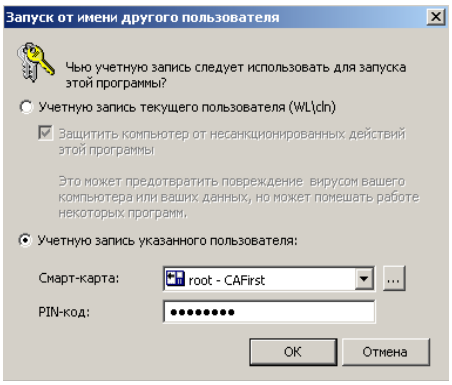
Чтобы только аутентифицированные в домене пользователи могли получить доступ к веб-серверу необходимо запретить анонимный доступ и настроить DACL на файлах и каталогах IIS (в NTFS).



Microsoft Windows начиная с XP, поддерживает аутентификацию с помощью смарт-карты в Internet Explorer. При наличии зарегистрированного считывателя после считывания сертификата со смарт-карты появляется окно с запросом ввода пин-кода для входа на защищенный сайт.



Примечание. В Microsoft Windows начиная с XP сертификат, находящийся на смарт-карте, при вставке в считыватель автоматически копируется в хранилище сертификатов MY текущего пользователя. И смарт-карта, кроме аутентификации на веб-сервере, может быть использована, например, для выполнения задач под другим пользователем (**Run As**), подключения защищенных сетевых дисков (**net use /smartcard**) или для защиты почты.



Для работы этой функции в реестре для процесса Winlogon должен быть зарегистрирован нотификатор (по умолчанию установлен):

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ScCertProp]
"Impersonate"=dword:00000001
"Enabled"=dword:00000001
"Lock"="SCardSuspendCertProp"
"Unlock"="SCardResumeCertProp"
"Logoff"="SCardStopCertProp"
"Logon"="SCardStartCertProp"
"DLLName"="wlnotify.dll"
"Asynchronous"=dword:00000001
```

3.1.6.Настройка ISA-сервера

Microsoft ISA Server может быть настроен, например, для ограничение доступа пользователей домена во внешние сети. Для этого необходимо на рабочие места пользователей установить Firewall Client. А в параметрах брандмауэра установить обязательную аутентификацию клиентов внутренней сети и создать правило доступа/запрета доступа для необходимых клиентов (групп).

Для защиты трафика между сервером и клиентом может быть использован протокол КриптоПро TLS.

3.1.7. Настройка SQL-сервера

MS SQL Server также может быть настроен на использование протокола аутентификации Kerberos, так, что только прошедшие проверку пользователи получат доступ к серверу.

3.1.8. Настройка MS Exchange сервера & MS Outlook

Если для подключения MS Outlook к MS Exchange серверу используется протокол exchange, аутентификация клиентов будет производиться по протоколу Kerberos. Дополнительно можно потребовать «Всегда запрашивать имя и пароль» - в этом случает будет отображаться окно ввода пароля/вставки смарт-карты на MS Windows XP и старше.

Также сертификаты и ключи со смарт-карты (при использовании соответствующего шаблона сертификатов, например, «пользователь со смарт-картой») могут быть использованы для подписи и шифрования почты. (На MS Windows XP и старше – устанавливаются в хранилище автоматически при вставке смарт-карты)

3.2. Использование КриптоПро Winlogon для удаленной аутентификации в домене Microsoft Windows 2003 Server

КриптоПро Winlogon может применяться для удаленной аутентификации в домене. Например, при использовании клиента удаленного рабочего стола или MS Outlook (для MS Windows старше XP) и соответствующей настройке брандмауэра.

4. Установка версии

Установка ПО производится в соответствие с документом «Установка и развертывание КриптоПро Winlogon».

5. Информация для пользователей

Для получения дополнительной информации о данном продукте, а так же о других продуктах ООО "Крипто-Про", можно обращаться по адресу:

Служба маркетинга и технической поддержки Крипто-Про.

127018, Москва, улица Образцова 38, ООО "Крипто-Про".

Телефон: +7 (495) 780 4820

Факс: +7 (495) 780 4820

e-mail: info@CryptoPro.ru

WWW: http://www.CryptoPro.ru