ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-05 92 02–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 5.0

ПРОГРАММНЫЙ МОДУЛЬ ПОДДЕРЖКИ «TLS»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

ВАМБ.00060-05 92 02

2016

Аннотация

Данный документ содержит описание процесса эксплуатации программного модуля поддержки TLS криптопровайдера «Валидата CSP» версии 5.0.

Документ предназначен для пользователей как руководство по эксплуатации программного модуля поддержки TLS криптопровайдера «Валидата CSP» версии 5.0.

Содержание

1 НАЗНАЧЕНИЕ ПРОГРАММНОГО МОДУЛЯ

Программный модуль поддержки TLS криптопровайдера «Валидата CSP» предназначен для:

– обеспечения защищенного канала связи между сервером и клиентом по протоколу TLS 1.2 (RFC 5246) или TLS 1.0 (RFC 2246) с использованием шифрования в соответствии с ГОСТ 28147-89;

– обеспечения контроля целостности защищенного канала связи между сервером и клиентом по протоколу TLS с использованием имитозащиты в соответствии с ГОСТ 28147-89;

– выполнения аутентификации сервера клиентом по протоколу TLS посредством вычисления ключа парной связи Диффи-Хелмана с использованием пар закрытых и открытых ключей, созданных в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001;

– выполнения аутентификации клиента сервером по протоколу TLS посредством вычисления электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001;

– обеспечения начальной аутентификации клиента в домене Microsoft Active Directory по протоколу Kerberos PKInit (RFC 4556) посредством вычисления электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001.

Программный модуль поддержки TLS криптопровайдера «Валидата CSP» предназначен для использования на нижеследующих версиях ОС:

– Microsoft Windows Vista с пакетом обновлений 1 и выше;

– Microsoft Windows Server 2008 с пакетом обновлений 1 и выше;

– Microsoft Windows 7;

– Microsoft Windows Server 2008 R2;

– Microsoft Windows 8/8.1;

– Microsoft Windows Server 2012/2012 R2;

При этом поддерживаются как 32-битные ОС Microsoft Windows (x86), так и 64-битные ОС Microsoft Windows (x64). Для корректной работы модуля поддержки TLS необходимо наличие установленного обновления ОС Microsoft Windows KB 980436 (http://support.microsoft.com/kb/980436), или более нового обновления, его заменяющего.

В качестве клиентского ПО, использующего протокол TLS, поддерживаются следующие программные продукты:

– Microsoft Internet Explorer (IE) версий 6.0, 7.0, 8.0, 9.0, 10.0 и 11.0;

– Remote Desktop Client (RDC) версий 5.2, 6.0, 6.1, 7.0, 8.0 и 8.1.

В качестве серверного ПО, использующего протокол TLS, поддерживаются следующие программные продукты:

– Internet Information Server (IIS) версий 6.0 (из состава Microsoft Windows Server 2003), 7.0 (из состава Microsoft Windows Server 2008), 7.5 (из состава Microsoft Windows Server 2008 R2), 8.0 (из состава Microsoft Windows Server 2012) и 8.5 (из состава Microsoft Windows Server 2012 R2);

– Terminal Services (TS) из состава Microsoft Windows Server 2008/2008 R2/2012/2012 R2;

– Terminal Services Gateway (TS Gateway) из состава Microsoft Windows Server 2008/2008 R2/2012/2012 R2.

В качестве серверного ПО, использующего протокол Kerberos PKInit, поддерживаются контроллеры доменов Microsoft Active Directory под управлением ОС Microsoft Windows Server 2008/2008 R2/2012/2012 R2.

2 ОПИСАНИЕ МЕХАНИЗМА ПОСТРОЕНИЯ ЦЕПОЧЕК СЕРТИФИКАТОВ В ОС WINDOWS С МОДУЛЕМ ПОДДЕРЖКИ TLS

2.1 Общие положения

Программный модуль поддержки TLS криптопровайдера «Валидата CSP» встраивается в ОС Windows и обеспечивает возможность работы с сертификатами, созданными в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012, в частности, для построения и проверки их цепочек, с помощью стандартного программного интерфейса Crypto API 2.0. Данные возможности, таким образом, становятся доступными прикладному программному обеспечению (ППО), разработанному, в том числе, и сторонними производителями ППО.

Цепочка сертификатов, известная также как путь сертификации, предназначена для аутентификации, посредством ЭП, конечного сертификата с помощью сертификата корневого Центра сертификации (ЦС, Certificate Authority, CA), находящегося в начале цепочки, и, возможно, сертификатов промежуточных ЦС, находящихся в цепочке между сертификатом корневого ЦС и конечным сертификатом. Сертификат корневого ЦС является самоподписанным, т.е. данный сертификат аутентифицирует себя сам. Также сертификат корневого ЦС аутентифицирует следующий за ним в цепочке сертификат промежуточного ЦС. Далее, по цепочке, мы приходим к последнему сертификату промежуточного ЦС, который уже аутентифицирует собственно конечный сертификат.

2.2 Проверка текущего статуса

Для проверки текущего статуса, или действительности, конечного сертификата цепочки сертификатов как таковой недостаточно - например, если с момента выпуска конечного сертификата последний был аннулирован (или отозван). Для подтверждения действительности сертификатов используют либо Списки отозванных сертификатов (COC, Certificate Revocation List, CRL), либо Протокол сетевого статуса сертификата (ПССС, Online Certificate Status Protocol, OCSP).

COC представляет собой список серийных номеров отозванных сертификатов данного ЦС, заверенный ЭП на закрытом ключе ЦС. Дополнительно, COC содержит время отзыва каждого сертификата и, возможно, причину отзыва. ПССС позволяет получить от ответчика OCSP, для каждого выпущенного данным ЦС конечного сертификата, заверенное ЭП подтверждение текущего статуса этого сертификата. Для отозванных сертификатов заверенное ЭП подтверждение содержит время и, возможно, причину отзыва. В ответчике OCSP для простановки ЭП используется специальный конечный сертификат, выпущенный данным ЦС и содержащий необходимое расширенное использование ключа.

При использовании COC для проверки действительности конечного сертификата для каждого ЦС (и корневого, и промежуточных) производится попытка найти в COC данного ЦС серийный номер следующего сертификата цепочки. Если, при наличии искомого серийного номера в COC, время отзыва уже наступило, то следующий сертификат цепочки и, следовательно, конечный сертификат, считаются отозванными.

При использовании ПССС для проверки действительности конечного сертификата для каждого ЦС (и корневого, и промежуточных) производится посылка OCSP запроса, содержащего серийный номер следующего сертификата цепочки, соответствующему данному ЦС OCSP ответчику. Последний формирует заверенное ЭП подтверждение, содержащее текущий статус проверяемого сертификата. Если проверяемый сертификат отозван и время отзыва уже насту-

пило, то следующий сертификат цепочки и, следовательно, конечный сертификат, считаются отозванными.

2.3 Хранилища сертификатов и СОС

В ОС Windows хранилища сертификатов используют Реестр ОС для хранения сертификатов и СОС, и делятся на хранилища компьютера и пользовательские. Как следует из названия, хранилища компьютера являются общими для всех пользователей и используются, в том числе, системными процессами ОС. Пользовательские хранилища привязаны к каждому конкретному пользователю, и у каждого пользователя они индивидуальные. При этом, в пользовательские хранилища автоматически включаются также сертификаты и СОС из хранилищ компьютера (за исключением хранилища *Личное*).

Также хранилища различаются по типу хранимых ими объектов:

– *Личное (Personal, MY)* - предназначено для хранения личных сертификатов, для которых есть соответствующие им закрытые ключи;

– *Другие пользователи (Other People, AddressBook)* - предназначено для хранения сертификатов сторонних пользователей;

– *Доверенные корневые центры сертификации (Trusted Root Certification Authorities, ROOT)* - предназначено для хранения сертификатов и СОС корневых ЦС;

– *Промежуточные центры сертификации (Intermediate Certification Authorities, CA)* - предназначено для хранения сертификатов и СОС промежуточных ЦС.

Таким образом, хранилища пользователя *Другие пользователи*, *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации* включают в себя сертификаты и СОС из соответствующих хранилищ компьютера.

Для управления объектами, расположенных в хранилищах сертификатов ОС Windows, рекомендуется использовать *Консоль управления Microsoft (Microsoft Management Console, MMC)*. После запуска *MMC* следует добавить оснастку *Сертификаты (Certificates)* учетной записи пользователя или учетной записи компьютера - от этого выбора зависит, какие хранилища сертификатов будут отображаться. Следует отметить, что для добавления оснастки *Сертификаты* учетной записи компьютера необходимы права локального администратора.

2.4 Описание алгоритма построения цепочек

Для построения и проверки цепочек сертификатов ППО использует функции Crypto API 2.0. При вызове этих функций ППО выбирает ”двигатель” (Engine), используемый для построения цепочек - компьютера или пользовательский (используется по умолчанию). При выборе ”двигателя” компьютера используются хранилища сертификатов компьютера, при выборе пользовательского ”двигателя” используются хранилища сертификатов пользователя.

Построение цепочки сертификатов начинается с проверяемого (конечного) сертификата. Для возможности построения цепочки в проверяемом сертификате должно присутствовать расширение (Extension) *Идентификатор ключа Центра сертификации (Authority Key Identifier)*. В данном расширении находится, в числе прочего, *Идентификатор ключа (Key Identifier)* - хэш открытого ключа - сертификата ЦС, на котором был выпущен проверяемый сертификат. По этому идентификатору и производится поиск сертификата ЦС в локальных хранилищах *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации* - в искомом сертификате ЦС этот идентификатор равен значению, находящемуся в расширении *Идентификатор ключа субъекта (Subject Key Identifier)*.

При отсутствии искомого сертификата ЦС в локальных хранилищах производится попытка

нахождения в проверяемом сертификате расширения *Доступ к информации о Центре сертификации (Authority Information Access, AIA)*. В данном расширении, в числе прочего, находится список уникальных идентификаторов ресурса (Unique Resource Identifier, URI), указывающих на искомый сертификат ЦС, доступный по сети. Каждый URI из списка используется при попытке загрузки сертификата ЦС последовательно до успешной загрузки искомого объекта.

После успешного нахождения искомого сертификата ЦС (локально или по сети) производится поиск СОС, соответствующего найденному сертификату ЦС. Поиск СОС также изначально производится в локальных хранилищах *Доверенные корневые центры сертификации* и *Промежуточные центры сертификации*. В искомом СОС значение *Идентификатор ключа* из состава расширения *Идентификатор ключа Центра сертификации* должно быть равно значению, находящемуся в расширении *Идентификатор ключа субъекта* сертификата ЦС.

При отсутствии искомого СОС в локальных хранилищах производится попытка нахождения в проверяемом сертификате расширения *Точки распространения СОС (CRL Distribution Points, CDP)*. В данном расширении находится список URI, указывающих на искомый СОС, доступный по сети. Каждый URI из списка используется при попытке загрузки СОС последовательно до успешной загрузки искомого объекта.

Следует упомянуть об особенностях, связанных с использованием для построения цепочек СОС, содержащих расширение *Точка распространения выдачи (Issuing Distribution Point, IDP)*:

– в ОС Windows расширение *IDP* не используется для загрузки и/или обновления СОС по сети;

– сертификаты, выпущенные на сертификате ЦС, соответствующем СОС с расширением *IDP*, должны содержать расширение *CDP*;

– списки URI, содержащиеся в расширении *IDP* СОС и в расширении *CDP* сертификатов, выпущенных данным ЦС, должны совпадать.

Вместо СОС для определения действительности проверяемого сертификата может использоваться ПССС. Для этого в расширении *Доступ к информации о Центре сертификации* проверяемого сертификата должен присутствовать URI OCSP ответчика данного ЦС. При использовании ПССС формируется OCSP запрос и посылается OCSP ответчику. Полученное от OCSP ответчика подтверждение содержит текущий статус проверяемого сертификата.

После нахождения сертификата ЦС и СОС (или после получения подтверждения от OCSP ответчика) выполняется криптографическая проверка полученных объектов, а также проверка действительности проверяемого сертификата. При успешном выполнении проверок, если найденный сертификат ЦС не является самоподписанным или не был найден в локальном хранилище *Доверенные корневые центры сертификации*, он занимает место проверяемого сертификата, и весь вышеописанный алгоритм повторяется рекурсивно.

Результат построения и проверки цепочки сертификата определяется следующим образом:

– *Аутентичность конечного сертификата не установлена* - если, по какой-либо причине, очередной искомый сертификат ЦС не был найден, или если цепочка не начинается с самоподписанного сертификата корневого ЦС, найденного в локальном хранилище *Доверенные корневые центры сертификации*;

– *Действительность конечного сертификата не установлена* - если, по какой-либо причине, очередной искомый СОС данного ЦС не был найден, или не было получено доверенное подтверждение от OCSP ответчика данного ЦС;

– *Конечный сертификат отозван* - если очередной проверяемый сертификат был найден в СОС вышестоящего ЦС или OCSP ответчик вышестоящего ЦС возвратил подтверждение, содержащее статус 'отозван', и время отзыва уже наступило;

– *Конечный сертификат действителен* - в остальных случаях.

В состав современных версий ОС Windows (Windows Vista и более новых) входит очень полезная утилита *CertUtil*, с помощью которой можно выполнять различные операции, связанные с сертификатами, СОС, цепочками, и т.п. К сожалению, данная утилита не входит в состав ОС Windows XP/Server 2003, поэтому для ее использования необходимо вначале установить пакет средств администрирования Windows Server 2003.

В частности, для построения и проверки цепочки сертификата с именем субъекта *CN=Test,CN=Users,DC=Company,DC=ru*, находящегося в хранилище пользователя *Личное*, можно использовать следующую команду:
certutil.exe -user -verifystore MY Test
Результатом выполнения данной команды будет либо подтверждение действительности проверяемого сертификата, либо описание ошибки, возникшей в результате построения или проверки его цепочки.

2.5 Кэширование объектов

При построении цепочек сертификатов возможно выполнение загрузки сертификатов промежуточных ЦС или СОС по сети на основании информации, содержащейся в расширениях *AIA* и/или *CDP*. Для исключения необходимости повторной загрузки уже загруженных объектов последние запоминаются в специальном файловом кэше. При выполнении загрузки объекта по сети вначале производится попытка найти его в этом кэше для повышения общей производительности криптографической подсистемы.

Используемый кэш зависит от "двигателя", выбранного ППО для построения цепочек - "двигатель" компьютера и каждый пользовательский "двигатель" используют собственный выделенный кэш. Объекты хранятся в кэше, в общем случае, до истечения срока их действия - например, СОС, находящийся в кэше, будет действителен до момента времени, указанного в поле *Следующее обновление (Next Update)*.

Для детального просмотра содержимого кэша можно воспользоваться следующей командой:
*certutil.exe -v -urlcache **
Для полной очистки содержимого кэша можно воспользоваться следующей командой:
*certutil.exe -v -urlcache * delete*
На современных ОС Windows (Windows Vista и более новых) рекомендуется не пользоваться командой очистки кэша, а помечать все записи кэша как недействительные с помощью следующей команды (для выполнения требуются права локального администратора):
certutil.exe -setreg chain\ChainCacheResyncFiletime @now
Более детально описание механизма кэширования объектов приведено в статье по ссылке http://technet.microsoft.com/en-us/library/ee619754%28v=ws.10%29.aspx.

3 ИСПОЛЬЗОВАНИЕ INTERNET INFORMATION SERVER (IIS) С МОДУЛЕМ ПОДДЕРЖКИ TLS

Перед началом использования Microsoft Internet Information Server (IIS) совместно с программным модулем поддержки TLS криптопровайдера «Валидата CSP» необходимо поместить все требуемые сертификаты и списки отозванных сертификатов (СОС) в системное хранилище сертификатов локального компьютера. Для этого необходимо выполнить следующие шаги:

– загрузить корневой(ые) сертификат(ы) ЦС и соответствующие ему (им) СОС(ы) в системное хранилище корневых сертификатов ЦС локального компьютера посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить промежуточный(ые) сертификат(ы) ЦС и соответствующие ему (им) СОС(ы) в системное хранилище промежуточных сертификатов ЦС локального компьютера посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить сертификат Web сервера IIS с одновременной привязкой его к контейнеру с соответствующим закрытым ключом в системное хранилище личных сертификатов локального компьютера посредством использования конфигурационной программы «Валидата CSP». При выдаче сертификата Web сервера IIS необходимо учесть, что в нем должен присутствовать OID Проверки подлинности сервера (1.3.6.1.5.5.7.3.1) и должно быть указано разрешённое использование закрытого ключа (Key Usage) для выполнения ЭП и шифрования. Дополнительно, DNS имя Web сервера должно быть прописано в атрибуте CN X.500 имени владельца (Subject Name) и в альтернативном имени владельца (Subject Alternative Name) сертификата Web сервера.

Далее необходимо настроить Web сервер IIS на использование установленного сертификата. Для этого необходимо вызвать пункт меню «Пуск»→«Программы»→«Администрирование»→«Диспетчер служб IIS» и, подсветив нужный Web сайт правой кнопкой «мыши», выбрать пункт меню «Свойства». После этого необходимо выбрать закладку «Безопасность каталога» и нажать на кнопку «Сертификат» группы «Безопасные подключения» (Рисунок 1).

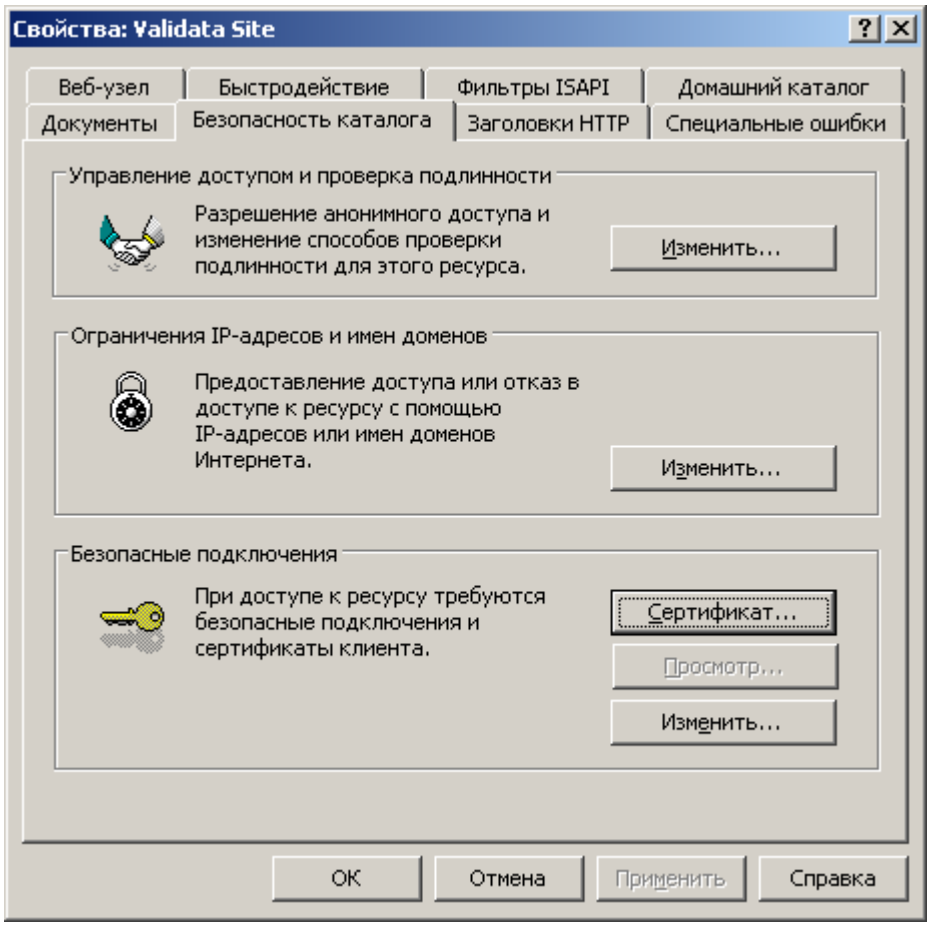

Рисунок 1 – Диалог безопасности каталога

В появившемся диалоге необходимо выбрать пункт «Назначение существующего сертификата» и нажать кнопку «Далее». На экран будет выдан диалог выбора сертификата для Web сервера IIS (Рисунок 2).

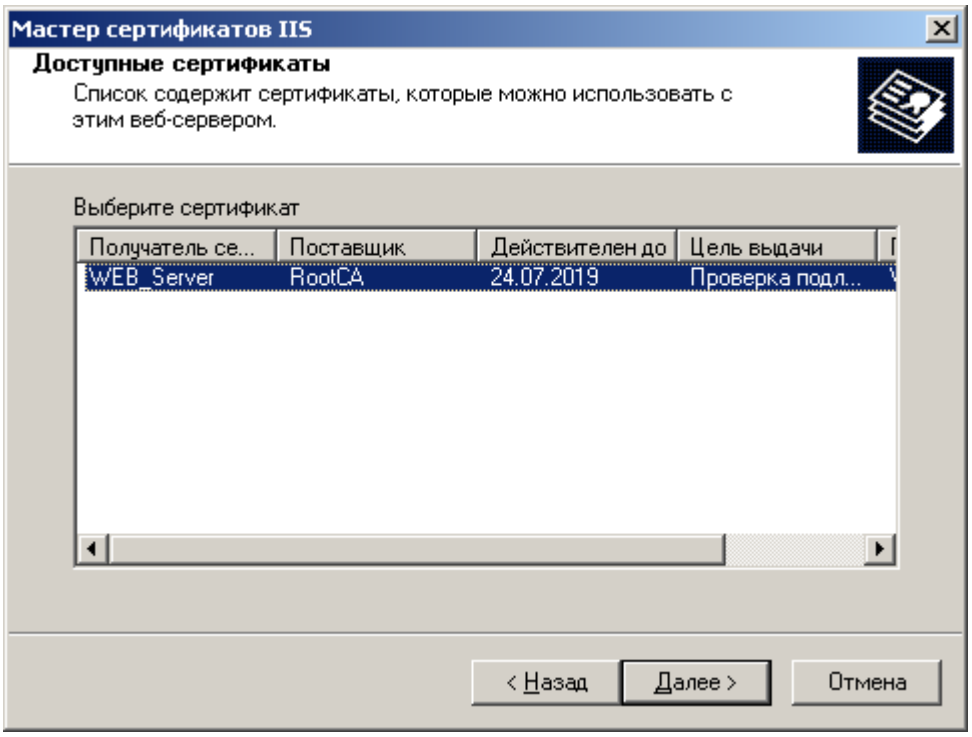

Рисунок 2 – Диалог выбора сертификата

Выбрав нужный сертификат, необходимо нажать кнопку «Далее» на этом и следующем диалогах, а в конце нажать на кнопку «Готово». По умолчанию Web сервер IIS не требует наличия сертификатов у клиентов и, соответственно, не проводит проверку подлинности клиентов на основании их сертификатов. Для включения проверки подлинности клиентов необходимо в диалоге безопасности каталога нажать на кнопку «Изменить» группы «Безопасные подключения» (Рисунок 3).

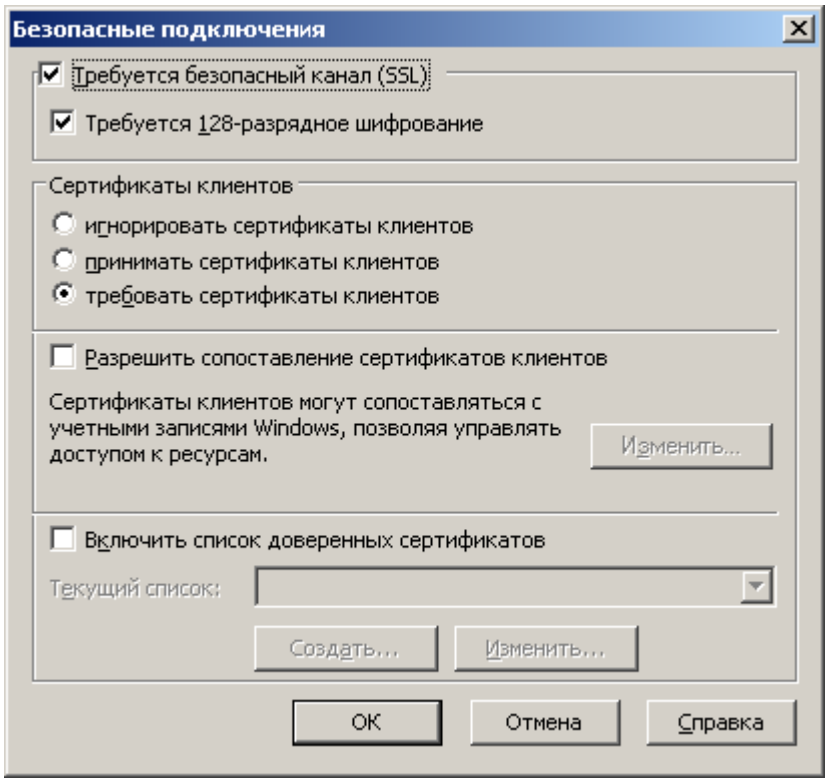

Рисунок 3 – Диалог подключений

Далее в диалоге подключений необходимо включить свойство «Требуется безопасный канал (SSL)», установить переключатель «Сертификаты клиентов» в положение «требовать сертификаты клиентов» и нажать на кнопку «OK». Для правильной работы Web сервера IIS совместно с модулем поддержки TLS необходимо выполнение следующих требований:

– у закрытого ключа сертификата Web сервера IIS должен отсутствовать пароль и/или ПИН-код;

– при использовании Биологического ДСЧ (или любого другого ДСЧ, требующего отображения графического интерфейса при инициализации) последний должен быть проинициализирован перед использованием Web сервера IIS;

– носитель с закрытым ключом Web сервера IIS должен быть смонтирован перед использованием Web сервера IIS.

4 ИСПОЛЬЗОВАНИЕ MICROSOFT INTERNET EXPLORER С МОДУЛЕМ ПОДДЕРЖКИ TLS

Перед началом использования Microsoft Internet Explorer (IE) совместно с программным модулем поддержки TLS криптопровайдера «Валидата CSP» необходимо поместить все требуемые сертификаты и списки отозванных сертификатов (СОС) в системное хранилище сертификатов пользователя. Для этого необходимо выполнить следующие шаги:

– загрузить корневой(ые) сертификат(ы) ЦС и соответствующие ему (им) СОС(ы) в системное хранилище корневых сертификатов ЦС пользователя посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить промежуточный(ые) сертификат(ы) ЦС и соответствующие ему (им) СОС(ы) в системное хранилище промежуточных сертификатов ЦС пользователя посредством использования оснастки Сертификаты консоли управления Microsoft (Microsoft Management Console, MMC);

– загрузить сертификат клиента с одновременной привязкой его к контейнеру с соответствующим закрытым ключом в системное хранилище личных сертификатов пользователя посредством использования конфигурационной программы «Валидата CSP». При выдаче сертификата клиента необходимо учесть, что в нем должен присутствовать OID Проверки подлинности клиента (1.3.6.1.5.5.7.3.2).

На современных ОС (ОС Windows Vista и выше) для правильной работы клиентского ПО не требуется запускать программу TLS монитора, так как модуль поддержки TLS будет автоматически определять алгоритм открытого ключа сертификата Web сайта и, в зависимости от этого алгоритма, вырабатывать ключи шифрования для защиты канала.

Для правильной работы клиентского ПО совместно с модулем поддержки TLS на ОС предыдущего поколения (ОС Windows XP/Server 2003) необходимо выполнить следующие действия:

– запустить программу TLS монитора (см. подраздел 9);

– перевести программу TLS монитора во включенное состояние;

– запустить клиентское ПО и подключиться к требуемому защищенному Web серверу. При этом во время выполнения подключения может быть отображена последовательность диалоговых окон для инициализации ДСЧ, если это не было проделано ранее;

– по окончании сеанса работы завершить клиентское ПО и программу TLS монитора.

Для использования клиентского ПО на ОС предыдущего поколения (ОС Windows XP/Server 2003) с Web сайтами, использующими сертификаты со сторонними алгоритмами открытого ключа (такими как RSA), необходимо выполнить следующие действия:

– перевести программу TLS монитора в выключенное состояние и завершить ее (см. подраздел 9);

– запустить клиентское ПО и подключиться к требуемому защищенному Web серверу;

– по окончании сеанса работы завершить клиентское ПО.

5 ИСПОЛЬЗОВАНИЕ TERMINAL SERVICES С МОДУЛЕМ ПОДДЕРЖКИ TLS

Перед началом использования Terminal Services (TS, службы терминалов) совместно с программным модулем поддержки TLS криптопровайдера «Валидата CSP» необходимо поместить все требуемые сертификаты и списки отозванных сертификатов (СОС) в системное хранилище сертификатов локального компьютера - так же, как это описано для Internet Information Server (IIS) в подразделе 3.

Далее необходимо настроить службу терминалов на использование установленного сертификата. Для этого необходимо вызвать пункт меню «Пуск»→«Администрирование»→«Службы удаленных рабочих столов»→«Конфигурация узла сеансов удаленных рабочих столов» и выбрать требуемое подключение, щелкнув по нему дважды правой кнопкой «мыши» (Рисунок 4).

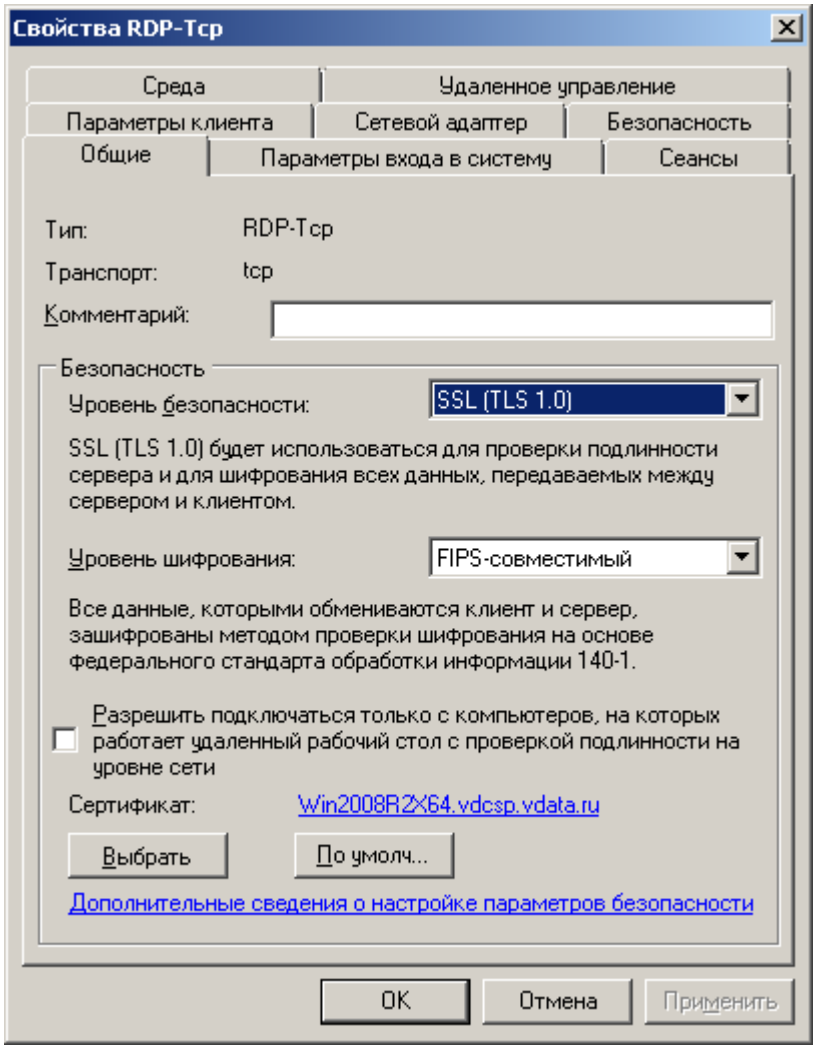

Рисунок 4 – Диалог настройки безопасности

После этого необходимо установить Уровень безопасности в «SSL (TLS 1.0)», Уровень шифрования в «Высокий» или «FIPS-совместимый», и указать сертификат службы терминалов, нажав на кнопку «Выбрать». Выбрав нужный сертификат в диалоговом окне, необходимо нажать кнопку «OK» (Рисунок 5).

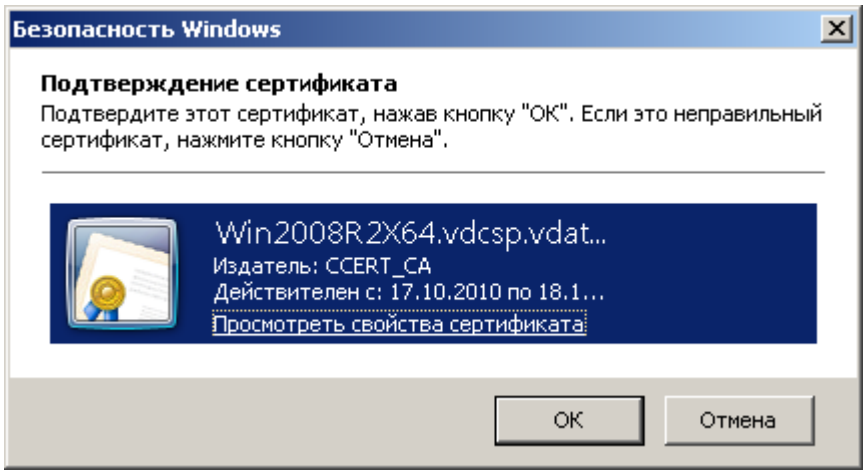

Рисунок 5 – Диалог выбора сертификата

Служба терминалов не имеет возможности проводить проверку подлинности сертификатов клиентов. При необходимости выполнения проверки подлинности клиентов на основании их сертификатов следует либо использовать шлюз служб терминалов, функционирующий между удаленными рабочими станциями клиентов и серверами терминалов, либо включить проверку подлинности на уровне сети (Network Level Authentication, NLA).

Детальное руководство по настройке службы терминалов приведено (на русском языке) по ссылке http://technet.microsoft.com/ru-ru/library/dd640164(WS.10).aspx.

Для правильной работы службы терминалов совместно с модулем поддержки TLS необходимо выполнение тех же требований к закрытому ключу службы терминалов и к состоянию инициализации ДСЧ, что приведены для Internet Information Server (IIS) в подразделе 3.

5.1 Использование Terminal Services с модулем поддержки TLS на ОС Windows Server 2012/2012 R2

Изменения пользовательского интерфейса процедуры конфигурирования службы терминалов в ОС Windows Server 2012/2012 R2 привели к тому, что описанный выше способ настройки оказывается неэффективным. Для настройки службы терминалов в ОС Windows Server 2012/2012 R2 следует пользоваться специальным командным файлом, настраивающим службу терминалов через инструментарий управления Windows (Windows Management Instrumentation, WMI).

Для начала следует определить так называемый отпечаток (Thumbprint) сертификата терминального сервера, который состоит из двадцати байт. Для этого следует, используя MMC, просмотреть свойства сертификата терминального сервера и скопировать его отпечаток (в виде строки, состоящей из пар шестнадцатиричных цифр, разделенных пробелами) в текстовый редактор (например, Notepad). Далее в копии строки с отпечатком следует удалить пробелы и скопировать получившуюся строку в приведенный ниже шаблон командного файла, заменив ей строку *xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx*:

```
@echo off

set WMIC=%WINDIR%\system32\Wbem\wmic.exe

echo.
```

```
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting SET MinEncryptionLevel="3"
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting SET SecurityLayer="2"
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting SET SSLCertificateSHA1Hash="
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

echo.

%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting GET MinEncryptionLevel
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting GET SecurityLayer
%WMIC% /NAMESPACE:\\root\CIMV2\TerminalServices PATH
   Win32_TSGeneralSetting GET SSLCertificateSHA1Hash
```

Для завершения процедуры настройки следует выполнить получившийся командный файл и перезгрузить терминальный сервер.

6 ИСПОЛЬЗОВАНИЕ TERMINAL SERVICES GATEWAY С МОДУЛЕМ ПОДДЕРЖКИ TLS

Перед началом использования Terminal Services Gateway (TS Gateway, шлюза служб терминалов) совместно с программным модулем поддержки TLS криптопровайдера «Валидата CSP» необходимо поместить все требуемые сертификаты и списки отозванных сертификатов (СОС) в системное хранилище сертификатов локального компьютера - также, как это описано для Internet Information Server (IIS) в подразделе 3.

Далее необходимо настроить шлюз служб терминалов на использование установленного сертификата. Для этого необходимо вызвать пункт меню «Пуск» →«Администрирование»→«Службы удаленных рабочих столов»→«Диспетчер шлюза удаленных рабочих столов», найти требуемый шлюз и, щелкнув по нему левой кнопкой «мыши», выбрать пункт меню «Свойства». Далее следует выбрать закладку «Сертификат SSL» (Рисунок 6).

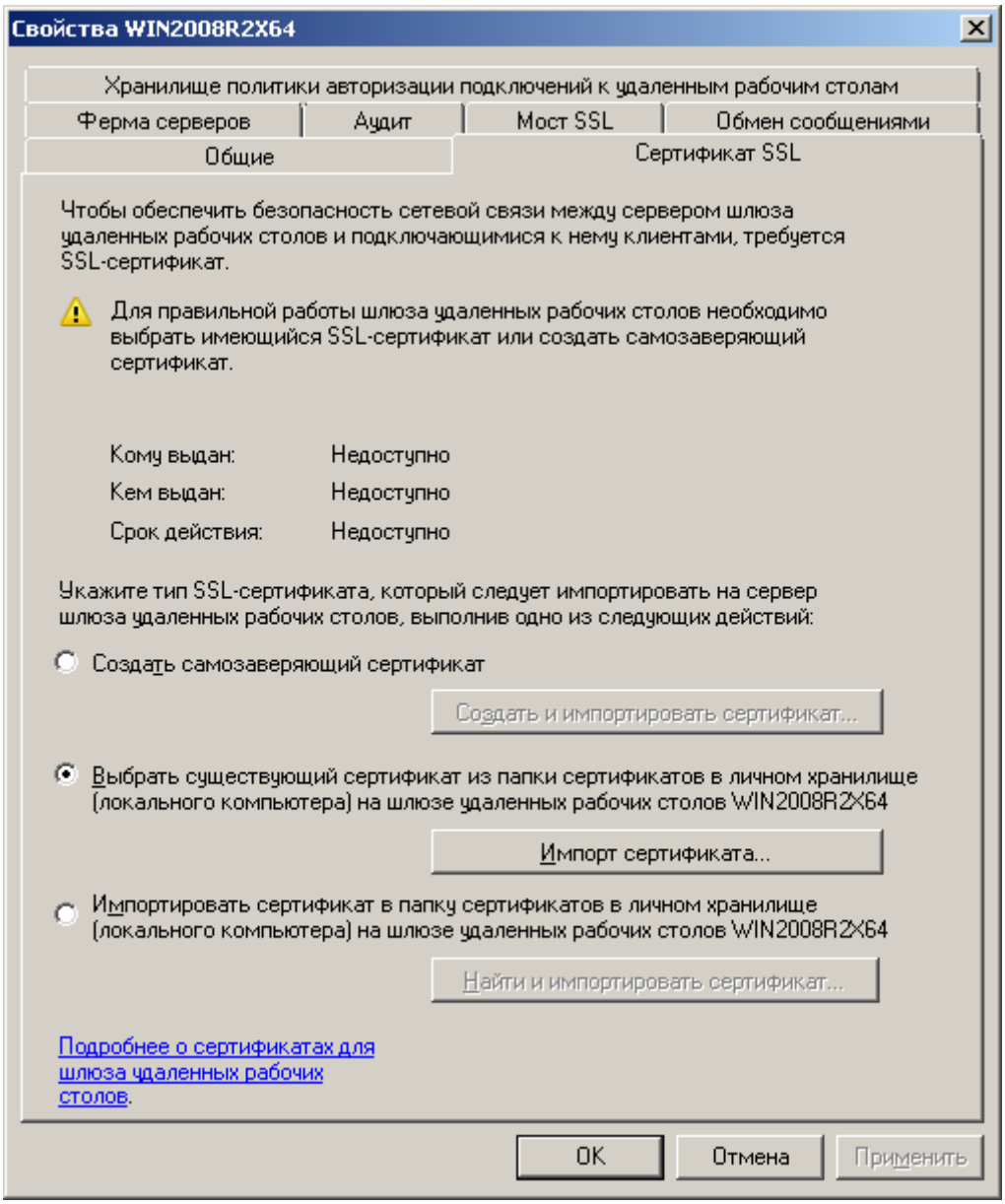

Рисунок 6 – Диалог свойств шлюза

После этого необходимо выбрать сертификат шлюза служб терминалов, нажав на кнопку «Импорт сертификата» (Рисунок 7).

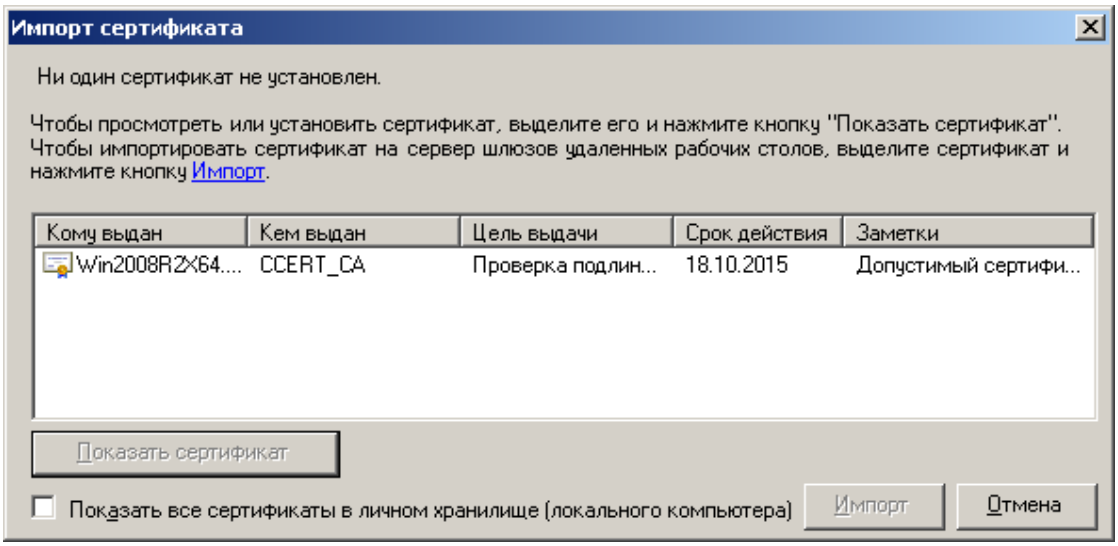

Рисунок 7 – Диалог выбора сертификата

Выбрав нужный сертификат, необходимо нажать кнопку «Импорт», и кнопку «ОК» на родительском диалоге.

Каждый шлюз служб терминалов позволяет различным пользователям подключаться к различным защищаемым данным шлюзом ресурсам (серверам терминалов). Нижеследующие политики безопасности шлюза служб терминалов позволяют гибко регламентировать подключения пользователей к защищаемым ресурсам (серверам терминалов):

– Политики авторизации подключений - данные политики позволяют указать разрешённые методы проверки подлинности Windows (пароль и/или смарт-карта) для каждого конкретного пользователя или группы пользователей;

– Политики авторизации ресурсов - данные политики позволяют указать конкретных пользователей или группы пользователей, которым разрешено подключаться к каждому конкретному защищаемому ресурсу (серверу терминалов).

Детальное руководство по настройке шлюза служб терминалов приведено (на русском языке) по ссылке http://technet.microsoft.com/ru-ru/library/cc771530(WS.10).aspx.

Для правильной работы шлюза служб терминалов совместно с модулем поддержки TLS необходимо выполнение тех же требований к закрытому ключу шлюза служб терминалов и к состоянию инициализации ДСЧ, что приведены для Internet Information Server (IIS) в подразделе 3.

7 ИСПОЛЬЗОВАНИЕ REMOTE DESKTOP CLIENT С МОДУЛЕМ ПОДДЕРЖКИ TLS

Перед началом использования Remote Desktop Client (RDC) совместно с программным модулем поддержки TLS криптопровайдера «Валидата CSP» необходимо поместить все требуемые сертификаты и списки отозванных сертификатов (СОС) в системное хранилище сертификатов пользователя - так же, как это описано для Microsoft Internet Explorer (IE) в подразделе 4.

На современных ОС (ОС Windows Vista и выше) для правильной работы клиентского ПО не требуется запускать программу TLS монитора, так как модуль поддержки TLS будет автоматически определять алгоритм открытого ключа сертификата сервера терминалов или шлюза служб терминалов и, в зависимости от этого алгоритма, вырабатывать ключи шифрования для защиты канала.

Для правильной работы клиентского ПО на ОС предыдущего поколения (ОС Windows XP/Server 2003) необходимо выполнить те же действия по использованию программы TLS монитора, что приведены для Microsoft Internet Explorer (IE) в подразделе 4.

Использование Remote Desktop Client (RDC) версии 6.0 или более новой поддерживается при наличии установленного и настроенного пакета безопасности CredSSP. Данное условие автоматически выполняется для современных ОС (ОС Windows Vista и выше). Для ОС предыдущего поколения (ОС Windows XP) необходимо наличие установленного пакета обновлений 3 (SP3). Также необходимо настроить пакет безопасности CredSSP, выполнив следующие действия (более подробно описание пакета безопасности CredSSP приведено в статье по ссылке http://support.microsoft.com/kb/951608/ru):

– добавить строку tspkg в значение Security Packages (типа REG_MULTI_SZ) ключа реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa;

– добавить строку credssp.dll в значение SecurityProviders (типа REG_SZ) ключа реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders;

– выполнить перезагрузку.

После запуска RDC (программы MSTsc.exe) на экран будет выдано главное диалоговое окно программы (Рисунок 8) . Для возможности выполнения расширенной настройки нажмите кнопку «Параметры».

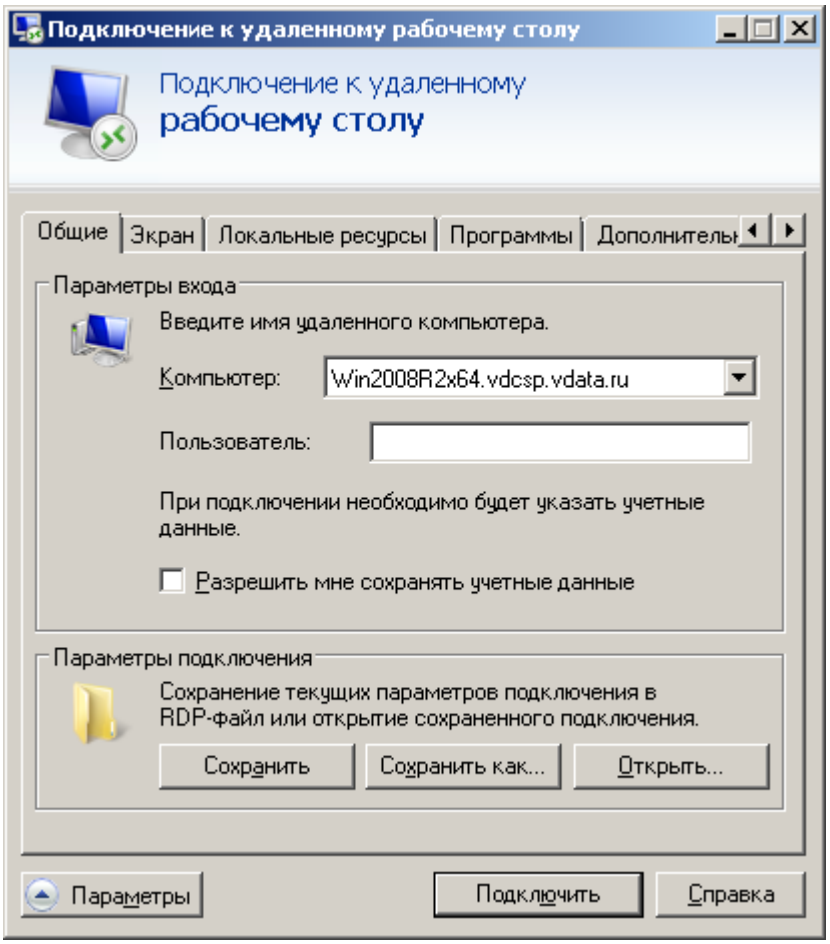

Рисунок 8 – Главное окно программы

Для ввода имени удаленного сервера терминалов используйте поле ввода «Компьютер». При необходимости, укажите имя шлюза служб терминалов, выбрав закладку «Подключение» и нажав кнопку «Параметры...». В появившемся окне установите переключатель в положение «Использовать следующие параметры сервера шлюза удаленных рабочих столов» и введите имя шлюза служб терминалов в поле «Имя сервера» (Рисунок 9).

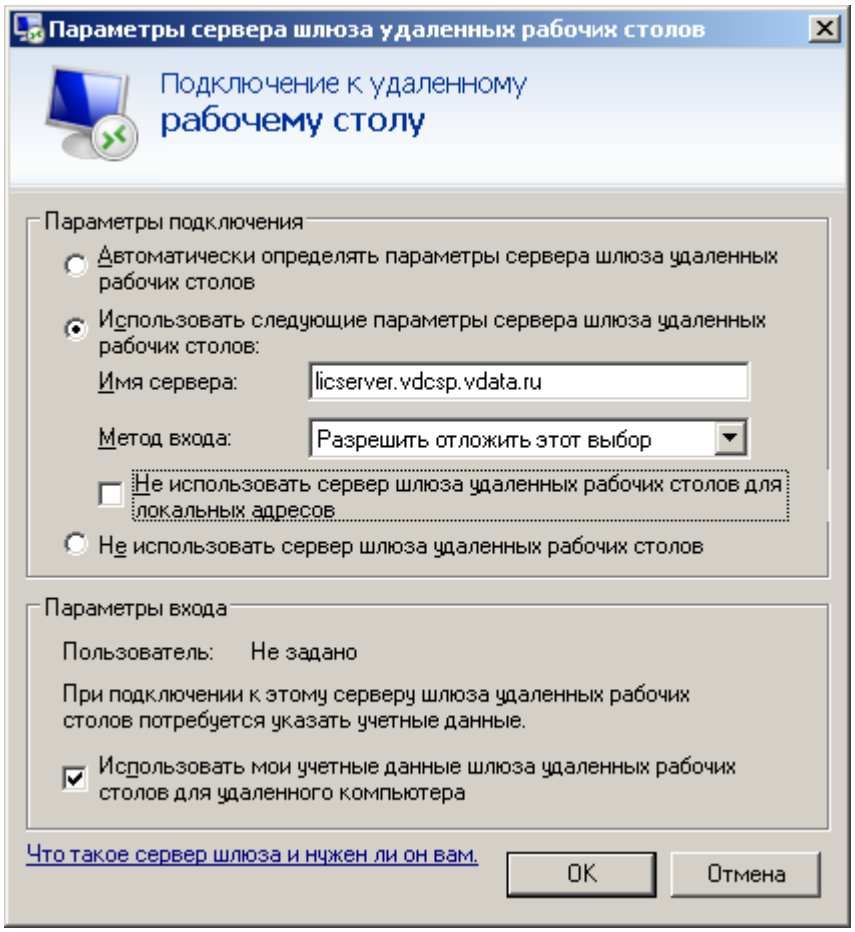

Рисунок 9 – Диалог ввода имени шлюза служб терминалов

После выполнения настройки необходимо нажать на кнопку «Подключить» для подключения к серверу терминалов.

Если свойство «Использовать мои учетные данные шлюза удаленных рабочих столов для удаленного компьютера» включено и подключение выполняется через шлюз служб терминалов, то учетные данные пользователя (имя пользователя и его пароль или ПИН-код смарт-карты) будут запрашиваться только один раз. Если же это свойство выключено и подключение выполняется через шлюз служб терминалов, то учетные данные пользователя будут запрашиваться дважды - первый раз для шлюза служб терминалов, а второй - для терминального сервера.

8 ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА KERBEROS PKINIT С МОДУЛЕМ ПОДДЕРЖКИ TLS

Программный модуль поддержки TLS криптопровайдера «Валидата CSP» поддерживает аутентификацию клиентов по протоколу Kerberos PKInit в двух режимах: локальном и удаленном. В первом случае выполняется аутентификация непосредственно во время входа клиента на рабочую станцию или сервер через Windows Login Screen. Во втором случае выполняется аутентификация клиента в терминальной сессии при подключении через Remote Desktop Client по протоколу RDP.

Аутентификация клиента выполняется одним из контроллеров домена на основании закрытого ключа клиента и соответствующего ему сертификата. Закрытый ключ клиента и его сертификат должны находиться на ключевом носителе типа смарт-карта (например, eToken или ruToken), поэтому такой процесс аутентификации клиента называют «Входом со смарт-картой». Дополнительно, копия сертификата клиента должна находиться в системном хранилище личных сертификатов пользователя и быть привязана к закрытому ключу последнего.

Каждый контроллер домена, в котором клиенты используют протокол Kerberos PKInit для аутентификации, также должен иметь сертификат с соответствующим ему и привязанным к нему закрытым ключом, расположенный в системном хранилище личных сертификатов локального компьютера. При этом к контроллеру домена предъявляются следующие требования:

– у закрытого ключа сертификата контроллера домена должен отсутствовать пароль и/или ПИН-код;

– при использовании Биологического ДСЧ (или любого другого ДСЧ, требующего отображения графического интерфейса при инициализации) последний должен быть проинициализирован перед тем, как клиенты начнут попытки входа со смарт-картой;

– носитель с закрытым ключом контроллера домена должен быть смонтирован перед тем, как клиенты начнут попытки входа со смарт-картой.

На рабочих станциях клиентов, на терминальных серверах и на шлюзах терминальных серверов, а также на контроллерах домена, в котором клиенты используют протокол Kerberos PKInit для аутентификации, должно быть установлено ПО поддержки (драйверы устройств и библиотеки) используемых ключевых носителей типа смарт-карта, а также библиотеки поддержки соответствующих ключевых носителей из состава «Валидата CSP».

В начале выполнения процесса аутентификации клиента пакет безопасности Kerberos посылает в службу распространения ключей (Key Distribution Center, KDC), находящуюся на контроллере домена, первоначальный запрос на аутентификацию KRB_AS_REQ. Данный запрос содержит Имя участника-пользователя (User Principal Name, UPN) клиента, метку времени и их ЭП, вычисленную на закрытом ключе клиента, а также сертификат клиента. При получении запроса контроллер домена (KDC) проверяет ЭП запроса и подлинность сертификата клиента. После успешного проведения проверок KDC подготавливает ответ KRB_AS_REP, содержащий зашифрованный сессионный ключ клиента для обмена данными с KDC, и билет (Ticket Granting Ticket, TGT). Поскольку сессионный ключ зашифрован на открытый ключ из сертификата клиента, только клиент может его расшифровать с помощью своего закрытого ключа.

Для возможности выполнения начальной аутентификации по протоколу Kerberos PKInit сертификат клиента должен удовлетворять следующим условиям (более подробно требования к сертификатам клиентов описаны в статье по ссылке http://technet.microsoft.com/ru-ru/library/ff404293(WS.10).aspx):

– в сертификате клиента должна быть указана функционирующая точка распространения СОС (CRL Distribution Point);

– в сертификате клиента должно быть указано разрешённое использование закрытого ключа (Key Usage) для выполнения ЭП и шифрования;

– в сертификате клиента базовые ограничения (Basic Constraints) не должны содержать признак сертификата ЦС, и ограничение на длину пути должно отсутствовать;

– в сертификате клиента расширенное использование ключа (Extended Key Usage) должно содержать OID Проверки подлинности клиента (1.3.6.1.5.5.7.3.2) и OID Входа со смарт-картой (1.3.6.1.4.1.311.20.2.2);

– в сертификате клиента в альтернативном имени субъекта (Subject Alternative Name) должно присутствовать Имя участника-пользователя (например UPN=user1@contoso.com). Имя участника-пользователя имеет формат адреса электронной почты (RFC 822) и состоит из имени пользователя и полного имени домена Microsoft Active Directory;

– в сертификате клиента имя субъекта (Subject Name) должно соответствовать имени контейнера клиента в Microsoft Active Directory (например, CN=User1, CN=Users, DC=Contoso, DC=COM);

– сертификат ЦС, на котором был выпущен сертификат клиента, должен присутствовать в Microsoft Active Directory в хранилище NTAuth и в локальных копиях хранилища NTAuth на контроллерах домена. Добавить сертификат в хранилище NTAuth можно следующим образом (более подробно механизм загрузки сертификатов ЦС в хранилище NTAuth описан по ссылке (на русском языке) http://support.microsoft.com/kb/295663/ru):

  • на одном из контроллеров домена (с правами администратора домена) выполнить команду certutil -dspublish -f <Файл сертификата ЦС> NTAuthCA;

  • на всех контроллерах домена (с правами администратора домена) выполнить команду certutil -enterprise -addstore NTAuth <Файл сертификата ЦС>.

– все сертификаты ЦС и СОС, необходимые для построения полной цепочки сертификатов клиентов и контроллеров домена, должны находиться в соответствующих системных хранилищах сертификатов ЦС (в хранилище корневых сертификатов ЦС - для корневого сертификата и СОС цепочки, в хранилище промежуточных сертификатов - для промежуточных сертификатов ЦС и СОС цепочки) локального компьютера (см. подраздел 3).

Для возможности выполнения начальной аутентификации по протоколу Kerberos PKInit сертификат контроллера домена должен удовлетворять следующим условиям:

– в сертификате контроллера домена должна быть указана функционирующая точка распространения СОС (CRL Distribution Point);

– в сертификате контроллера домена должно быть указано разрешённое использование закрытого ключа (Key Usage) для выполнения ЭП и шифрования;

– в сертификате контроллера домена базовые ограничения (Basic Constraints) не должны содержать признак сертификата ЦС, и ограничение на длину пути должно отсутствовать;

– в сертификате контроллера домена расширенное использование ключа (Extended Key Usage) должно содержать OID Проверки подлинности сервера (1.3.6.1.5.5.7.3.1), OID Проверки подлинности клиента (1.3.6.1.5.5.7.3.2), OID Входа со смарт-картой (1.3.6.1.4.1.311.20.2.2) и OID Аутентификации центра распределения ключей (1.3.6.1.5.2.3.5);

– в сертификате контроллера домена в альтернативном имени субъекта (Subject Alternative Name) должно присутствовать DNS имя домена (например DNS=contoso.com);

– в сертификате контроллера домена имя субъекта (Subject Name) должно соответствовать DNS имени сервера (например, CN=dc1.contoso.com);

– все сертификаты ЦС и СОС, необходимые для построения полной цепочки сертификатов клиентов и контроллеров домена, должны находиться в соответствующих системных хранилищах сертификатов ЦС (в хранилище корневых сертификатов ЦС - для корневого сертификата и СОС цепочки, в хранилище промежуточных сертификатов - для промежуточных сертификатов ЦС и СОС цепочки) локального компьютера (см. подраздел 3).

При использовании точки распространения СОС, доступной по протоколу LDAP и расположенной в хранилище Microsoft Active Directory, к ней должен быть разрешен анонимный доступ посредством выполнения следующих действий:

– необходимо установить значение атрибута dsHeuristics, расположенного в контейнере CN=Directory Services,CN=Windows NT,CN=Services,CN=Configuration, в 0000002001001. Для изменения значения атрибута можно воспользоваться диалоговой программой adsiedit.msc;

– необходимо разрешить анонимный доступ к контейнеру точки распространения, в котором расположен СОС. Это также можно сделать с помощью диалоговой программы adsiedit.msc, разрешив доступ на чтение к указанному выше контейнеру пользователю NT AUTHORITY\АНОНИМНЫЙ ВХОД.

Для выполнения локального входа со смарт-картой пользователю ОС предыдущего поколения (ОС Windows XP/Server 2003) достаточно вставить смарт-карту в соответствующий считыватель (когда отображается Windows Login Screen). При этом ОС автоматически распознает вставленную смарт-карту, считает находящийся на ней сертификат (ОС предыдущего поколения поддерживают только один сертификат на смарт-карте) и предложит ввести ПИН-код, необходимый для чтения закрытого ключа клиента (Рисунок 10).

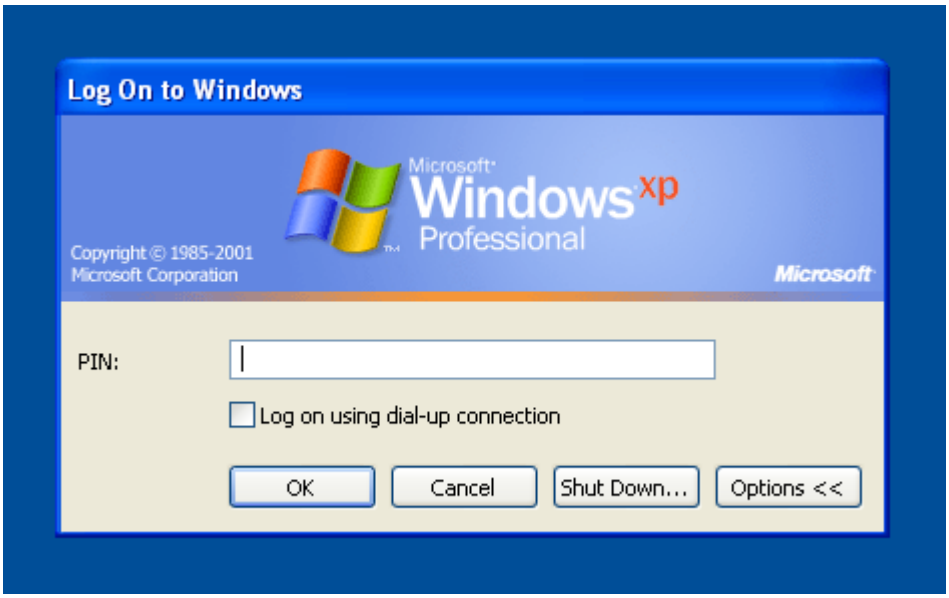

Рисунок 10 – Ввод ПИН-кода на ОС Windows XP

Для выполнения локального входа со смарт-картой пользователю современных ОС (ОС Windows Vista и выше) необходимо вставить смарт-карту в соответствующий считыватель и нажать Ctrl-Alt-Del (когда отображается Windows Login Screen). При этом ОС автоматически распознает вставленную смарт-карту, считает все находящиеся на ней сертификаты и предложит их список для выбора клиента (Рисунок 11).

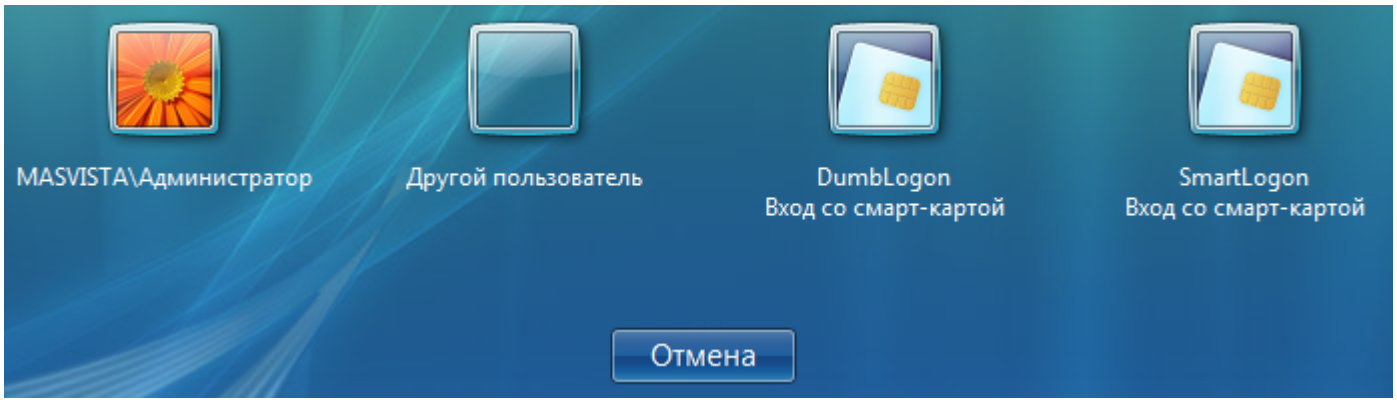

Рисунок 11 – Выбор сертификата на ОС Windows Vista

Далее, после выбора требуемого для входа сертификата клиента, выдаётся диалог ввода ПИН-кода, необходимого для чтения закрытого ключа клиента (Рисунок 12).

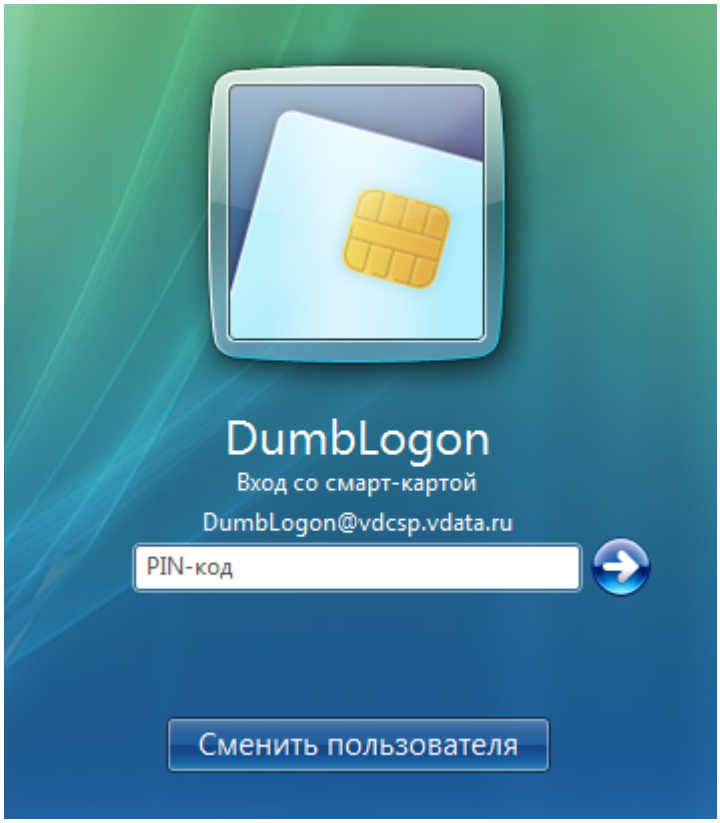

Рисунок 12 – Ввод ПИН-кода на ОС Windows Vista

После ввода ПИН-кода (как на ОС предыдущего поколения, так и на современных ОС), выполняется аутентификация пользователя в Microsoft Active Directory.

Для выполнения удаленного входа со смарт-картой необходимо использовать Remote Desktop Client (RDC) версии 6.0 или выше. Для ОС предыдущего поколения (ОС Windows XP) необходимо, чтобы тип используемой смарт-карты соответствовал настроенному считывателю закрытого ключа в конфигурации по умолчанию (для всех пользователей). Для современных ОС (ОС Windows Vista и выше) достаточно, чтобы тип используемой смарт-карты соответствовал настроенному считывателю закрытого ключа в конфигурации пользователя.

Пользователю ОС предыдущего поколения (ОС Windows XP) следует вставить смарт-карту в соответствующий считыватель и запустить RDC (программу MSTsc.exe), как это описано в подразделе 7. После ввода имени удаленного сервера терминалов (и имени шлюза служб терминалов, если это необходимо) и нажатия кнопки «Подключить» на экран будет выдано диалоговое окно с доступным на смарт-карте сертификатом (ОС предыдущего поколения поддерживают только один сертификат на смарт-карте) (Рисунок 13).

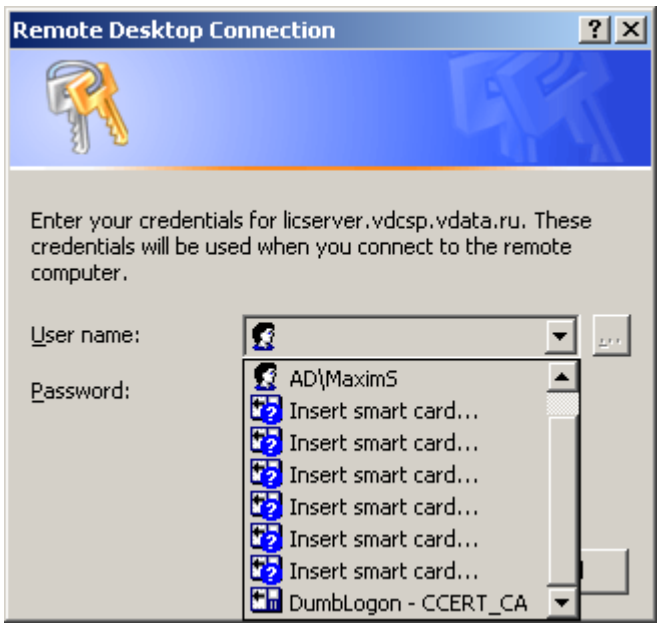

Рисунок 13 – Выбор сертификата и ввод ПИН-кода на ОС Windows XP

После выбора требуемого сертификата необходимо ввести ПИН-код для возможности доступа к закрытому ключу клиента.

Пользователю современных ОС (ОС Windows Vista и выше) следует выполнить те же действия, что описаны выше, за исключением того, что современные ОС поддерживают несколько сертификатов на смарт-карте (Рисунок 14).

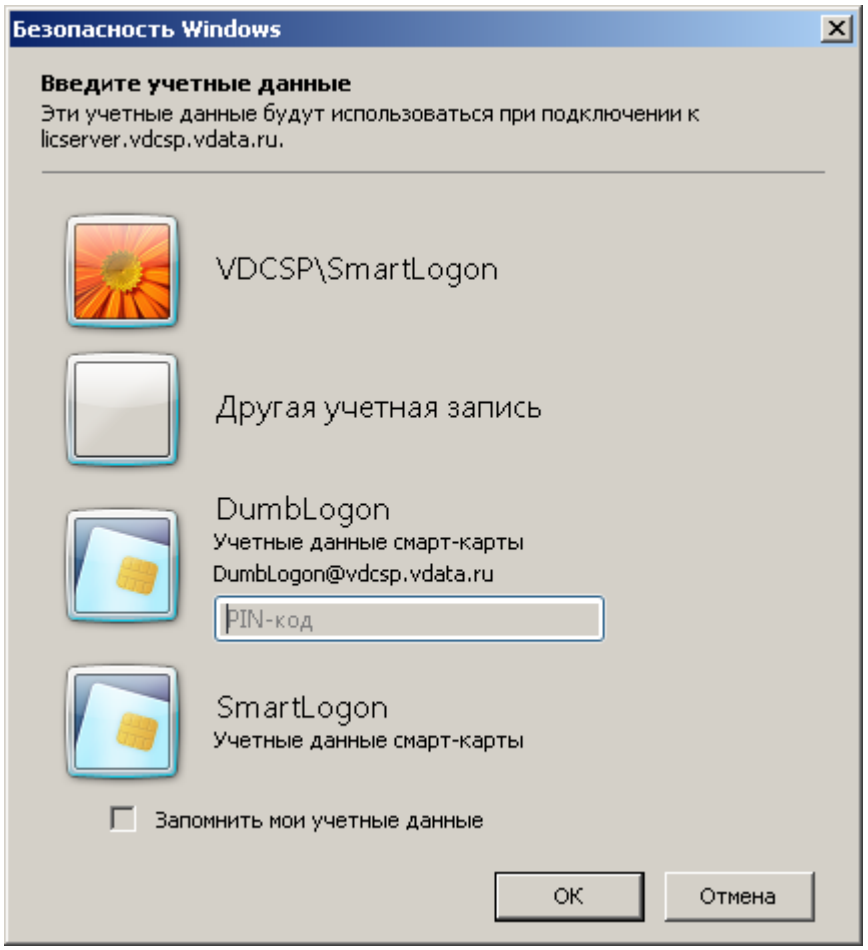

Рисунок 14 – Выбор сертификата и ввод ПИН-кода на ОС Windows Vista

После ввода ПИН-кода и нажатия на кнопку «ОК» (как на ОС предыдущего поколения, так и на современных ОС), выполняется подключение к удалённому рабочему столу и аутентификация пользователя в Microsoft Active Directory.

9 TLS МОНИТОР

TLS монитор предназначен для ведения списка клиентских программ, использующих исключительно сертифицированную реализацию протокола TLS криптопровайдера «Валидата CSP», для включения и выключения использования данного списка, а также для выполнения других настроек модуля поддержки TLS.

Список программ, использующих исключительно сертифицированную реализацию протокола TLS, настраивается каждым пользователем индивидуально. По умолчанию он содержит программы клиента Internet Explorer (IExplore.exe) и Remote Desktop Client (MSTsc.exe) и для подавляющего большинства пользователей не потребует никакой дополнительной настройки.

9.1 Запуск и включение TLS монитора

После запуска TLS монитора (программы vdtls_mon.exe) на панели задач появится новый значок (Рисунок 15).

Рисунок 15 – Значок TLS монитора на панели задач

TLS монитор после запуска всегда оказывается в выключенном состоянии, что обозначается красным крестом, перечёркивающим значок. Если подвести к нему курсор «мыши», появится всплывающая подсказка (Рисунок 16).

Рисунок 16 – Всплывающая подсказка TLS монитора

Если нажать на значок TLS монитора правой кнопкой «мыши», то появится контекстное меню (Рисунок 17).

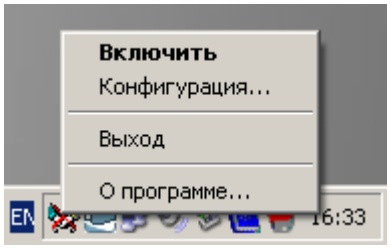

Рисунок 17 – Контекстное меню TLS монитора

Чтобы включить TLS выберите пункт меню «Включить» (или просто дважды щёлкните «мышью» на значке TLS монитора). Красный крестик на значке монитора исчезнет (Рисунок 18).

Рисунок 18 – TLS монитор включён

Чтобы выключить TLS монитор выберите в контекстном меню пункт «Выключить» или дважды щёлкните «мышью» на значке включённого TLS монитора.

Чтобы посмотреть информацию о версии TLS монитора (Рисунок 19), выберите в контекстном меню пункт «О программе ...».

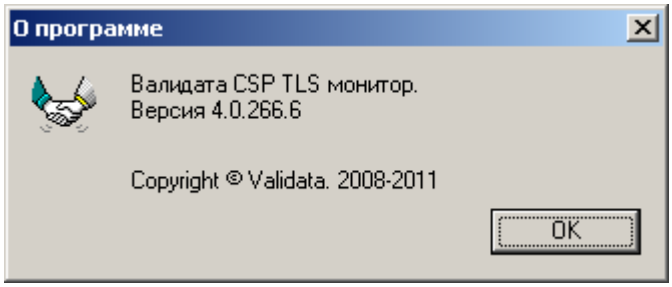

Рисунок 19 – Информация о версии TLS монитора

Для завершения работы TLS монитора выберите в контекстном меню пункт «Выход».

9.2 Конфигурация TLS монитора

Для того, чтобы запустить конфигурацию TLS монитора, выберите в контекстном меню пункт «Конфигурация ...» (Рисунок 20).

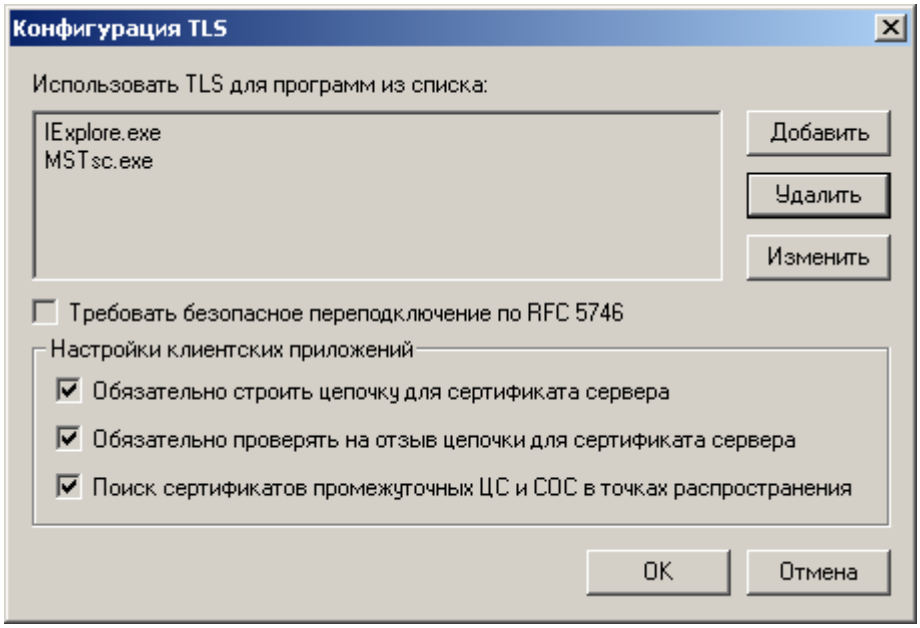

Рисунок 20 – Диалог конфигурации TLS

Чтобы добавить новый исполняемый модуль клиентской программы, который использует сертифицированную реализацию протокола TLS, нажмите кнопку «Добавить» и в стандартном диалоге открытия файла выберите требуемый модуль.

Чтобы удалить элемент списка, выделите его, нажмите кнопку «Удалить» и подтвердите своё решение (Рисунок 21).

Чтобы заменить один модуль другим, выберите модуль в списке, нажмите кнопку «Изменить» и в стандартном диалоге открытия файла выберите новый исполняемый модуль.

Вы можете также отредактировать имя исполняемого модуля вручную - для этого выберите модуль в списке и ещё раз нажмите на него «мышью» (Рисунок 22).

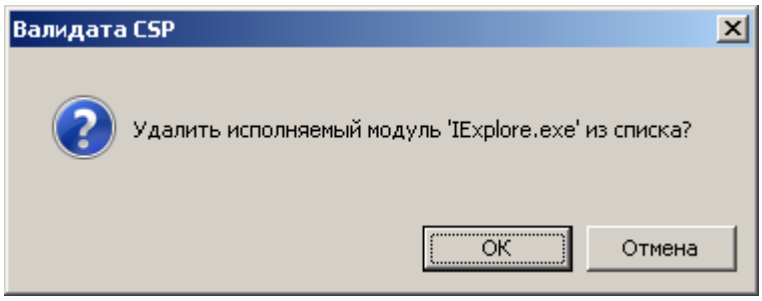

Рисунок 21 – Подтверждение удаления элемента списка

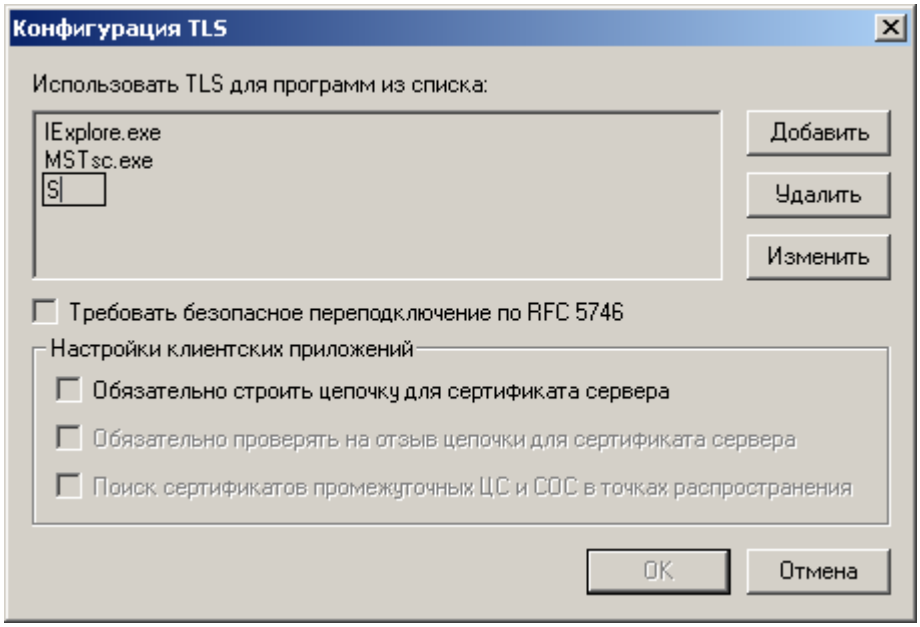

Рисунок 22 – Ручное редактирование элемента списка

Закончив редактирование, нажмите клавишу «Enter».

Кроме редактирования списка исполняемых модулей, TLS монитор позволяет выполнить следующие настройки модуля поддержки TLS (для их выполнения требуются права локального администратора, для вступления их в силу требуется перезагрузка):

– требовать безопасное переподключение по RFC 5746 - данная опция может быть настроена как для серверной стороны, так и для клиентской. Если данная опция включена, то все переподключения по созданию новой TLS сессии, выполняющиеся в контексте уже существующей TLS сессии, будут включать в себя криптографически связывающие TLS расширения. При этом, если по какой-то причине криптографически связывающие TLS расширения отсутствуют, то переподключение будет невозможно;

– игнорировать список владельцев сертификатов ЦС - данная опция может быть настроена как для серверной стороны, так и для клиентской. При аутентификации клиента на основании его сертификата сервер посылает список имен владельцев сертификатов ЦС (список имен издателей), которые разрешены в качестве издателей сертификатов клиентов. Клиент же, со своей стороны, проверяет наличие имени издателя сертификата сервера в этом списке. Если данная опция включена, то отрицательный результат поиска имени издателя сертификата в списке имен издателей будет проигнорирован. По умолчанию отрицательный результат поиска имени издателя сертификата в списке имен издателей приводит к ошибочному завершению процедуры

аутентификации;

– игнорировать предупреждения обмена в протоколе TLS - данная опция может быть настроена как для серверной стороны, так и для клиентской. Если данная опция включена, то все предупреждения обмена в протоколе TLS (TLS Alerts) будут проигнорированы. По умолчанию получение предупреждения обмена в протоколе TLS приводит к ошибочному завершению этого обмена;

– обязательно строить цепочку для сертификата сервера - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то построение и проверка цепочки сертификата сервера будет выполняться безусловно, независимо от поведения клиентского приложения. В этом случае, при ошибке построения или проверки цепочки сертификата сервера, защищенный канал связи между клиентом и сервером установлен не будет;

– обязательно проверять на отзыв цепочки сертификата сервера - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то проверка построенной цепочки сертификата сервера на отзыв будет выполняться безусловно, независимо от поведения клиентского приложения. В этом случае, при ошибке проверки цепочки сертификата сервера на отзыв, защищенный канал связи между клиентом и сервером установлен не будет;

– поиск сертификатов промежуточных ЦС и СОС в точках распространения - данная опция может быть настроена только для клиентской стороны. Если данная опция включена, то при построении цепочки сертификата сервера будет разрешена загрузка необходимых сертификатов промежуточных ЦС и СОС по сети из их точек распространения, независимо от поведения клиентского приложения.

– игнорировать безопасное переподключение по RFC 5746 - данная опция может быть настроена толко для серверной стороны. Если данная опция включена, то сервер будет игнорировать все криптографически связывающие TLS расширения, посылаемые клиентом. Таким образом, включение данной опции блокирует возможность безопасного переподключения.

Для того, чтобы внесённые изменения вступили в силу, нажмите кнопку «ОК».

ПЕРЕЧЕНЬ РИСУНКОВ

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					