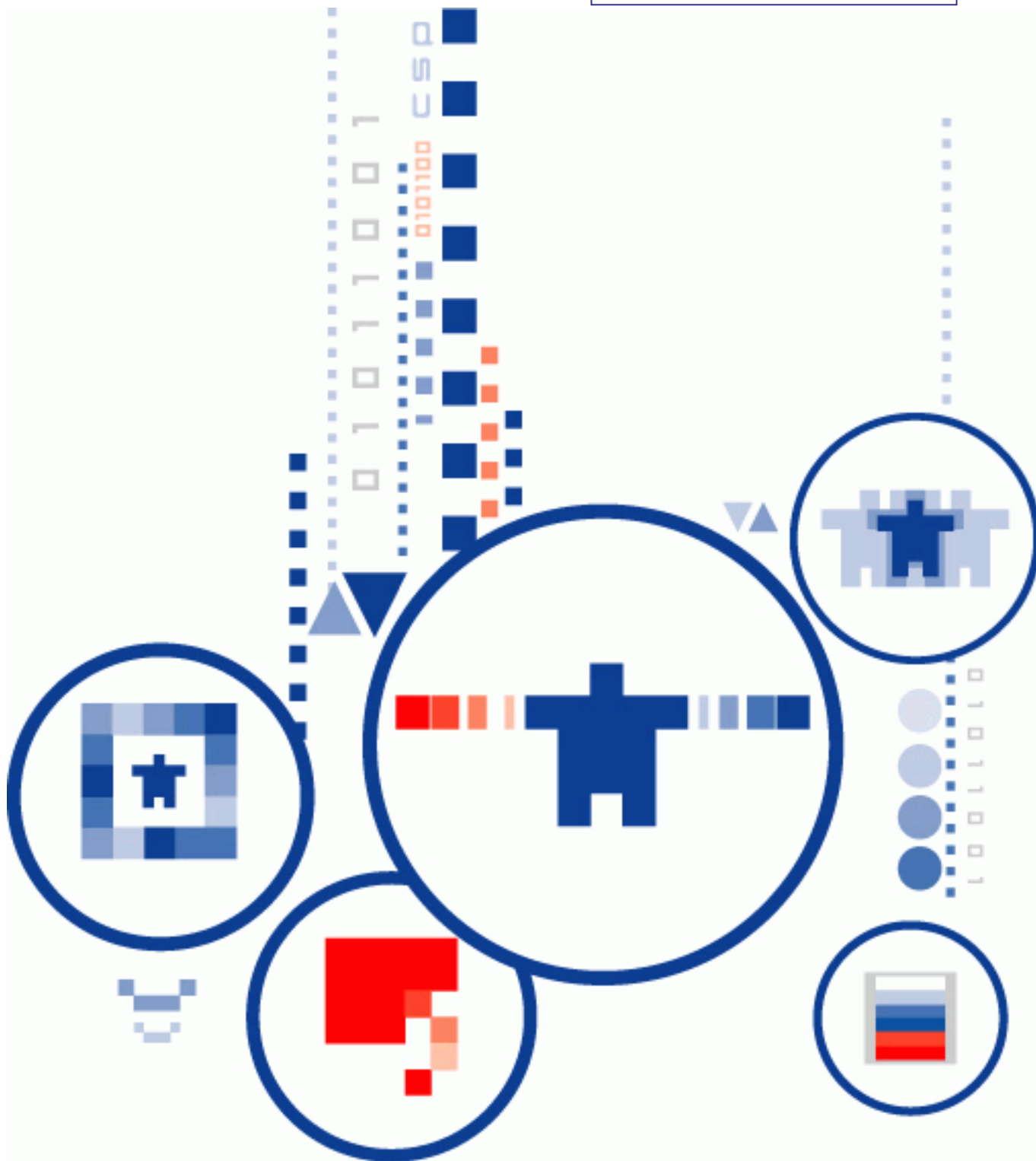




Службы УЦ

КриптоПро Revocation Provider

Версия 2.0

АННОТАЦИЯ

Настоящий документ содержит описание процесса установки и эксплуатации программного обеспечения «КристоПро Revocation Provider» (далее – Revocation Provider), предназначенной для проверки статусов сертификатов ключей проверки электронной подписи.

Документ предназначен для администраторов и пользователей как руководство по установке и эксплуатации «КристоПро Revocation Provider».

Информация о разработчике «КристоПро Revocation Provider»:

ООО «КРИПТО-ПРО»

127018, г. Москва, ул. Сущевский вал, д. 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

<https://www.CryptoPro.ru>

E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Установка Revocation Provider	4
1.1. Требования к аппаратному и программному обеспечению	4
1.2. Установка в интерактивном режиме	4
2. Описание работы Revocation Provider	9
2.1. Как вызывается Revocation Provider	9
2.2. Настройка приложений для проверки статусов сертификатов	9
2.3. Как работает Revocation Provider	9
2.4. Как проверяется OCSP-ответ	10
3. Настройка Revocation Provider	12
3.1. Групповые политики	12
4. Перечень сокращений	18
5. Перечень ссылочных документов	19

1. Установка Revocation Provider

1.1. Требования к аппаратному и программному обеспечению

Revocation Provider предназначен для функционирования в следующих ОС:

- Microsoft Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
- Microsoft Windows Server 2008 R2/2012/2012 R2/2016 (x64).

Требования к аппаратному обеспечению определяются требованиями ОС, на которой планируется эксплуатировать Revocation Provider.

1.2. Установка в интерактивном режиме

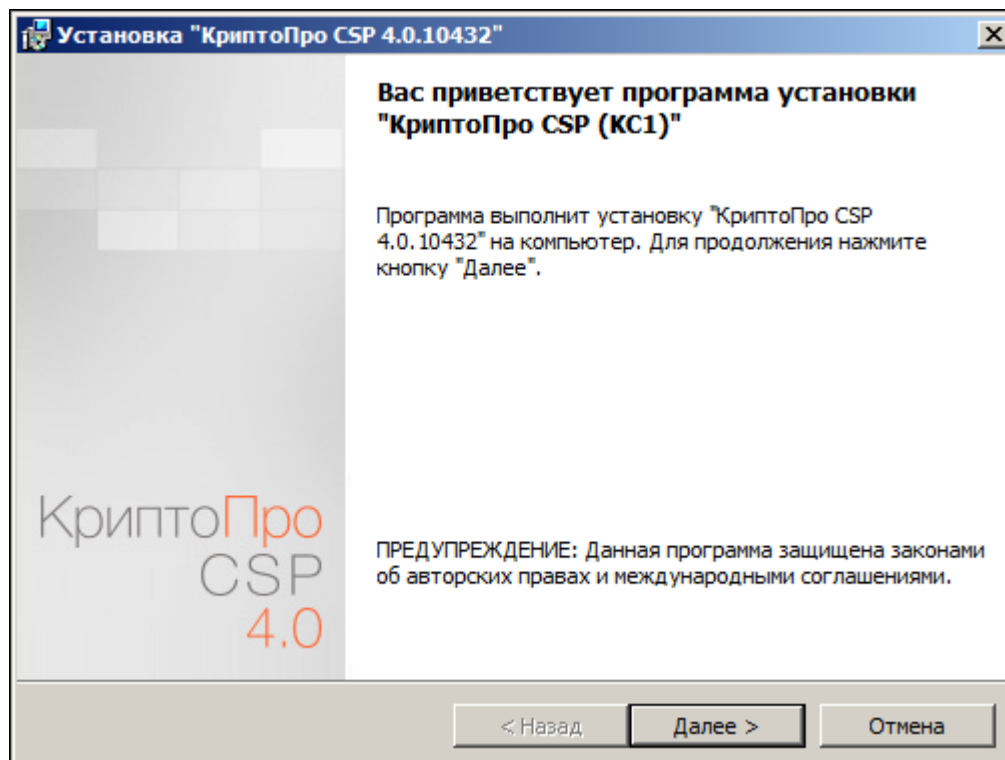
Установка Revocation Provider осуществляется в составе КриптоПро CSP:

1. Запустите с компакт-диска установку пакета в соответствии с версией ОС:

- Для **32-битных Windows** – **csp-win32-rus.msi**.
- Для **64-битных Windows** – **csp-x64-rus.msi**.

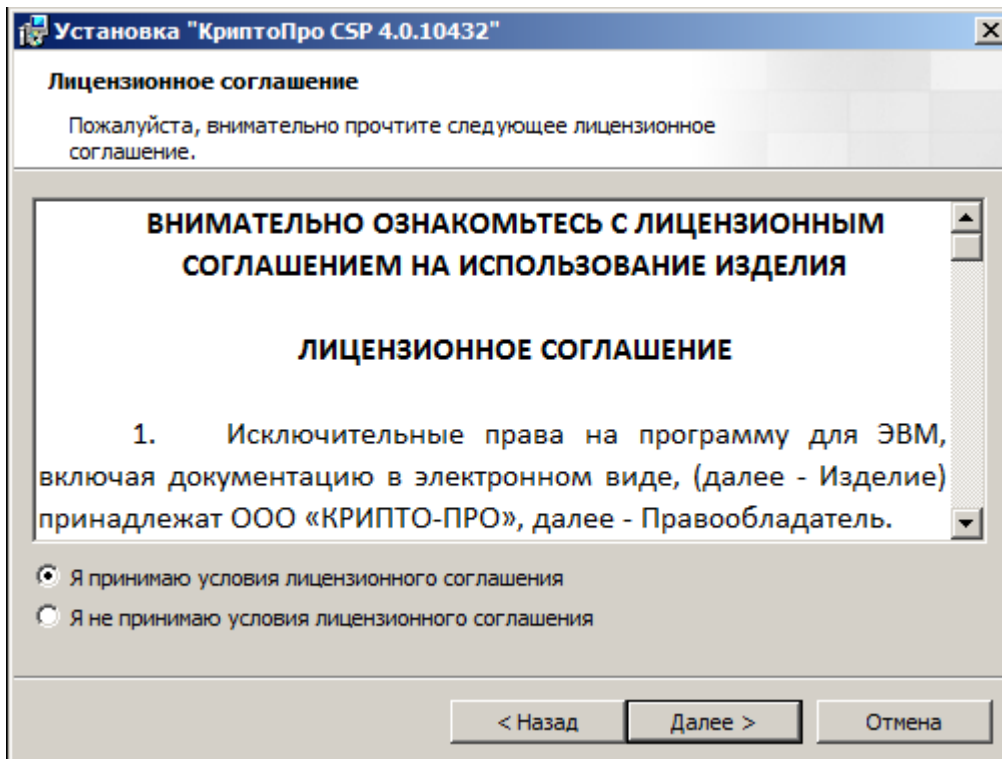
После коротких подготовительных процедур на экране появится окно мастера установки (см. Рисунок 1). Нажмите кнопку **Далее**.

Рисунок 1. Мастер установки КриптоПро CSP



2. В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование КриптоПро CSP. Если Вы согласны со всеми пунктами соглашения, выделите пункт **Я принимаю условия лицензионного соглашения**, и нажмите **Далее** (см. Рисунок 2).

Рисунок 2. Лицензионное соглашение на использование продукта



3. Следующим шагом необходимо ввести информацию о пользователе, производящем установку, и серийный номер лицензии на использование КриптоПро CSP (см. Рисунок 3).

Рисунок 3. Сведения о пользователе

Установка "КриптоПро CSP 4.0.10432"

Сведения о пользователе
Укажите сведения о себе.

Пользователь:

Организация:

Серийный номер:

Введите серийный номер, соответствующий лицензионному соглашению.
Без заданного серийного номера срок действия продукта три месяца.

< Назад Далее > Отмена

- После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 4), где необходимо выбрать вид установки. Для установки Revocation Provider необходимо выбрать выборочную установку. После этого будет предложено выбрать необходимые компоненты, которые будут установлены на локальный компьютер (см. Рисунок 5). Для установки Revocation Provider необходимо выбрать его в списке компонентов и включить в установку.

Рисунок 4. Вид установки

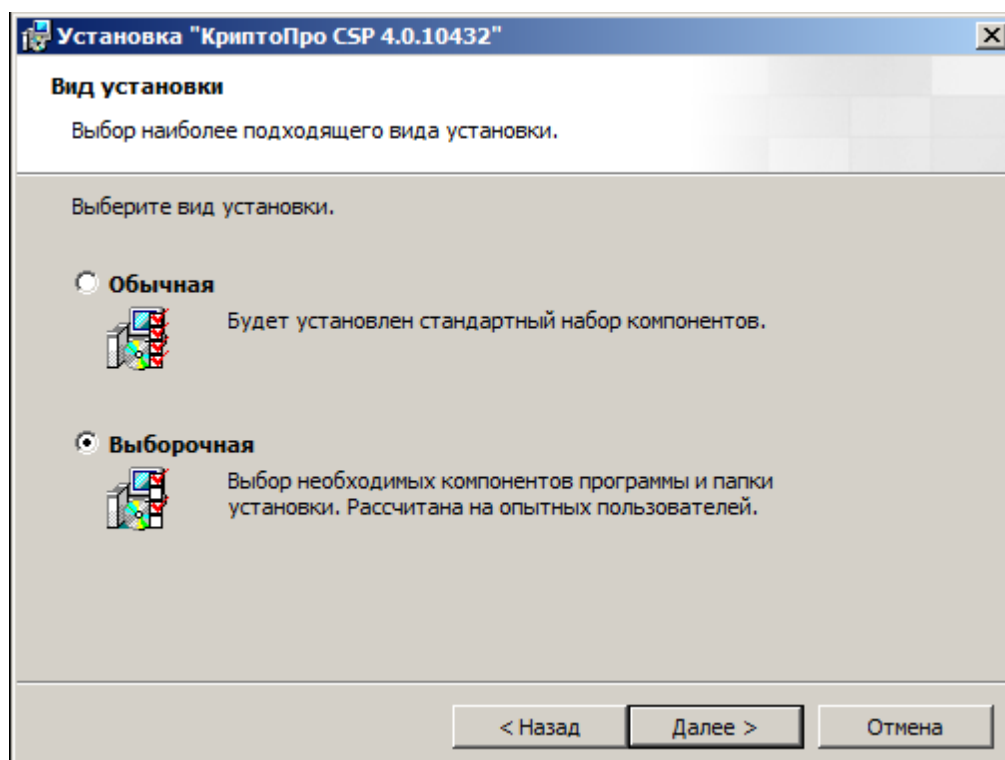
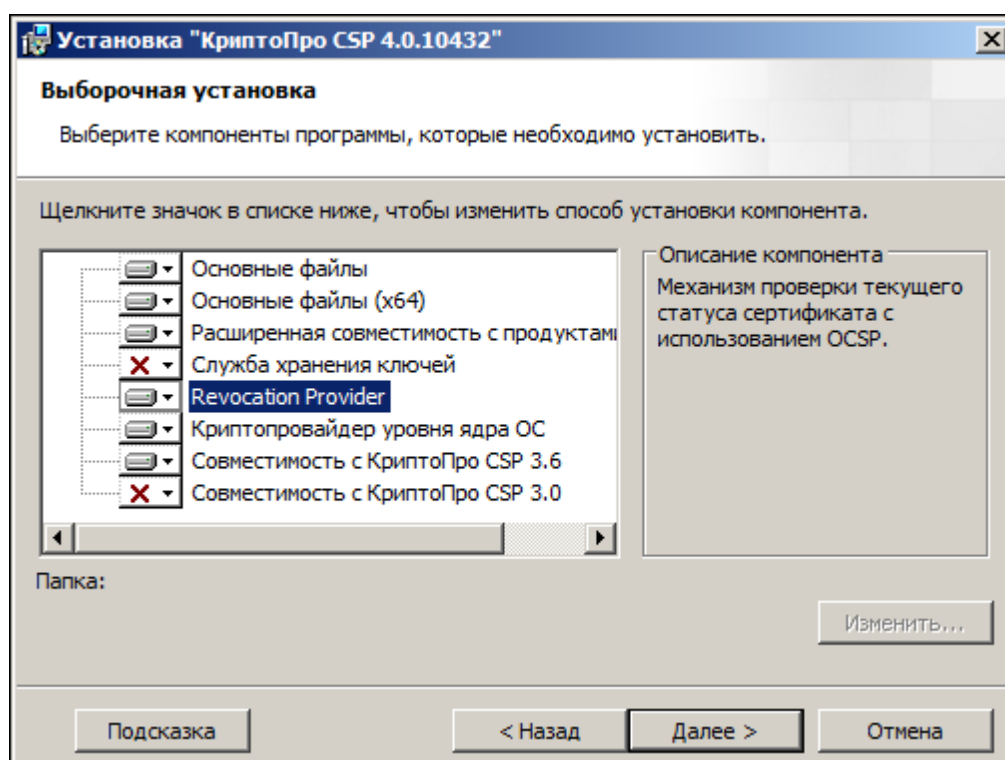
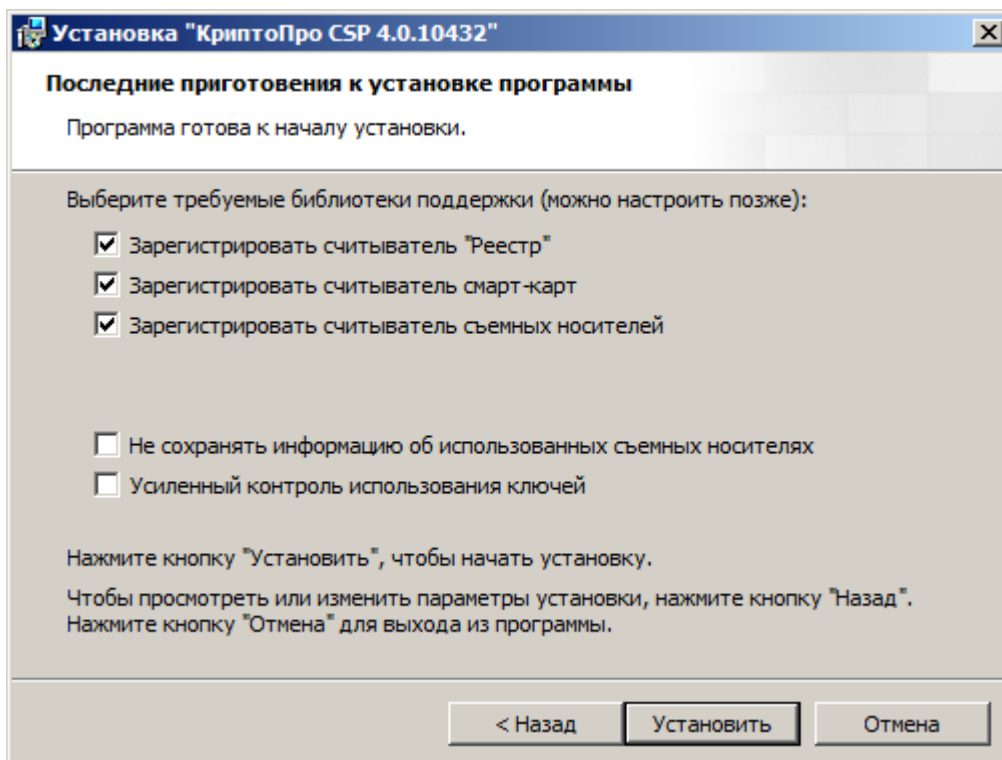


Рисунок 5. Выбор компонентов для установки



5. Следующее окно мастера служит для подтверждения установки и настройки дополнительных параметров (см. Рисунок 6). Для подтверждения нажмите кнопку **Установить**.

Рисунок 6. Окно подтверждения установки



После выполнения всех описанных шагов мастер устанавливает КриптоПро CSP вместе с Revocation Provider на локальный компьютер. По окончании установки мастер показывает окно с подтверждением успешной установки КриптоПро CSP, где необходимо нажать кнопку **Готово**. На данном этапе появится окно с сообщением о необходимости перезагрузки компьютера. Рекомендуется выполнить перезагрузку компьютера и начать работу с Revocation Provider.

2. Описание работы Revocation Provider

2.1. Как вызывается Revocation Provider

Будучи установленным в системе, Revocation Provider вызывается для проверки сертификата(ов) при каждом вызове функции CryptoAPI **CertVerifyRevocation**. Фактически, все параметры этой функции передаются без изменений в Revocation Provider. Помимо непосредственного вызова, эта функция, а значит и Revocation Provider, вызывается неявно внутри функций **CertGetCertificateChain** и **WinVerifyTrust**.

Подробнее об этих функциях, их параметрах и алгоритме работы можно узнать в соответствующих статьях Microsoft MSDN Library:

- **CertVerifyRevocation**—
<https://docs.microsoft.com/en-us/windows/desktop/api/wincrypt/nf-wincrypt-certverifyrevocation>
- **CertGetCertificateChain**—
<https://docs.microsoft.com/en-us/windows/desktop/api/wincrypt/nf-wincrypt-certgetcertificatechain>
- **WinVerifyTrust**—
<https://docs.microsoft.com/en-us/windows/desktop/api/wintrust/nf-wintrust-winverifytrust>

2.2. Настройка приложений для проверки статусов сертификатов

Большинство приложений, работающих с сертификатами ключей проверки электронной подписи, проверяют их статус с использованием описанных функций. Некоторые приложения имеют специальные настраиваемые параметры, управляющие этой проверкой.

2.3. Как работает Revocation Provider

Когда приложение, работающее с CryptoAPI, вызывает функцию проверки статуса сертификата, в Revocation Provider передаётся этот сертификат вместе с рядом дополнительных параметров.

Revocation Provider, получив на проверку сертификат, создаёт OCSP-запрос на данный сертификат и обращается к одной или нескольким службам OCSP с этим запросом. При получении OCSP-ответа, осуществляет его проверку. Если ответ проходит проверку и содержит статус сертификата **good** или **revoked**, в отличие от **unknown** (см. [1]), то на этом проверка заканчивается и полученный статус возвращается приложению. Если же ответ содержит статус **unknown** или не проходит проверку, то происходит обращение по следующему адресу.

Очередность обращения к службам OCSP определяется следующим образом:

1. По расширению AIA (AuthorityInformationAccess) в сертификате. Среди различных точек AIA выбирает те, к которым указан метод доступа по протоколу OCSP (см. [2]), обращения к ним происходят по очереди их расположения в сертификате.

2. Если ни по одному из адресов OCSP-серверов, указанных в расширении AIA сертификата, не удаётся получить удовлетворяющий этим условиям ответ, или если таких адресов в сертификате не указано, то Revocation Provider пробует обратиться за статусом к OCSP-серверу, адрес которого задан групповой политикой **Службы OCSP: адрес службы OCSP по умолчанию** (см. раздел 3), если она определена.

Если на предыдущих шагах не удаётся получить удовлетворяющий описанным условиям ответ, то сертификат передаётся на проверку в Microsoft Revocation Provider, входящий в состав ОС Windows. Microsoft Revocation Provider осуществляет проверку данного сертификата с использованием СОС. Полученный статус сертификата возвращается приложению.

2.4. Как проверяется OCSP-ответ

Проверка OCSP-ответа осуществляется в следующем порядке:

- Осуществляется поиск сертификата, которым подписан ответ. Сертификат ищется в самом OCSP-ответе, в хранилищах **AddressBook (Другие пользователи)**, **CA (Промежуточные центры сертификации)**, **ROOT (Доверенные корневые центры сертификации)**. Если сертификат найти не удаётся, ответ проверить нельзя.
- Проверяется подпись службы OCSP под ответом на найденном сертификате.
- По сертификату службы проверяется, уполномочен ли данный OCSP-сервер Удостоверяющим Центром, издавшим сертификат, чей статус запрашивался, выдавать информацию о статусе данного сертификата (см. [1], подраздел 4.2.2.2). OCSP-сервер считается уполномоченным, если он подписал OCSP-ответ тем же ключом, которым подписан сертификат, чей статус запрашивался, или если сертификат OCSP-сервера подписан этим ключом и содержит в расширении ECU назначение **Подпись ответов службы OCSP (id-kp-OCSPSigning)**. Кроме этого, возможен следующий вариант.
- Если сертификат службы перечислен в групповой политике **Службы OCSP: сертификаты уполномоченных служб OCSP** (см. раздел 3), то он проходит данную проверку.
- Строится и проверяется цепочка сертификатов для сертификата службы. Проверяются статусы всех сертификатов цепочки, кроме корневого. На этом этапе происходят повторные обращения к Revocation Provider, которые обрабатываются в точности по описанному алгоритму. Если сертификат службы содержит расширение **Признак доверия службе OCSP (id-pkix-ocsp-nocheck)** (см. [1], подраздел 4.2.2.2.1), или он перечислен в групповой политике **Службы OCSP: непроверяемые на отзыв сертификаты служб OCSP** (см. раздел 3), то его статус не проверяется.



Если сертификат службы OCSP содержит расширение **id-pkix-ocsp-nocheck**, то его статус, согласно [1], не проверяется. Это может быть удобным во избежание необходимости распространения СОС в системе, в которой внедряется протокол OCSP, но нужно иметь в виду, что в данном случае компрометация ключа службы OCSP почти так же нежелательна по своим последствиям, как и компрометация ключа УЦ. При использовании данного расширения рекомендуется установить в регламенте УЦ небольшой срок действия сертификатов служб OCSP.

3. Настройка Revocation Provider

Настройка Revocation Provider производится администратором компьютера или домена с помощью групповых политик (group policy).

Revocation Provider в своей работе использует функции КриптоПро OCSP Client, поэтому групповые политики, настраиваемые для OCSP-клиента влияют непосредственно на функционирование Revocation Provider.

Групповые политики КриптоПро OCSP Client, описаны в файле административного шаблона **ocspcli.adm**. На компьютере, где установлен КриптоПро OCSP Client (устанавливается вместе с Revocation Provider), этот файл располагается в папке **%WinDir%\GroupPolicy\Adm** и уже подключен в оснастке **Групповая политика**. Для настройки политик в домене потребуется скопировать шаблон на контроллер домена и подключить его в оснастке **Групповая политика**.

Все политики могут задаваться как для пользователя, так и для компьютера, причем политика компьютера имеет преимущество перед политикой пользователя. Политики располагаются в узле **Крипто-Про\Клиент службы актуальных статусов сертификатов**. В настоящем разделе приводится описание этих групповых политик.

3.1. Групповые политики

Nonce: включать расширение 'nonce' в запрос по умолчанию

Определяет, будет ли клиент по умолчанию включать расширение 'nonce' в OCSP-запросы.

Nonce: запретить использование расширения 'nonce' в запросах

Позволяет запретить клиенту включать расширение 'nonce' в запросы на OCSP-запросы.

См. также политику "Nonce: требовать использование расширения 'nonce' в запросах".

Nonce: размер значения расширения 'nonce' в запросах

Определяет размер значения расширения 'nonce' (в байтах), включаемого клиентом в запросы.

Nonce: требовать использование расширения 'nonce' в запросах

Позволяет запретить клиенту отправлять OCSP-запросы не имеющие расширения 'nonce'.

См. также политику "Nonce: запретить использование расширения 'nonce' в запросах".

Аутентификация (прокси-сервер): запрещенные типы

Определяет типы аутентификации, которые запрещено использовать для подключения к прокси-серверу.

Если необходимо, например, запретить соединения без использования SSL, то можно запретить все типы аутентификации в данной политике.

Аутентификация (прокси-сервер): запрещенные типы (с использованием SSL)

Определяет типы аутентификации, которые запрещено использовать для подключения к прокси-серверу при использовании SSL-соединения.

Если необходимо, например, запретить соединения с использованием SSL, то можно запретить все типы аутентификации в данной политике.

Аутентификация (прокси-сервер): тип по умолчанию

Позволяет задать тип аутентификации, используемый по умолчанию при соединении с прокси-сервером.

Аутентификация (прокси-сервер): тип по умолчанию (с использованием SSL)

Позволяет задать тип аутентификации (с SSL), используемый по умолчанию при соединении с прокси-сервером.

Аутентификация: запрещенные типы

Определяет типы аутентификации, которые запрещено использовать для подключения к службе OCSP.

Если необходимо, например, запретить соединения без использования SSL, то можно запретить все типы аутентификации в данной политике.

Аутентификация: запрещенные типы (с использованием SSL)

Определяет типы аутентификации, которые запрещено использовать для подключения к службе OCSP при использовании SSL.

Если необходимо, например, запретить соединения с использованием SSL, то можно запретить все типы аутентификации в данной политике.

Аутентификация: тип по умолчанию

Позволяет задать тип аутентификации, используемый по умолчанию для подключения к службе OCSP.

Аутентификация: тип по умолчанию (с использованием SSL)

Позволяет задать тип аутентификации (с SSL), используемый по умолчанию для подключения к службе OCSP.

Запрос: алгоритм используемый для хеширования данных

Определяет идентификатор (OID) алгоритма хеширования, используемого клиентом для хеширования различных полей при создании OCSP-запроса.

Значением, установленным политикой является часть строки до пробела, остальная часть строки считается комментарием.

Запрос: запретить неподписанные запросы

Позволяет запретить отправку неподписанных OCSP-запросов.

Запрос: запретить подписанные запросы

Позволяет запретить отправку подписанных OCSP-запросов.

Запрос: сертификаты, включаемые в OCSP-запрос

Определяет, какие сертификаты включать в OCSP-запрос. Эти сертификаты могут понадобиться службе OCSP для проверки подписи запроса.

Возможные варианты:

- не включать сертификаты;
- сертификат подписчика;
- цепочку кроме корневого сертификата;
- цепочку сертификатов целиком.

Ответ: максимальное расхождение времени получения ответа и времени подписи

Данная политика определяет максимально возможное расхождение времени получения ответа от службы OCSP и времени, когда служба его подписала. Эта политика используется в случае, если ни в запросе, ни в

ответе не присутствует расширение 'nonce', для подтверждения соответствия выданного OCSP-ответа запросу на него.

Значение задается в миллисекундах.

Если расхождение больше, чем указано в политике, то ответ признается некорректным.

Если политика не задана, то используется значение 3 минуты.

Ответ: максимальная давность поля "ThisUpdate"

Данная политика определяет максимально возможную давность поля "ThisUpdate" OCSP-ответа, содержащего время выпуска СОС, по которому был определен статус сертификата.

Значение задается в миллисекундах.

Если расхождение больше, чем указано в политике, то ответ признается некорректным.

Если политика не задана, то используется значение 1 день.

Ответ: не использовать стандартный Revocation Provider Windows

Запрещает использование стандартного Revocation Provider Windows (cryptnet.dll) при проверке сертификата службы OCSP на отзыв в случае, если его статус не удалось определить по протоколу OCSP.

Прокси-серверы: прокси-сервер по умолчанию

Определяет прокси-сервер, используемый по умолчанию при подключении к службе OCSP.

Формат: "<протокол>://<сервер>[:порт]". Здесь в качестве протокола можно указать "http" или "https".

Прокси-серверы: разрешенные прокси-серверы

Определяет адреса разрешенных прокси-серверов.

Если политика не задана, то разрешены любые прокси-серверы.

Службы OCSP: адрес службы OCSP по умолчанию

Определяет адрес службы OCSP по умолчанию.

Формат адреса: "<протокол>://<сервер>[:порт]/[путь]". Здесь в качестве протокола можно указать "http" или "https".

Службы OCSP: непроверяемые на отзыв сертификаты служб OCSP

Этой политикой можно определить сертификаты служб OCSP, которые не следует проверять на отзыв.

Службы задаются посредством перечисления значений хэш-функций (по алгоритму SHA-1) их сертификатов в шестнадцатеричном виде. Получить это значение для сертификата можно в стандартном окне Windows для его отображения, выбрав на вкладке "Состав" в списке атрибутов "Печать" (зависит от операционной системы, обычно последний в списке). Значение может содержать пробелы.

Службы OCSP: разрешенные службы OCSP

Определяет адреса служб OCSP, к которым клиент может обращаться.

Если политика не задана, то разрешены любые службы OCSP.

Службы OCSP: сертификаты уполномоченных служб OCSP

Этой политикой можно определить сертификаты служб OCSP, наделенных полномочиями выдавать ответы со статусами любых сертификатов. Не заданные в данной политике службы проходят проверку на то, что они уполномочены Удостоверяющим Центром, издавшим проверяемый сертификат, выдавать информацию о статусе данного сертификата (см. [1], подраздел 4.2.2.2).

Службы задаются посредством перечисления значений хэш-функций (по алгоритму SHA-1) их сертификатов в шестнадцатеричном виде. Получить это значение для сертификата можно в стандартном окне Windows для его отображения, выбрав на вкладке "Состав" в списке атрибутов "Печать" (зависит от операционной системы, обычно последний в списке). Значение может содержать пробелы.

Типы ответов: включать расширение 'AcceptableResponses' в запрос по умолчанию

Определяет, будет ли клиент по умолчанию включать расширение 'AcceptableResponses' в OCSP-запросы.

Типы ответов: запретить использование расширения 'AcceptableResponses' в запросах

Позволяет запретить клиенту включать расширение 'AcceptableResponses' в OCSP-запросы.

См. также политику "Типы ответов: требовать использование расширения 'AcceptableResponses' в запросах".

Типы ответов: требовать использование расширения 'AcceptableResponses' в запросах

Позволяет запретить клиенту отправлять OCSP-запросы не имеющие расширение 'AcceptableResponses'.

См. также политику "Типы ответов: запретить использование расширения 'AcceptableResponses' в запросах".

4. Перечень сокращений

EKU	Расширенное использование ключа (Extended Key Usage)
OCSP	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
RFC	Рекомендация Internet Engineering Task Force (Request for Comments)
SSL	Протокол защиты сокетов (Secure Sockets Layer)
TLS	Протокол защиты транспортного уровня (Transport Layer Security)
ИОК	Инфраструктура открытых ключей (Public Key Infrastructure)
СОР	Список отзыва сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

5. Перечень ссылочных документов

1. Santesson, S., et al., "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP", IETF, RFC 6960, June 2013.
2. Cooper, D., et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", IETF, RFC5280, May 2008.