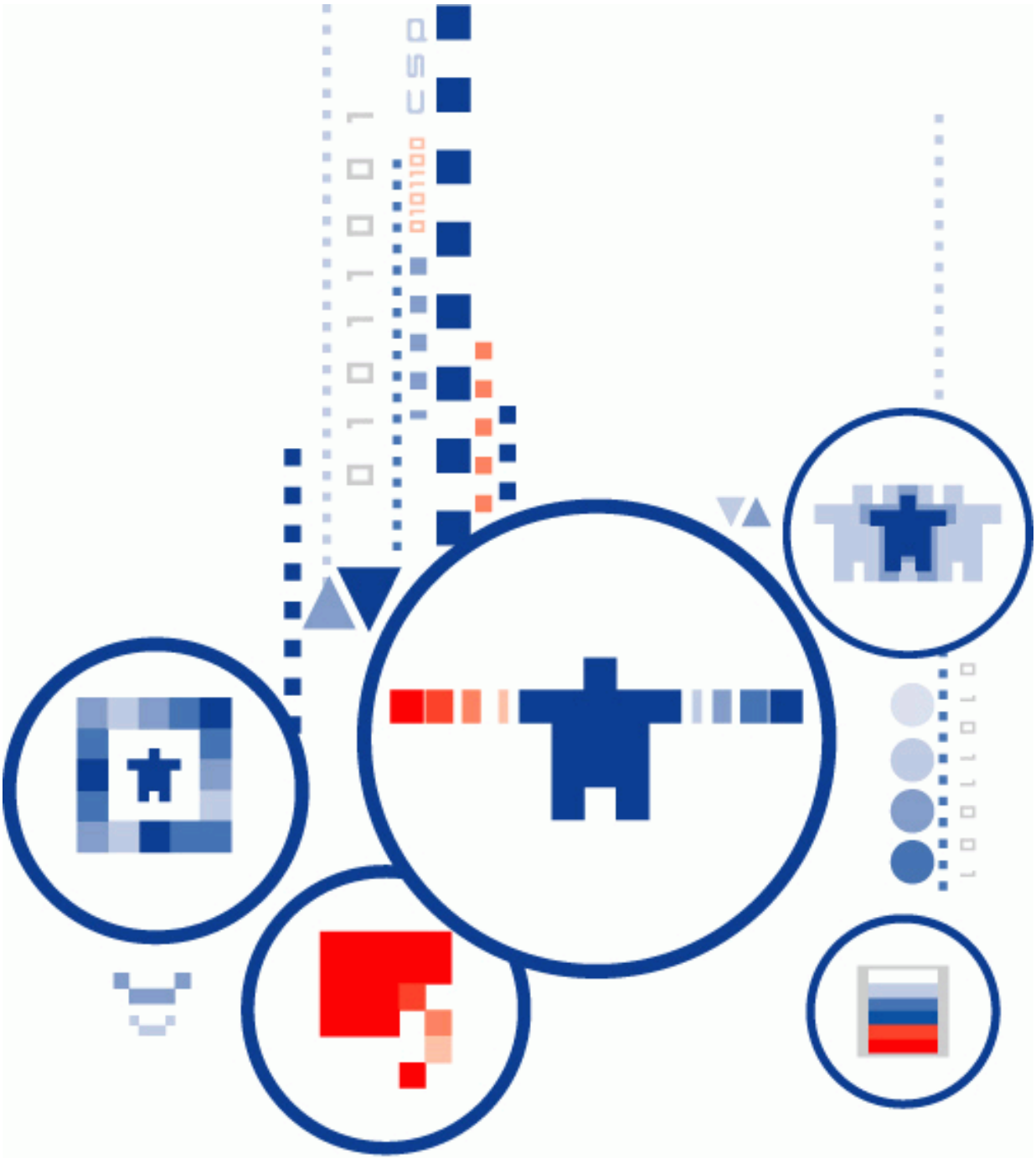

Служба проверки сертификатов и электронной подписи

КриптоПро SVS

Общее Описание

АННОТАЦИЯ

Настоящий документ содержит описание программного комплекса Службы проверки сертификатов и электронной подписи «КриптоПро SVS» (ПК «КриптоПро SVS»).

Документ предназначен для администраторов как ознакомительный материал перед установкой и эксплуатацией КриптоПро SVS.

Информация о разработчике «КриптоПро SVS»:

ООО «КРИПТО-ПРО»
127018, Москва, ул. Сущёвский вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Общие сведения о КриптоПро SVS

1.1. Назначение КриптоПро SVS

Криптографическая защита информации в современных системах осуществляется с использованием сертификатов открытых ключей на основе инфраструктуры открытых ключей (ИОК, PKI). Задачей ИОК является определение политики выпуска цифровых сертификатов, выдача их и прекращение действия, хранение информации, необходимой для последующей проверки правильности сертификатов. В число приложений, поддерживающих ИОК, входят: защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной подписью (ЭП).

Для удостоверения факта принадлежности ключевой пары определенному субъекту (объекту) в ИОК служит сертификат ключа проверки – подписанный ЭП электронный документ, содержащий информацию о владельце ключевой пары и ключ проверки. Подпись сертификатов осуществляется доверенной третьей стороной – Удостоверяющим центром (УЦ). Доверие к ключевой паре УЦ также основывается на его сертификате, который может быть подписан либо вышестоящим УЦ, либо самим УЦ.

В процессе управления ключами УЦ имеет возможность отзыва выпущенных им сертификатов, что необходимо для досрочного прекращения их действия, например, в случае компрометации ключа. Процедура проверки ЭП предусматривает помимо подтверждения ее математической корректности еще и построение, и проверку цепочки сертификатов до доверенного УЦ, а также проверку статусов сертификатов в цепочке.

Таким образом, проверка статусов сертификатов важна как для приложений, использующих ИОК, так и при ведении документооборота с использованием ЭП, поскольку, например, принятие к обработке подписанного ЭП документа, соответствующий сертификат ключа проверки электронной подписи которого прекратил действие, может быть впоследствии оспорено и привести к финансовым потерям.

Для выполнения процедур верификации сертификата ключа проверки электронной подписи и подтверждения подлинности электронных подписей документов может быть использована Служба проверки сертификатов и электронной подписи «КриптоПро SVS» (далее — КриптоПро SVS), которая кроме удобного пользовательского интерфейса предоставляет также программные интерфейсы на основе веб-сервисов (SOAP, REST).

1.2. Требования к клиентскому рабочему месту

Операции верификации сертификата ключа проверки электронной подписи и подтверждения подлинности электронных подписей документов выполняются на стороне сервера, что не требует установки на компьютер клиента специализированного программного обеспечения (например, КриптоПро PDF, Крип-тоПро Office Signature, КриптоАРМ). Вся работа клиента с КриптоПро SVS производится через веб-браузер.

Для обеспечения доверия к ответам сервиса КриптоПро SVS взаимодействие с ним может производиться по протоколу TLS.

1.3. Поддерживаемые форматы электронной подписи

КриптоПро SVS поддерживает следующие форматы электронной подписи:

- Подпись формата CMS (PKCS#7/CAdES BES, см. [RFC5652])
  - Присоединенная подпись;
  - Отделенная подпись;
- Усовершенствованная подпись (CAdES-T, CAdES-X Long Type 1);
  - Присоединенная подпись;
  - Отделенная подпись;

- Подпись XML-документов (XML Digital Signature, XMLDSig);
- Необработанная (чистая) электронная подпись ГОСТ Р 34.10–2001, ГОСТ Р 34.10-2012;
- Подпись документов PDF (CAdES BES, CAdES-T, CAdES-X Long Type 1);
- Подпись документов Microsoft Office (Word и Excel).

1.4. Возможности КриптоПро SVS

На сервере, обеспечивающем работу КриптоПро SVS, устанавливаются следующие компоненты:

- Веб-интерфейс Пользователя,
- SOAP-сервис Проверки Подписи,
- REST-сервис Проверки Подписи.

Настройка конфигурации и администрирование сервиса производится с помощью Windows PowerShell.

КриптоПро SVS использует встроенный в ОС механизм проверки цепочки сертификатов, используя собственное хранилище корневых сертификатов УЦ. Это означает, что необходимые для построения цепочки сертификаты, CRL или OCSP-ответы берутся из системных хранилищ или скачиваются автоматически.

Веб-интерфейс КриптоПро SVS можно использовать не только как самостоятельный сервис, но и интегрировать в Веб-интерфейс Сервиса Подписи в составе СЭП «КриптоПро DSS».

При проверке документов в веб-интерфейсе КриптоПро SVS в браузере может отображаться содержимое документов. Поддерживаются следующие форматы документов: PDF, DOC, DOT, DOCM, DOTM, DOCX, DOTX, XML, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, ODT, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML и TXT.

Набор отображаемых документов может быть расширен путём написания плагинов для нужных форматов (см. документ «ЖТЯИ.00094-01 94 03 Службы УЦ 2.0. КриптоПро SVS. Руководство разработчика»).

В качестве криптопровайдера может быть использовано СКЗИ «КриптоПро CSP» версии 4.0 варианта исполнения 2-Base или 3-Base.

В качестве OCSP-сервера может использоваться КриптоПро OCSP Server или другой совместимый соответствующий требованиям RFC 6960.

2. Варианты использования КриптоПро SVS

КриптоПро SVS позволяет организовать процедуры верификации сертификата ключа проверки электронной подписи и подтверждения подлинности электронных подписей для клиентов и встроить функциональности этих процедур в различные приложения.

1. Обращение Пользователя к КриптоПро SVS происходит одним из способов:
    a. Пользователь КриптоПро SVS запрашивает у сервера проверку сертификата или подписи через веб-интерфейс КриптоПро SVS;
    b. Пользователь обращается к КриптоПро SVS через приложение, реализованное с использованием SOAP-сервиса проверки подписи.
2. Если затребована проверка подписи, проверяется математическая корректность подписи, затем проверяется сертификат.
3. Для проверки сертификата строится цепочка до доверенного корневого УЦ.
4. Сервер КриптоПро SVS определяет статус проверяемого сертификата и всей цепочки до сертификата корневого УЦ одним из вариантов:
    a. обращением к CRL, который хранится на этом сервере и регулярно обновляется;
    b. обращением непосредственно к серверу УЦ, предназначенному для публикации актуального CRL;
    c. обращением к OCSP-серверу по протоколу OCSP.
5. Ответ возвращается пользователю.

Схема использования КриптоПро SVS представлена на Рисунке 1.

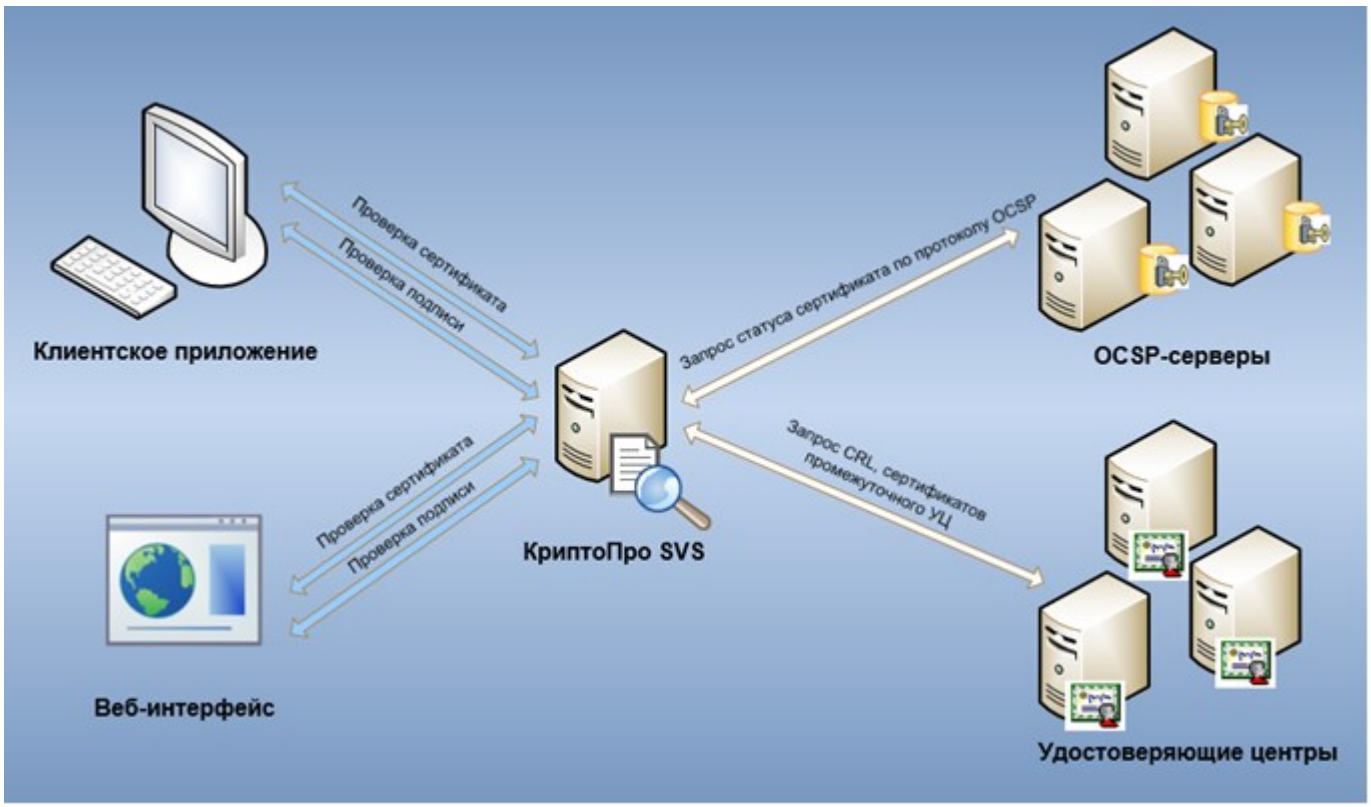

Рисунок 1 — - Схема использования КриптоПро SVS

3. Ключевые особенности КриптоПро SVS

Служба проверки сертификатов и электронной подписи КриптоПро SVS имеет следующие ключевые особенности:

- Реализует проверку сертификатов и электронной подписи с учётом использования российских криптографических алгоритмов.
- Использует встроенный веб-сервер Microsoft IIS, поддерживающий различные методы аутентификации и протокол TLS (SSL).
- Поддерживает развёртывание нескольких экземпляров службы на одном компьютере.
- Может получать информацию о статусах сертификатов из следующих источников:
  - Локально установленные списки отзыва сертификатов (CRL);
  - CRL, доступные по сети;
  - Сервисы OCSP.
- Процесс проверки статусов сертификатов реализуется средствами ОС Windows и средствами КриптоПро SDK (см. документ ЖТЯИ.00094-01 90 10. «Службы УЦ. КриптоПро PKI SDK. Руководство разработчика»).
- Устанавливается с помощью Windows Installer.

4. Перечень сокращений

CSP	Криптопровайдер (Cryptographic Service Provider)
IIS	Internet Information Services
IP	Центр идентификации (Identity Provider)
URL	Единый указатель ресурсов (Uniform Resource Locator)
WCF	Windows Communication Foundation
БД	База данных
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СЭП	Сервер электронной подписи
ЭЦП	Электронная цифровая подпись
ЦИ	Центр идентификации
OTP	One-time password (одноразовый пароль)
МФА	Многофакторная аутентификация
УЦ	Удостоверяющий Центр
HOTP	Алгоритм аутентификации с использованием одноразовых паролей на основе HMAC (HMAC-Based One-Time Password Algorithm)