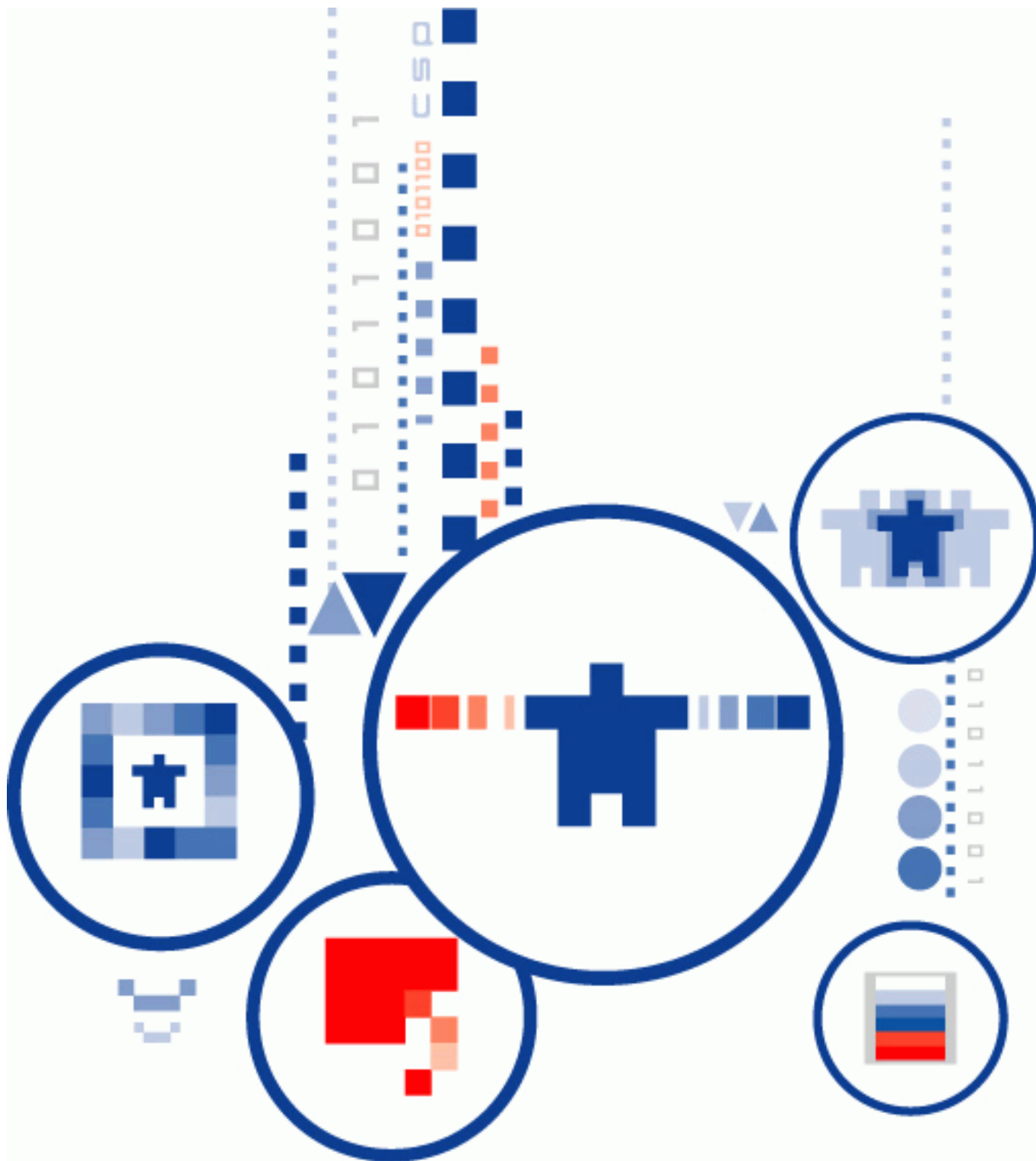




Службы УЦ

КриптоПро OCSP Server

Версия 2.0

**Использование КриптоПро OCSP Server совместно с
КриптоПро УЦ**

АННОТАЦИЯ

Настоящий документ содержит описание вариантов совместного использования продуктов КриптоПро OSCP Server и КриптоПро УЦ для предоставления пользователям актуальной информации о статусах сертификатов по протоколу OSCP.

Рассматривается вариант использования в качестве источника информации о статусах сертификатов базы данных Реестра сертификатов КриптоПро УЦ, а также резервирования этого источника с помощью списков отзыва сертификатов (COC).

Описывается способ организации доступа пользователей к OSCP-серверам, обеспечивающий отказоустойчивость.

Приводится сравнение различных методов предоставления информации о статусах сертификатов пользователям.

Информация о разработчике ПК «КриптоПро OSCP Server» и «КриптоПро УЦ»:

ООО «КРИПТО-ПРО»
127018, г. Москва, ул. Суцевский вал, д. 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
<https://www.cryptopro.ru>
E-mail: info@cryptopro.ru

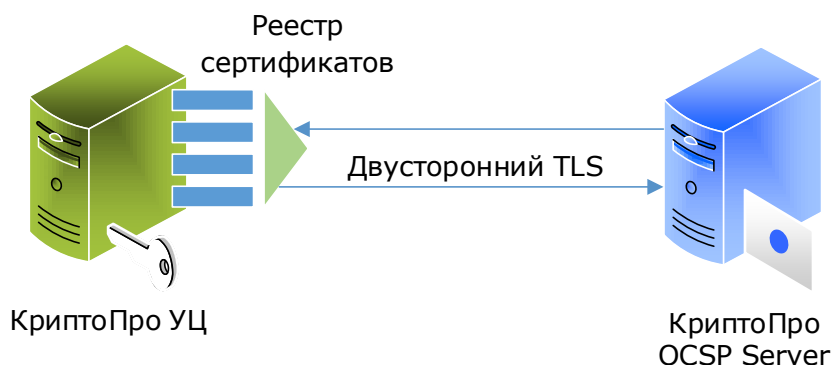
СОДЕРЖАНИЕ

1. Типовая схема взаимодействия	4
1.1. Работа по базе данных Реестра сертификатов КриптоПро УЦ	4
1.2. Работа с использованием списков отозванных сертификатов	5
2. Указание адресов OSCP для обеспечения отказоустойчивости	6
3. Сравнение методов предоставления информации о статусах сертификатов	7
4. Перечень сокращений.....	8
5. Перечень ссылочных документов.....	9

1. Типовая схема взаимодействия

На рисунке (см. Рисунок 1) представлена Схема доступа к Реестру сертификатов КриптоПро УЦ.

Рисунок 1. Схема доступа к Реестру сертификатов КриптоПро УЦ



Источниками информации о статусах сертификатов для КриптоПро OSCP Server могут являться:

- БД Реестра сертификатов КриптоПро УЦ;
- Списки сертификатов, досрочно прекративших действие (далее могут использоваться термины Списки отозванных сертификатов, СОС, CRL).

Примечание: в случае подключения КриптоПро OSCP Server с учетом требований «ЖТЯИ.00094-03 30 01 Службы УЦ 2.0. Формуляр», к информационно-телекоммуникационным сетям, доступ к которым не ограничен определенным кругом лиц (в том числе к сети «Интернет»), источником информации о статусах сертификатов могут являться только Списки отзыва сертификатов.

В каждом конкретном случае выбирается схема взаимодействия компонентов, исходя из нужд обеспечения доступности услуг УЦ и OSCP Server для пользователей, в том числе и для отказоустойчивости.

1.1. Работа по базе данных Реестра сертификатов КриптоПро УЦ

Данный режим обеспечивает наибольшую актуальность информации в OSCP-ответах, поскольку работа идёт непосредственно с базой данных, хранящей информацию о статусах сертификатов.

Для работы по БД Реестра сертификатов КриптоПро УЦ необходимо выполнить настройку OSCP Server и УЦ в соответствии с «ЖТЯИ.00094-03 91 01 Службы УЦ 2.0. КриптоПро OSCP Server. Руководство администратора». При этом защита Реестра сертификатов УЦ на сетевом уровне должна обеспечиваться настройкой межсетевого экрана. Настраивается фильтрация соединений от OSCP Server к Реестру сертификатов УЦ, разрешающая только сетевое взаимодействие, необходимое для доступа по протоколу HTTPS.

При размещении аппаратного обеспечения УЦ и OSCP Server на одной площадке схема соединений компонентов соответствует типовой (см. Рисунок 1).

При размещении аппаратного обеспечения УЦ и OSCP Server на разных площадках доступ OSCP Server к УЦ должен осуществляться посредством VPN.

Для обеспечения отказоустойчивости возможна установка нескольких OSCP Server.

За более подробной информацией обращайтесь к «ЖТЯИ.00094-03 91 01 Службы УЦ 2.0. КриптоПро OSCP Server. Руководство администратора».

1.2. Работа с использованием списков отозванных сертификатов

Для работы по СОС необходимо настроить их автоматическую публикацию на OSCP Server. Публикация может осуществляться как с сервера Реестра сертификатов, так и с ЦР. Настройка может быть выполнена следующим образом:

1. На сервере Реестра сертификатов или ЦР настраивается публикация СОС в папку.
2. На веб-сервере настраивается публикация папки с СОС.
3. На сервере OSCP Server настраивается задача переноса опубликованных СОС в папку-приемник.

За более подробной информацией обращайтесь к «ЖТЯИ.00094-03 91 01 Службы УЦ 2.0. КриптоПро OSCP Server. Руководство администратора».

2. Указание адресов OSCP для обеспечения отказоустойчивости

В данном разделе предлагается способ организации доступа к OSCP-серверам в территориально распределенной системе с большим числом пользователей, обеспечивающий отказоустойчивое обслуживание. Данный способ может применяться в этих же целях в любых других информационных системах, с небольшими модификациями, учитывающими особенности этих систем.

Поскольку клиенты определяют местоположение OSCP-серверов по точке AIA в сертификате, предлагается включать в сертификаты две точки AIA в следующем порядке:

1. Локальный адрес.
2. Глобальный адрес.

Под локальными и глобальными адресами здесь подразумевается использование DNS-имен, которые будут разрешаться в IP-адреса следующим образом. В локальном адресе будет содержаться имя сервера, подобное **local.ocsp.myis.ru**, а в глобальном – **global.ocsp.myis.ru**. При этом DNS-серверы распределенной системы настраиваются таким образом, что имя **global.ocsp.myis.ru** имеет одинаковые IP-адреса для всех пользователей и ссылается на центральный OSCP-сервер – максимально надежный, а имя **local.ocsp.myis.ru** имеет разные IP-адреса для разных пользователей, тем самым обеспечивая обращение пользователя к ближайшему OSCP-серверу. Для ещё большего повышения отказоустойчивости можно развернуть на каждой площадке несколько OSCP-серверов, работающих в режиме балансировки нагрузки между ними.

Подобную настройку DNS можно осуществить, например, одним из следующих способов:

- Создать зону ocsp.myis.ru на всех DNS-серверах системы как первичную и настроить два указанных имени на каждом сервере. local.ocsp.myis.ru – на ближайший(е) сервер(ы), global.ocsp.myis.ru – на центральный(е) сервер(ы). В этом случае управление адресами будет распределенным.
- Сопоставить два указанных имени с множеством всех адресов серверов распространения СОС. global.ocsp.myis.ru – один или несколько центральных серверов, local.ocsp.myis.ru – все региональные серверы. Такую настройку необходимо осуществить на первичном DNS-сервере системы, с которого адреса будут автоматически получены всеми вторичными серверами. При запросе адреса сервера local.ocsp.myis.ru служба DNS в ответе упорядочит все известные ей адреса по принципу близости к подсети клиента, таким образом, первый адрес будет указывать на ближайший сервер. Возможность такого автоматического упорядочивания на основе адреса подсети клиента присутствует в наиболее распространенных продуктах – службе DNS в ОС Microsoft и BIND в ОС UNIX. В этом случае управление адресами будет централизованным.

Указанный порядок точек AIA в сертификате обеспечивает следующую логику работы приложений. Первая попытка получения СОС происходит на территориально ближайший сервер. Если по каким-либо причинам попытка неудачна, то второе обращение происходит к центральному серверу.

Подробнее о балансировке нагрузки и обеспечении отказоустойчивости доступа пользователей к информации о статусах сертификатов см. в [2].

3. Сравнение методов предоставления информации о статусах сертификатов

В таблице (см. Таблица 1) представлены сравнительные характеристики различных методов предоставления информации о статусах сертификатов пользователям. Сравнение проводится по следующим параметрам:

- необходимость установки дополнительного ПО или изменения существующего,
- актуальность информации о статусах сертификатов,
- отказоустойчивость.

Таблица 1. Сравнение методов предоставления информации о статусах сертификатов

№ п/п	Метод предоставления информации	Установка дополнительного ПО	Модификация существующего ПО	Актуальность	Отказоустойчивость	
					Одна точка CDP или AIA	Две точки CDP или AIA
1	COC	Не требуется	Не требуется	Максимальная поддержка равна периоду публикации COC	Не обеспечивает	Обеспечивает, кроме отказов УЦ
2	COC + CRLUpdate	Установка CRLUpdate	Встраивание вызова CRLUpdate	Лучше п. 1 при внеочередных публикациях COC	Не обеспечивает	Обеспечивает, кроме отказов УЦ
3	OCSP-сервер, работающий по COC	Установка КриптоПро Revocation Provider	Не требуется	Соответствует п. 2	Обеспечивает, кроме отказов самого OCSP-сервера	Обеспечивает
4	OCSP-сервер, работающий по БД Реестра сертификатов КриптоПро УЦ	Установка КриптоПро Revocation Provider	Не требуется	Наибольшая актуальность информации	Обеспечивает, кроме отказов самого OCSP-сервера	Обеспечивает

4. Перечень сокращений

AIA	Точка доступа к информации о Центре (Authority Information Access)
CDP	Точка доступа к СОС (CRL Distribution Point)
DNS	Доменная система имён (Domain Name System)
HTTP	Протокол передачи гипертекста (Hypertext Transfer Protocol)
HTTPS	Безопасный протокол передачи гипертекста (Secure HTTPS)
IP	Протокол Интернет (Internet Protocol)
OCSP	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
RPC	Удалённый вызов процедур (Remote Procedure Call)
VPN	Виртуальная частная сеть (Virtual Private Network)
APM	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПК	Программный комплекс
СОС	Список отзыва сертификатов (CRL – Certificate Revocation List)
УЦ	Удостоверяющий Центр
ЦР	Центр Регистрации
ЦС	Центр Сертификации

5. Перечень ссылочных документов

1. ЖТЯИ.00094-03 91 01. Службы УЦ 2.0. КриптоПро OSCP Server. Руководство администратора.
2. Смирнов П. Балансировка нагрузки и отказоустойчивость при проверке статусов сертификатов в ИОК // PCWEEK Russian Edition, №44(458), 2004. — с. 24-26.
URL: <https://www.itweek.ru/infrastructure/article/detail.php?ID=69051>.