Структура и компоненты Инфраструктуры Открытых Ключей, модели доверия

Котенко А.В., Нурдавлетова Д.Р.

В данной работе проанализирована структура удостоверяющих центров (УЦ) и описаны компоненты, из которых состоят УЦ, а также приведено сравнение структур зарубежных и Российских Удостоверяющих Центров и описаны существующие модели доверия.

Сложилось так, что ИОК создавалась на базе зарубежных стандартов криптографии. Широкое развитие за рубежом данная технология получила за счет поддержки ее со стороны таких крупных американских производителей программного обеспечения, как Microsoft, HewlettPackard, Intel и др.

Идея защиты информации на основе инфраструктуры открытых ключей, использующей отечественные криптографические стандарты, относительно нова. [1] Однако за последнее время, с выходом нового федерального закона "Об ЭП" и множества дополнительных рекомендательных указов ФСБ РФ криптография с открытым ключом получила широкое распространение. Для более подробного разбора элементов PKI и структуры УЦ обратимся к уже существующим аккредитованным удостоверяющим центрам Российской Федерации и рассмотрим, из каких элементов они состоят, а также далее будут рассмотрены наиболее известные зарубежные удостоверяющие центры.

Составляющие элементы удостоверяющих центров показаны в таблице 1.

Таблица 1 - Составляющие элементы УЦ в России и за рубежом

Название / Структурные элементы	VipNet	Верба УЦ «ЗАО МО ПНИЭИ»	Крипто про	Сигнал ком	KEON	Start Com	En Trust
Центр регистрации (ЦР)	+	+	+	+	+	+	+
Центр сертификации (ЦС)	+	+	+	+	+	+	+
Общедоступный список отозванных сертификатов	+	+	+	+	+	+	+
Справочник сертификатов	+	+	+	+	+	+	+
Web-интерфейс Удостоверяющего центра	-	-	+	+	-	-	+
АРМ Оператора (Администратора) ЦР	+	+	+	+	-	+	+
АРМ разбора конфликтных ситуаций	-	+	+	+	-	-	-
АРМ пользователя	+	-	+	+	-	+	+

Далее рассмотрены и описаны компоненты инфраструктуры открытых ключей.

1 Центр сертификации (ЦС)

Центр сертификации представляет собой основную управляющую компоненту ИОК, предназначенную для формирования электронных сертификатов для подчиненного Центра Регистрации (или нескольких подчиненных центров) или конечных пользователей.

Кроме сертификатов, ЦС формирует список отозванных сертификатов (СОС, X.509 - CRL (Certificate Revocation List)), с регулярностью, определенной Регламентом УЦ.[1]

Модуль центра сертификации включает в себя следующие компоненты:

– серверная часть;

– АРМ администратора УЦ;

– глобальное хранилище сертификатов (репозиторий).

Основной функцией серверной части центра сертификации является прием и проверка подлинности запросов на электронный сертификат от клиентов системы. Так же производится прием и проверка подлинности запросов на отзыв электронного сертификата от клиентов системы.

Одной из самых главных функций и обязанностей АРМ администратора являются генерация закрытого ключа центра сертификации и формирование соответствующего сертификата центра сертификации, содержащего его открытый ключ. Важно, чтобы сертификат был актуальным, потому что он играет главную роль в верификации выданных сертификатов. В обязанности администратора центра сертификации входит обеспечение регистрации новых клиентов системы и добавление их в общую базу. Так же с помощью АРМ производится формирование электронных сертификатов открытых ключей клиентов системы на основе принятых запросов на сертификат от клиентов. По запросу клиента может быть произведен отзыв сертификата до окончания срока его действия. Причиной этого чаще всего является компрометация закрытого ключа. Кроме того, по истечению срока действия сертификата производится его замена.

Старые сертификаты заносятся в СОС. Периодически формирующиеся списки отозванных и действующих сертификатов доступны для всех пользователей системы. Глобальное хранилище сертификатов должно быть защищено от несанкционированного доступа, а также предоставлять нескольким клиентам возможность одновременного доступа к хранилищу. Немаловажным является обеспечение целостности хранимых данных в репозитории.[2]

2 Центр Регистрации (ЦР)

Центр Регистрации – серверный компонент, который осуществляет ведение баз данных учетных записей пользователей, изготовленных сертификатов ключей подписей, запросов на сертификаты и т.д. [6] Основная задача ЦР - регистрация пользователей и обеспечение их взаимодействия с ЦС. В задачи Центра Регистрации может также входить публикация сертификатов и СОС. ЦР является единственной точкой входа и регистрации пользователей. Только зарегистрированный пользователь может получить сертификат на свой открытый ключ в Центре Сертификации. [1]

Центров Регистрации для одного Центра Сертификации может быть несколько. [6]

3 Сетевой справочник

Справочник сертификатов – субъект инфраструктуры PKI, обеспечивающий хранение сертификатов открытых ключей и Списков Отозванных Сертификатов (СОС), формируемых в УЦ. Выданные сертификаты публикуются в специализированный сетевой справочник, доступ к которому имеют все пользователи.

Информация, публикуемая в справочнике, пополняется из реестра УЦ. Внесение изменений в сетевой справочник с целью публикации новых сертификатов и СОС выполняется в УЦ автоматически, при их формировании. Списки Отозванных Сертификатов доступны чаще всего через Web-интерфейс либо через приложение. [7]

4 Web-интерфейс УЦ

Web-интерфейс УЦ обеспечивает защищенное взаимодействие удаленных пользователей с Удостоверяющим Центром в процессе генерации ключей и передачи в УЦ запросов на создание сертификата, с последующей доставкой изготовленных сертификатов на рабочие места пользователей. Взаимодействие обеспечивается через личные кабинеты пользователей, зарегистрированных на портале УЦ, с использованием протокола http. [7]

5 АРМ администратора Центра Регистрации

Автоматизированное рабочее место (АРМ) администратора Центра Регистрации – компонент, который предназначен для выполнения операций, связанных с регистрацией пользователей, формированием закрытых ключей и запросов на сертификаты открытых ключей, обработкой запросов на сертификаты открытых ключей, получением изданных Центром Сертификации сертификатов, управлением (аннулированием, приостановлением и возобновлением действия) сертификатов и выполнением иных действий по выполнению целевых функций Удостоверяющего Центра.

АРМов администраторов для одного Центра Регистрации может быть несколько. [6]

6 АРМ пользователя (модуль клиента)

Модуль клиента системы управления сертификатами должен состоять из следующих компонентов:

– ПО работы с ключевой информацией;

– ключевой информации (контейнера) пользователя;

– локального хранилища сертификатов.

АРМ пользователя имеет возможность создания новых ключей пользователя, и формирования запросов в центр сертификации для регистрации и получения сертификата для нового открытого ключа. В случае необходимости может быть подан запрос на отзыв того или иного сертификата. АРМ может самостоятельно обращаться в реестр сертификатов для проверки подлинности того или иного сертификата, и получения по нему необходимой информации. [2]

7 АРМ разбора конфликтных ситуаций

АРМ разбора конфликтных ситуаций – компонент, обеспечивающий выполнение процедур по подтверждению подлинности электронной подписи в электронных документах и установлению статуса сертификата открытого ключа на определенный момент времени.

Итогом работы АРМ разбора конфликтных ситуаций является протокол, содержащий результаты выполненных проверок. [6]

8 Криптопровайдер

Криптопровайдер (система криптографической защиты) должна обеспечивать:

– конфиденциальность;

– целостность;

– контроль доступа;

– аутентификацию пользователей;

– неотказуемость.[1]

Начальным элементом цепочки является сертификат центра сертификации, хранящийся в защищенном персональном справочнике пользователя.

Процедура верификации цепочки сертификатов проверяет наличие связи между именем Владельца сертификата и его открытым ключом, она подразумевает, что все "правильные" цепочки начинаются с сертификатов, изданных одним доверенным центром сертификации. Под доверенным центром понимается главный УЦ, открытый ключ которого содержится в самоподписанном сертификате.

Алгоритм верификации цепочек использует следующие данные:

– X.500 имя Издателя сертификата;

– X.500 имя Владельца сертификата;

– открытый ключ Издателя;

– срок действия открытого (секретного) ключа Издателя и Владельца;

– дополнения, используемые при верификации цепочек;

– СОС для каждого Издателя (даже если он не содержит отзываемых сертификатов).

Модели доверия

Одним из наиболее важных вопросов, относящихся к инфраструктуре открытых ключей, является вопрос о том, каким открытым ключам можно доверять. Чтобы ответить на него, следует сначала рассмотреть модели доверия, применяемые в удостоверяющих центрах, но прежде всего – то такое доверие вообще. [8]

Уровень доверия определяется мерой определенности во взаимоотношениях доверяющих сторон, но понятие доверия в значительной мере является интуитивным. В этом и кроется одна из причин того, почему до сих пор не существует единого формального определения понятия доверия. [4]

В стандарте X.509 данный термин трактуется следующим образом: «В целом, можно говорить, что один объект является «доверенным» по отношению к другому объекту, если первый объект может предположить, что второй объект будет вести себя исключительно в рамках предположения первого объекта».

Домен доверия можно определить как совокупность четко сформулированных политик и правил в пределах организации, позволяющих реализовать доверительные отношения. [5]

Формирование доменов может производиться по различным принципам:

– географическое деление (каждый региональный филиал большой компании, имеет свой собственный домен доверия);

– организационному принципу (в рамках одной организации существуют категории персонала с разным уровнем допуска к информации);

– структура бизнес-процессов (в качестве доменов могут быть выделены домен клиентов компании, партнеров, сотрудников и т.д.).

Кроме того, домены доверия могут частично перекрываться или быть включенными друг в друга. [4] Использование сертификатов, выпущенных в удостоверяющем центре, принадлежащего другому домену доверия гораздо сложнее, чем использование сертификатов УЦ, находящегося в вашем домене доверия. [5]

В рамках одной организации может существовать несколько различных доменов доверия. Для всех пользователей PKI в домене доверия удостоверяющий центр рассматривается как центр доверия, которому пользователь PKI может доверять при любых обстоятельствах. [8] Отсюда и появляется понятие якоря доверия.

Для ИОК характерно то, что якорь доверия является исходной точкой для построения всех отношений доверия и от его правильного определения, в конечном счете, зависит безопасность всей системы.

Модель доверия определяет механизм распространения доверия среди компонент системы путем установления отношений доверия между каждой парой компонент. [4] В процессе проверки подлинности сертификата программное обеспечение PKI пытается выстроить путь доверия до уровня УЦ, который является якорем доверия. [3] Таким образом, появляется понятие цепочки доверия, или цепочки сертификатов.

Все вышесказанные понятия, объекты, правила объединяются в одну систему – модель доверия.

Отношения доверия в PKI устанавливаются между двумя ЦС, когда один или оба из них выпускают сертификат открытого ключа другого ЦС. Отношения доверия могут быть односторонние или двусторонние. Примером односторонних доверительных отношений может служить переход из домена доверия с более высоким уровнем безопасности в домен с более низким уровнем. Например, отношения федерального УЦ и УЦ в регионах, когда федеральный центр стоит выше по иерархии региональных, и его сертификат является более доверительным. Двусторонние доверительные отношения имеют место при связывании

доменов с эквивалентным уровнем безопасности. К примеру, несколько УЦ, находящихся в одном регионе, и оба стоящие ниже федерального УЦ.

Одной из наиболее распространенных моделей доверия является иерархическая модель. В данной модели единственным якорем доверия является корневой ЦС. Модель строится путем установления отношений подчинения между корневым УЦ и теми УЦ, что располагаются ниже его по иерархии. Подчиненные УЦ, в свою очередь, устанавливают подобные отношения с подчиненными УЦ следующего уровня и т. д., вплоть до конечных Удостоверяющих Центров. Иерархическая структура имеет вид дерева, в которой ЦС, являющийся якорем доверия, играет роль корня. Данная модель применяется, когда необходимо снизить нагрузку на корневой Удостоверяющий Центр при управлении большим объемом сертификатов. Корневой УЦ передает часть своих полномочий по управлению группами пользователей/сертификатов подчиненным УЦ путем выпуска сертификатов, в которых указывается объем передаваемых полномочий. Еще одна причина использования этой модели – желание обезопасить ключ корневого ЦС путем сокращения частоты его использования. Опасения являются обоснованными, поскольку в данной модели компрометация ключа корневого УЦ приводит к разрушению всей архитектуры доверия. Построение пути сертификации в иерархической модели производится “снизу вверх”, от листьев к корню.

Сетевая модель (децентрализованная, распределенная модель) реализует альтернативный подход к формированию отношений доверия. Модель строится путем установления доверительных отношений между равноправными УЦ. При этом отношения могут быть односторонними или двусторонними. Якорем доверия в данном случае является локальный УЦ. Таких якорей доверия может быть много, в зависимости от числа участвующих УЦ. Особенностью данной модели является тот факт, что отношения доверия строятся, как правило, посредством перехода через границы доменов доверия. Поэтому, сертификаты, выпущенные для этих целей, называются кросс-сертификатами и имеют специальный вид. В составе кросс-сертификата, по сравнению с обычным сертификатом, присутствует информация преобразования политик безопасности. Удобство сетевой модели сертификации заключается в том, что в результате кросс-сертификации на уровне корневых УЦ, исчезает необходимость распространения корневого самоподписанного сертификата одной организации среди пользователей другой.

Иногда выделяют “гибридную”, или мостовую модель доверия, как смешение иерархической и сетевой моделей. Однако, по своей сути, эта модель является видом сетевой модели (так как основная ее структура основана все же на кросс-сертификации), с последующим расслоением дочерних УЦ по иерархиям. Не смотря на то, что все УЦ могут быть в тех или иных доменах доверия, или полностью доверять друг другу, всегда на уровне регламентов УЦ вводятся те или иные ограничения на сертификаты. Основные ограничения, накладываемые на сертификат – это ограничение на имя сертификата, на количество звеньев в цепочки доверия, ограничение на использование в различных доменах доверия и т.п.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

[1] – Инфраструктура Открытых Ключей// Валидата, информационная безопасность, – М., 2013, – Режим доступа: http://www.x509.ru/pki.shtml, свободный. – Загл. с экрана.

[2] – С. А. Петренко, Практика построения PUBLIC KEY INFRASTRUCTURE, PKI // «Защита информации. Конфидент», №6, – М., 2002.

[3] – Жан де Клерк, Принципы доверия PKI // «Windows IT Pro», № 07 – М., 2006, – Режим доступа: http://www.osp.ru/win2000/2006/07/3546159/, свободный. – Загл. с экрана.

[4] – Модели доверия PKI // Учебный центр безопасности информационных технологий Microsoft Московского инженерно-физического института – М., 2006.

[5] – PKI: Implementing & Managing E-Security // A. Nash, B. Duane, D. Brink, C. Joseph. – McGraw-Hill Osborne Media, 2001, ISBN-10: 00721312336 ISBN-13: 978-0072131239.