Практические приложения PKI: атрибутные сертификаты

Денис Копылов, *технический директор ООО "Топ Кросс"*

Общая картина

На сегодняшний день инфраструктура открытых ключей (PKI) является, по сути, основной платформой для развертывания различных высокотехнологичных сервисов и услуг, в том числе относящихся к "электронному государству". За последние десять лет данная технология прошла путь "с нуля" до законодательно обоснованного инструмента, позволяющего строить защищенные информационные системы в масштабах страны. Но инструмент этот далеко не прост, и одной из серьезных задач, с которыми обязательно столкнутся разработчики и внедряющие такие системы, будет стандартизация средств и способов размещения ролевой дополнительной информации о субъектах информационного обмена в системах, основанных на PKI.

Носителями "основной" информации – данных, позволяющих идентифицировать субъекта, – могут выступать решения типа социальной карты, создание и внедрение которых уже ведется (и в дальнейшем будет только добавлять значимости упомянутой выше задаче). Причин для такой зависимости несколько. Чтобы рассмотреть их подробнее, попробуем для начала прорисовать общую картину.

Имеется инфраструктура, основанная на PKI, основная услуга которой – выдача пользователям персональных цифровых носителей, содержащих данные, идентифицирующие пользователя.

Имеется также неопределенный и потенциально неограниченный круг информационных систем (таких, как банки, операторы сотовой связи, государственные учреждения), по разным причинам заинтересованных в обслуживании пользователей. У каждой из таких информационных систем существуют свои требования и ограничения, касающиеся объема дополнительной информации, необходимой для обслуживания пользователей.

Традиционно такая информация собирается обслуживающими системами параллельно и независимо друг от друга. Данный подход имеет ряд существенных недостатков с точки зрения каждого из участников информационного обмена:

- дублируется деятельность по идентификации пользователя;
- во многом дублируется деятельность по сбору дополнительной информации;
- со временем возникает проблема поддержания актуальности и непротиворечивости данных, продублированных во многих информационных системах.

Итог для обслуживающих организаций: масса накладных расходов, которых можно избежать, грамотно используя современные технологии.

Итог для пользователя: качество обслуживания, далекое от идеального.

Само собой напрашивается решение включить информацию, необходимую прикладной системе, в состав сертификата пользователя. И это решение, как самое очевидное, уже нашло свое применение во многих корпоративных системах. Однако такой подход не является идеальным даже в рамках корпорации, а в постановке для публичных систем и вовсе неприменим:

- в момент издания сертификата пользователя практически невозможно удовлетворить требования к информационному наполнению со стороны неограниченного круга информационных систем, в которые он может обратиться;
- действующий ФЗ "О персональных данных" ограничивает порядок обработки данных, которые необходимы многим прикладным системам, что делает невозможным размещение в публичном реестре сертификатов, содержащих, например, номер паспорта, в то время как по действующему ФЗ "Об ЭЦП" такая публикация необходима.

Существует, конечно, возможность размещения дополнительной информации на цифровом носителе пользователя отдельно от сертификата. Однако, открывая персональный носитель пользователя на запись для произвольной, возможно злонамеренной, прикладной системы, мы получим еще больше проблем и вопросов. Да и "складывать все яйца в одну корзину" в любом случае неправильно: одно дело – потерять пропуск или даже паспорт, и совсем другое – потерять все документы сразу.

Услуги Доверенной третьей стороны

Однако ситуация вовсе не является тупиковой. Достаточно вспомнить о том, что технология PKI является продуктом международного сотрудничества и давно и активно используется за рубежом.

Рекомендации X.842 Международного союза электросвязи (МСЭ, ITU – International Telecom-

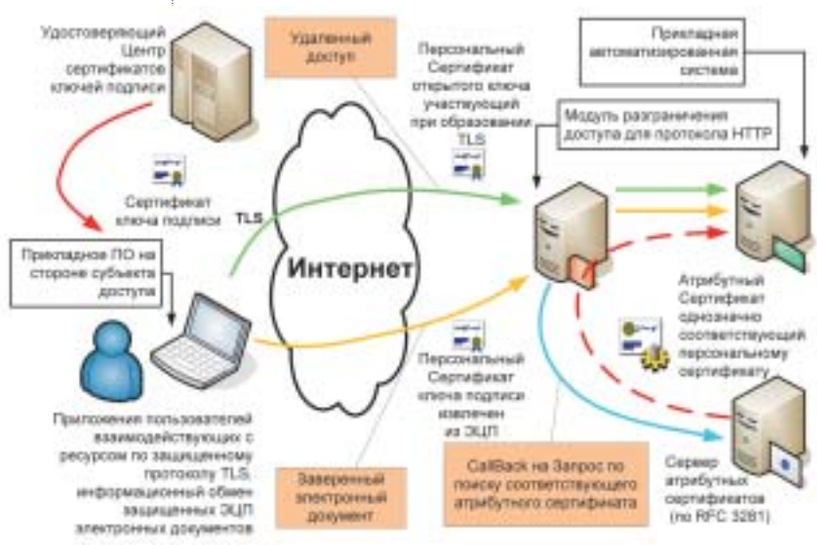

Рисунок. Структура PKI-системы с использованием сервиса атрибутирования (CA)