ЭТАПЫ ФОРМИРОВАНИЯ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ОПТИМАЛЬНОЕ РЕШЕНИЕ ЕГО ФУНКЦИЙ

В.М. Белов, Д.С. Яковлев, В.А. Кемпф

После выхода федерального закона «Об Электронной цифровой подписи» [1] прошло три года. За этот небольшой срок в нашей стране возникло около 150 удостоверяющих центров электронной цифровой подписи (УЦ ЭЦП). Несмотря на то, что в законе прописаны функции, которые должен выполнять УЦ ЭЦП, они могут быть осуществлены несколькими методами. В этой статье мы хотели бы выделить основные этапы при формировании УЦ ЭЦП, а также попытаться найти оптимальное решение для выполнения его функций.

Для определения этапов формирования нам необходимо рассмотреть следующие аспекты работы УЦ ЭЦП:

− взаимодействие с уполномоченным федеральным органом исполнительной власти;

− взаимодействие с владельцем сертификата ключа подписи;

− это взаимодействия между УЦ.

Первый шаг в работе УЦ − это взаимодействие с уполномоченным федеральным органом исполнительной власти. В соответствии с Постановлением Правительства РФ от 30.06.2004 № 319 на Федеральное агентство по информационным технологиям (Росинформтехнологии) возложено выполнение обязанностей уполномоченного федерального органа (УФО) исполнительной власти в области электронной цифровой подписи (ЭЦП).

1) УЦ до начала использования электронной цифровой подписи уполномоченного лица УЦ для заверения от имени УЦ сертификатов ключей подписей обязан представить в уполномоченный федеральный орган исполнительной власти сертификат ключа подписи уполномоченного лица УЦ в форме электронного документа, а также этот сертификат в форме документа на бумажном носителе с собственноручной подписью указанного уполномоченного лица, заверенный подписью руководителя и печатью УЦ.

2) Уполномоченный федеральный орган исполнительной власти ведет единый государственный реестр сертификатов ключей подписей, которыми удостоверяющие центры, работающие с участниками информационных систем общего пользования, заверяют выдаваемые ими сертификаты ключей подписей, обеспечивает возможность свободного доступа к этому реестру и выдает сертификаты ключей подписей соответствующих уполномоченных лиц УЦ.

3) ЭЦП уполномоченных лиц УЦ могут использоваться только после включения их в единый государственный реестр сертификатов ключей подписей. Использование этих ЭЦП для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

4) Уполномоченный федеральный орган исполнительной власти: - осуществляет по обращениям физических лиц, организаций, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления подтверждение подлинности электронных цифровых подписей уполномоченных лиц УЦ в выданных ими сертификатах ключей подписей; - осуществляет в соответствии с положением об уполномоченном федеральном органе исполнительной власти иные полномочия по обеспечению действия настоящего Федерального закона.

Таким образом, до начала работы УЦ необходимо получить заверение от федерального органа исполнительной власти. А уполномоченный удостоверяющий центр должен включить ЭЦП уполномоченных лиц удостоверяющих центров в свой реестр и только тогда УЦ сертификаты ключей УЦ будут иметь юридическую силу.

В июне 2005 г. был создан корневой удостоверяющий центр, который и будет выполнять функции уполномоченного удостоверяющего центра. Приведем его краткие характеристики. Корневой удостоверяющий центр содержит такие обязательные компоненты, как центры сертификации и регистрации, реестр сертификатов. Структура комплексной системы информационной безопасности включает в себя следующие элементы:

− системы защиты информации от несанкционированного доступа и управления доступом к критическим элементам комплекса;

− систему криптографической защиты, а также электронную цифровую подпись, вырабатываемую с использованием сертифицированных средств;

− систему обнаружения, предупреждения и защиты от компьютерных вторжений;

− систему антивирусной защиты.

Корневой удостоверяющий центр обеспечивает изготовление до 1000 сертификатов ключей подписи в сутки, ведение реестра на 300 тысяч сертификатов и ведение архива на 2 миллиона сертификатов.

Полученные к настоящему времени результаты в области применения закона «Об ЭЦП» являются первым шагом в направлении создания системы удостоверяющих центров.

Домрачев А.А. (заместителя начальника Управления государственных услуг Росинформтехнологии) считает, что необходимым условием создания единой системы УЦ является применение одних и тех же криптографических стандартов электронной цифровой подписи. Известно, что во многих странах возникает проблема несовместимости программных продуктов различных производителей. Но данную проблему можно решить и другим способом, предложенным добровольным объединением УЦ. Решение заключается в создании мостового УЦ, который обеспечивает взаимодействие региональных УЦ с помощью механизма кросс-сертификации. Проблемы несовместимости алгоритмов шифрования решает именно мостовой УЦ.

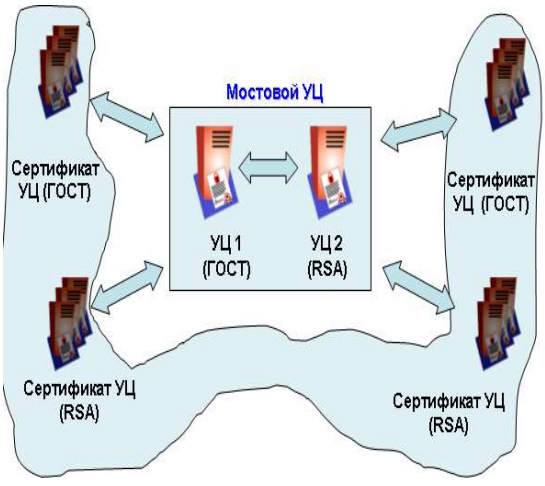

Рисунок 1 − Использование МУЦ для связи областей доверия с различными базовыми криптографическими алгоритмами

Это конечно более трудоемкий процесс, но тут решается проблема взаимодействия международных сертификатов подписи.

Следующий шаг при формировании УЦ это взаимодействие с владельцем сертификата ключа подписи.

Удостоверяющий центр при изготовлении сертификата ключа подписи принимает на себя следующие обязательства по отношению к владельцу сертификата ключа подписи:

− вносит сертификат ключа подписи в реестр сертификатов ключей подписей;

− обеспечивает выдачу сертификата ключа подписи обратившимся к нему участникам корпоративной системы;

− приостанавливает действие сертификата ключа подписи по обращению его владельца;

− уведомляет владельца сертификата ключа подписи о фактах, которые стали известны Удостоверяющему центру и которые существенным образом могут сказаться на возможности дальнейшего использования сертификата ключа подписи;

− выполняет разбор конфликтных ситуаций, связанных с применением электронной цифровой подписи участников системы корпоративного документооборота с выдачей экспертного заключения.

Таким образом, УЦ не просто выдает сертификаты ключей подписи, но и является органом регулирующим электронный документооборот в своем регионе.

На этом этапе идет определение внутренних функций УЦ таких как:

1) Регистрация пользователя услуг УЦ (сотрудники УЦ вносят в реестр данные по пользователю услуг УЦ и принимают решение о выдачи сертификата ключа подписи).

2) Изготовление и получение сертификата ключа подписи (УЦ выдает сертификат пользователю УЦ по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи).

3) Приостановление и возобновление действия сертификатов ключей подписей, а также их аннулирование.

4) Подтверждение подлинности ЭЦП в электронных документах.

На этом этапе формируется политика работы с пользователями и выданными им сертификатами. От того, как построить эти взаимоотношения и зависит оптимальность работы УЦ.

И последний шаг − это взаимодействия между УЦ.

В настоящее время в России формируются два типа таких отношений:

1) При помощи корневого УЦ. В этом случае заданы одинаковые стандарты и спецификации для подчиненных удостоверяющих центров. При этом корневой удостоверяющий центр целесообразно использовать в качестве головного для удостоверяющих центров федеральных и региональных органов государственной власти. Недостатком данного метода является подчиненность заданным стандартам.

2) При помощи добровольного объединения УЦ. В данном случае осуществляется техническая, экономическая помощь и поддержка региональным УЦ, вступившим в объединение.

Лучшим вариантом было бы вступить в обе эти системы. Под деятельностью УЦ понимаются функции связанные непосредственно с сертификатом ключа подписи.

В Федеральном законе «Об ЭЦП» определены следующие функции УЦ:

− изготовление сертификатов ключей подписей;

− создание ключей ЭЦП по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа электронной цифровой подписи;

− блокирование и возобновление действия сертификатов ключей подписей, а также аннулирование их;

− ведение реестра сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;

− проверка уникальности открытых ключей ЭЦП в реестре сертификатов ключей подписей и архиве удостоверяющего центра;

− выдача сертификатов ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;

− осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей;

− может предоставлять участникам информационных систем иные связанные с использованием электронных цифровых подписей услуги.

Исходя из этих функций, можно выделить следующие этапы работы УЦ:

1) Регистрация.
2) Выдача сертификата.
3) Обслуживание сертификата.
4) Аутентификация пользователя.

При регистрации УЦ необходимо собрать достоверную информацию о пользователе и принять решение о выдачи сертификата ключа. При принятии положительного решения, сотрудник УЦ выполняет регистрационные действия по занесению регистрационной информации в реестр УЦ.

Выдача сертификата ключа подписи производится в бумажном и (или) электронном виде на основании заявления на изготовление сертификата ключа подписи при личном прибытии пользователя УЦ в офис УЦ.

Обслуживание сертификата состоит из приостановления возобновления действия сертификата ключа подписи, а также аннулирования их. Эти операции производятся либо по заявлению пользователя УЦ, либо по инициативе УЦ в связи с нарушениями пользователем своих обязательств.

И последнее − это осуществление по обращению пользователя УЦ подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Что касается стандартов ЭЦП, то здесь наблюдается практически полное соответствие: стандарты ЭЦП России и США [2] базируются на родственных модификациях схемы ЭЦП Эль-Гамаля и отличаются рядом несущественных деталей. Совсем недавно эти стандарты были обновлены — переведены на «эллиптические кривые». Подобная поспешность может свидетельствовать в пользу того, что государственные структуры продвинулись в изучении проблемы дискретного логарифмирования в конечных полях несколько дальше, чем сообщество, ведущее открытые исследования в криптографии. Кроме того, практическая синхронность принятия и обновления стандартов ЭЦП в России и США может говорить в пользу того, что оба государства находятся на примерно одном и том же уровне в научных исследованиях в области криптографии.

В данном случае мы предложили использовать отечественный стандарт ГОСТ Р 34.10-2001. Таким образом, получается, что УЦ являет собой сервер безопасности.

На серверной стороне происходит формирование и регулирование сертификатов ключей подписей. Кроме того, по заявлению пользователя осуществляют проверку подлинности сертификата.

Клиентская же часть состоит из механизма создания подписи электронному документу и проверки подлинности ЭЦП у входящих электронных документов [3].

Проблема оптимизации функций свелась к проблеме построения оптимальной архитектуры взаимодействия сервера с клиентом и к вопросу программной оптимизации архитектуры УЦ ЭЦП.

ЛИТЕРАТУРА

1. Федеральный закон «Об электронной цифровой подписи».

2. Винокуров А.Ю. Стандарты аутентификации и ЭЦП России и США // Отраслевой каталог «Технологии и средства связи-2003».

3. Byte Magazine Online - Цифровая подпись - как это делается // http://www.bytemag.ru.