

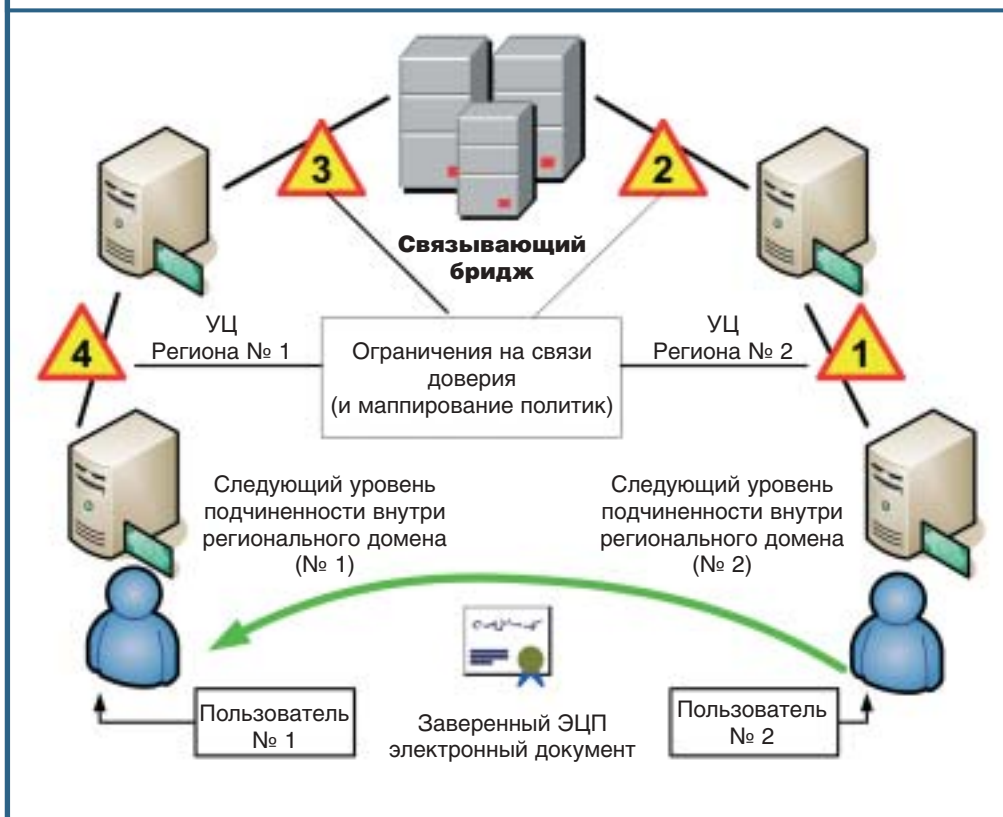
лее продолжителен, и существуют механизмы пролонгации квитанций (выпуск квитанции на квитанцию).

- Организация проверки ЭЦП "третьей" стороной для пользователей позволяет перевести сам факт проверки из плоскости криптографических вычислений сертифицированными СКЗИ в плоскость организации доверенной доставки квитанций с сервера ЭН, что во многих случаях значительно технологичнее. Степень "доверенности" доставки квитанций не регламентируется ФЗ "Об ЭЦП" и целиком определяется спецификой автоматизированной системы, в которой используются заверенные документы. Способов доставки квитанций достаточно много: курьерская служба, подтверждение по телефону, сравнение самих файлов-квитанций, полученных по сети и из репозитория ЭН (DVCS).

- Возложение на сервис ЭН функции проверки действительности некоего цифрового сертификата существенно упрощает автоматизированную систему, в которой находятся заверенные ЭД. Сама по себе процедура проверки сертификата весьма трудоемка, необходимо построить цепочку проверки конечного сертификата с проверкой всех промежуточных сертификатов издателей, определить точки распространения, получить и обработать списки отозванных сертификатов, возможно, включая обновления к ним и т.п.

- Данный сервис может быть весьма полезен для информационных систем, в которых используется факт обладания пользователем некой информацией без ее опубликования. Например, ИС проведения различных тендеров, регламент которых запрещает кому-либо до определенного срока доступ к конкурсному материалу (за исключением кратких аннотаций); только после начала конкурса "конверты" могут быть вскрыты. Для таких систем участники представляют квитанции на истинность ЭЦП конкурсного материала без фактической передачи самого материала до момента наступления конкурса. Истинность представленного впоследствии материала подтверждено ЭЦП из состава DVC-квитанции. В этом случае защита конкурсного ма-

Рис. 1. Путь сертификации и иерархии в общей защищенной зоне



териала возлагается на самих конкурсантов (самых заинтересованных в защите собственной информации лиц) и полностью снимает риск мошенничества в системе.

Особенности расположения Службы электронного нотариата в распределенной PKI-системе

Вопросы указаний в сертификатах ключей подписи на области их применения, а также ограничения, вводимые в сертификаты связи, в рамках всей PKI-системы тесно связаны со структурой системы УЦ взаимодействующих доменов.

В общем случае процесс обмена защищенными ЭЦП электронными документами проиллюстрирован на рис. 1.

Из рис. 1 видно, что цепочка сертификации должна строиться с учетом всех четырех ограничений, следовательно, в идеальном варианте Служба электронного нотариата должна располагаться в каждом конечном домене. В противном случае Служба электронного нотариата должна иметь информацию о конечной точке проверки (сертификат издате-

ля для пользователя № 1 – см. рис. 1) и/или конкретной политике использования сертификата, согласно которой будет выполняться проверка ЭЦП.

"Электронный нотариус" в электронном государстве

В последние годы много говорится о необходимости создания электронного государства. В частности, как известно, подготовлен проект "Концепции формирования институтов электронного государства", определяющей основные принципы формирования базовых институтов государственного администрирования. Данной концепцией как раз и вводится понятие "электронного нотариата", который должен подтверждать истинность открыто публикуемой государственными органами информации, а также контролировать все модификации данной информации с целью предотвращения возможности подделки.

Конечно, придется внести изменения в ряд правовых актов и, в первую очередь, в ФЗ "О нотариате", но без Службы электронного нотариуса электронного государства не построишь. ●