"Электронный нотариус" в PKI-системе

С.М. Муругов, *генеральный директор ООО "Топ Кросс"*

"Электронный нотариус" и выполняемые им задачи

Согласно ст. 9 ФЗ "Об электронной цифровой подписи" одной из функций Удостоверяющего центра (УЦ) является осуществление (по обращениям пользователей сертификатов ключей подписей) подтверждения подлинности ЭЦП в электронном документе в отношении выданных УЦ сертификатов ключей подписей. Таким образом, об этом сервисе, предоставляемом УЦ, можно говорить как об "электронном нотариусе". Естественно, что функции проверки сертификатов, а также другой информации и выдачи соответствующих квитанций, содержащих "штамп" времени, может выполнять и отдельная служба/сервис, не входящая в состав УЦ.

Надо отметить, что в первоначальной редакции указанного закона одной из функций УЦ было также проставление штампа времени на подписанные ЭЦП документы по просьбе пользователей. Однако в принятом законе этого пункта нет.

"Электронный нотариус" может являться техническим решением, стандартизированным в таких документах, как RFC 3029 "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols (DVCS)", RFC 2560 "Online Certificate Status Protocol – OCSP", RFC 3161 "Time-Stamp Protocol (TSP)".

Перечислим некоторые задачи, в которых может быть необходимо удостоверение информации:

- Создание единого домена защищенного электронного документооборота, в том числе построенного на несовместимых между собой средствах криптографической защиты информации (СКЗИ), для гетерогенных программно-аппаратных платформ. Данное свойство может быть полезно и при организации трансграничного обмена защищенными электронными документами со странами, в которых легитимным является криптографический алгоритм RSA.
- Получение штампа "истинного времени для конкретной PKI-системы" на заверенном электронном документе (ЭД). Это весьма важно для предупреждения коллизий при выработке ЭЦП: на ЭД корректно указывать дату подписания, однако простановка истинной даты целиком является ответственностью подписывающей стороны. Служба электронного нотариата в данном случае является "третьей" стороной – доверенным арбитром, который фиксирует факт наличия действительной ЭЦП на конкретный момент времени. Подобный сервис иногда называют Time Stamping (TSP). Наличие "третьей" независимой стороны может оказаться полезным, чтобы зафиксировать определенный этап (стадию) в технологической цепочке документооборота (например, на конкретный момент времени налоговая декларация заверена и доставлена от налогоплательщика в инспекцию). В более широком смысле Служба может быть использована в работе абстрактной прикладной системы как источник TSP-меток "эталонного времени[1]".
- Длительное архивное хранение электронных документов. ЭЦП на ЭД имеет "срок жизни", определяющийся, в частности, периодом действительности сертификата, закрытый ключ которого использовался в формировании ЭЦП. По многим причинам этот временной период весьма ограничен, что не позволяет строить полноценную систему документооборота, включая такой важный ее компонент, как архивное хранение. Наличие квитанций по факту проверки ЭЦП позволяет делать выводы о действительности ЭЦП даже после истечения срока действия сертификата, ключ которого был использован в выработке ЭЦП. Данное свойство объясняется тем, что срок действия сертификата ЭН (Службы электронного нотариата, DVCS), которым заверена квитанция, бо-

[1] *"Эталонное время" в PKI-системе может отличаться от астрономического времени, что определяется иным назначением – синхронизацией событий только в PKI-системе. Соответственно и требования к источнику "эталонного времени" в PKI-системе определяются прикладным назначением этой системы.*