Реализация архивного хранения электронных документов с использованием формата усовершенствованной электронной подписи

Фураков Александр Владимирович,
заместитель коммерческого директора
ООО «КРИПТО-ПРО»

Предлагаемая ООО «КРИПТО-ПРО» усовершенствованная подпись позволяет решить все основные трудности, связанные с применением ЭП, и обеспечить участников документооборота всей необходимой доказательной базой (причем собранной в самой ЭП в качестве реквизитов электронного документа), связанной с установлением момента подписи и статуса сертификата открытого ключа подписи на момент подписи.

Формат усовершенствованной подписи основан на европейском стандарте ETSI 101 733. Данный формат подписи решает описанные выше и множество других потенциальных проблем, обеспечивая:

- доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент,
- отсутствие необходимости сетевых обращений при проверке подписи
- **архивное хранение электронных документов,**
- простоту встраивания и отсутствие необходимости контроля встраивания.

Формат усовершенствованной подписи предусматривает обязательное включение в реквизиты подписанного документа доказательства момента подписания документа и доказательства действительности сертификата в момент подписания.

Для доказательства момента подписи используются штампы времени, в соответствии с международной рекомендацией RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

Доказательства действительности сертификата в момент подписи обеспечиваются вложением в реквизиты документа цепочки сертификатов до доверенного УЦ и OCSP-ответов. На эти доказательства также получается штамп времени, подтверждающий их целостность в момент проверки.

Вложение в реквизиты документа всех доказательств, необходимых для проверки подлинности ЭЦП, обеспечивает возможность оффлайн-проверки подлинности ЭЦП. Доступ к репозиторию сертификатов, службам OCSP и службам штампов времени необходим только в момент создания подписи.

Усовершенствованная подпись КРИПТО-ПРО просто встраивается в любое приложение. Для этого не требуется углублённое знание интерфейса CryptoAPI, а также не требуется работа со всеми структурами, составляющими подпись, такими как штампы времени и OCSP-ответы.

Вся работа с подписью заключается в вызове двух функций, одна из которых создаёт подпись, другая проверяет её.

Усовершенствованная подпись использует сертифицированное ФСБ СКЗИ КриптоПро CSP. Простота встраивания делает тривиальным контроль встраивания, который осуществляется следующим образом: если в коде приложения вызываются функции создания усовершенствованной подписи, и её проверки, то встраивание выполнено правильно.

Использование усовершенствованной подписи является необходимым условием архивного хранения электронных документов, удостоверенных ЭП.

В формате усовершенствованной подписи вся необходимая информация для проверки подлинности ЭП находится в реквизитах документа. Для сохранения юридической значимости электронных документов при архивном хранении остаётся только обеспечить их целостность организационно-техническими мерами. В этом случае подлинность ЭП может быть подтверждена через сколь угодно долгое время, в том числе и после истечения срока действия сертификата ключа подписи подписчика.