квалифицированная* электронная подпись на мобильном устройстве

как технологиям не только «взлететь», но и «подняться под облака»?

текст Денис Калемберг, генеральный директор компании SafeTech

Мобильные финансовые сервисы становятся все более востребованными клиентами банков, причем не только физическими, но и юридическими лицами. Но если первым из них для подтверждения транзакций, как правило, не требуется использовать сертифицированные средства электронной подписи, то для подписи в системах дистанционного банковского обслуживания (ДБО) юридических лиц банки в большинстве случаев предпочитают выдавать клиентам «ГОСТовые» решения. А как их использовать не только на стационарных компьютерах и ноутбуках, но и для мобильных пользователей? Между тем технологии, которые все-таки могут обеспечить «взлет» идеи электронной подписи на мобильном устройстве, уже существуют и успешно внедряются.

Камнем преткновения для реализации квалифицированной электронной подписи на смартфоне или планшете является подключение к устройству носителя ключа электронной подписи. Традиционными и надежными хранилищами ключей электронной подписи являются токены или смарт-карты, но для использования вне пределов стационарных рабочих мест они не так удобны. В этой связи переход на облачное хранение ключей электронной подписи, например, в HSM, Hardware Security Module, и доступ к ним с мобильного устройства давно представлялся экспертам перспективным решением. И в этом отношении оставался только один важнейший вопрос безопасности: «Каким образом конкретный пользователь – обладатель ключа электронной подписи, хранящегося в облаке, будет получать доступ к этому ключу»?

ДОСТУП К ОБЛАКУ – КАКОЙ ВАРИАНТ ВЫБРАТЬ?

В качестве способа доступа к ключам пользователей, хранящимся в облаке, уже давно было предложено на выбор несколько вариантов: многоразовый пароль, одноразовый пароль, включая отправку кода через СМС, аутентификация с использованием токена, подключаемого к компьютеру. При этом доступ к ключам при помощи одноразовых и/или многоразовых паролей не обеспечивает приемлемого уровня безопасности и, соответственно, противоречит требованиям регулирующих органов. А использование аппаратных смарт-карт и токенов «убивает» саму идею облачной подписи. Ввиду технологических и логистических ограничений до сих пор не получила значимого развития и электронная подпись на смартфоне, основанная на использовании специальных SIM-карт, которые фактически должны были стать носителями ключей пользователей и самим средством электронной подписи.

Обойти описанные выше ограничения позволила технология аутентификации владельца облачных ключей подписи при помощи специального приложения для смартфона КриптоПро myDSS – продукта партнерского взаимодействия компаний SafeTech и КриптоПро.

КРИПТОПРО MYDSS. КВАЛИФИЦИРОВАННАЯ* ЭЛЕКТРОННАЯ ПОДПИСЬ В СМАРТФОНЕ.

Комплексное решение КриптоПро myDSS позволило внедрить в облачный сервис электронной подписи КриптоПро DSS метод формирования подтверждений на подписание на основе технологий решения PayControl компании SafeTech. Для того чтобы облако (серверная часть) выполнило подписание, ему необходима санкция владельца ключа на совершение этого действия. Она зависит от четырех составляющих: времени, содержания подписываемого документа, уникальных признаков смартфона, а также уникального ключа, который хранится в смартфоне пользователя в защищенной области. Эта схема существенно более безопасна, чем использование одноразового или многоразового пароля, так как обеспечивает неизменность электронного документа в процессе передачи на сервер подписи, кроме того, в ней не используется недоверенный СМС-канал. И она реализована в форме приложения для современных мобильных платформ.

Разработав и задокументировав схему совместной работы, компании КриптоПро и SafeTech реализовали ее и представили продукт на сертификацию в Федеральную службу безопасности Российской Федерации. В настоящий момент ведется активная работа по сертификации КриптоПро myDSS, уже получен сертификат на серверную часть комплекса КриптоПро DSS, на очереди сертификация уже всего решения в целом.

Итак, использование комплексного решения КриптоПро DSS с модулем аутентификации myDSS позволит просто и удобно ставить квалифицированную электронную подпись со своего смартфона, получая доступ в системы дистанционного банкинга в любом месте и в любое время. Пользователи ДБО получат возможность подтверждать транзакции и подписывать своей электронной подписью любые документы, причем с сохранением всех свойств безопасности и совершенно не проигрывая в удобстве. NBJ

**Решение находится в процессе сертификации ФСБ РФ*