квалифицированная электронная подпись на мобильном устройстве

как защитить цифровое взаимодействие человека с бизнесом и государством?

текст **Денис Калемберг, генеральный директор компании SafeTech**

В век цифровой экономики технологии позволяют нам общаться, делать финансовые проводки и подписывать электронные документы, не видя друг друга. Это очень удобно и позволяет сэкономить огромное количество времени, однако требуется обеспечить безопасность личности и организаций, надежно защитить их транзакции от компьютерных мошенников и при этом сохранить удобство цифрового взаимодействия граждан с государством и бизнесом. Для решения этой задачи одним из наиболее подходящих решений могла бы стать квалифицированная облачная подпись на смартфоне – мобильном устройстве, которое в последние годы стало нашим верным спутником.

ДОСТУП К ОБЛАКУ: КАКОЙ ВАРИАНТ ВЫБРАТЬ?

Камнем преткновения для реализации квалифицированной облачной электронной подписи долгое время было сохранение уровня безопасности при удаленном акцептовании (подтверждении) операции подписи, ключ которой находится, например, в HSM, Hardware Security Module.

В качестве способа доступа к ключам пользователей, хранящимся в облаке, уже давно было предложено на выбор несколько вариантов: многоразовый или 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 специальных SIM-картах, 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 ПРИ ПОМОЩИ СМАРТФОНА.

Мобильное приложение «КриптоПро myDSS» позволяет пользователю при помощи буквально двух касаний экрана смартфона подтверждать операции подписи любых электронных транзакций, вырабатывая код подтверждения транзакции, который 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 одноразовых или многоразовых паролей, так как обеспечивает неизменность электронного документа в процессе передачи на сервер подписи.

Совсем недавно, 14 февраля 2018 года, комплекс облачной подписи «КриптоПро DSS» с модулем аутентификации myDSS получил положительное заключение Федеральной службы безопасности Российской Федерации, в ближайшее время ожидается получение сертификата на данное решение.

Итак, использование комплексного решения «КриптоПро DSS» с модулем аутентификации myDSS позволит просто и удобно подтверждать любые документы и операции квалифицированной электронной подписью при помощи смартфона, получая доступ к электронному документообороту и государственным услугам, а также в системы дистанционного банкинга в любом месте и в любое время, совершенно не проигрывая в удобстве.