подпись транзакций в мобильных сервисах

главный на сегодняшний день вопрос – как снизить риски и сохранить доверие клиентов

текст Денис Калемберг, генеральный директор компании SafeTech

В последнее время целевой аудиторией банков стало то самое «поколение Z», которое еще совсем недавно приносило прибыль только разработчикам компьютерных игр, а теперь внезапно обзавелось высокооплачиваемой работой, а то и собственным бизнесом с внушительным счетом в банке. При этом доступ к счету они хотят получать с устройства, в котором проводят большую часть своего времени, – со смартфона.

Проблема в том, что если технологии подтверждения транзакций в классических системах ДБО за последние 20 лет и достигли совершенства, то резкий всплеск популярности мобильных сервисов вынудил банки облегчать процедуру подтверждения транзакций в ущерб безопасности клиентов. Банковские пароли отправляются по каналам, изначально не предназначенным для передачи конфиденциальной информации, таким как SMS и PUSH. Это привело к значительному росту числа краж у мобильных пользователей и общему снижению доверия к дистанционным банковским сервисам.

КАКИМ РИСКАМ ПОДВЕРЖЕН СОВРЕМЕННЫЙ МОБИЛЬНЫЙ БАНКИНГ И КАКИЕ ТЕХНОЛОГИИ ПОМОГУТ СДЕЛАТЬ РАБОТУ ЕГО КЛИЕНТОВ ДЕЙСТВИТЕЛЬНО БЕЗОПАСНОЙ?

Риски кражи денег со счетов пользователей существовали и в интернет-банкинге, но за счет объединения в смартфоне каналов создания и подтверждения документов возможности мошенников возросли. С другой стороны, традиционное подтверждение операций с помощью SMS вызывает много нареканий – сообщения можно перехватить как в канале оператора связи, так и в самом смартфоне. Чтобы кардинально снизить риски кражи денег со счетов пользователей, нужно выполнить два главных условия:

- не передавать коды подтверждения транзакций по незащищенным каналам связи, а генерировать их на стороне клиента;
- формировать коды подтверждения в привязке к реквизитам каждой транзакции.

Эти задачи можно решить при помощи аппаратных средств – MAC-калькуляторов (вариант затратный и требует сложной логистики), однако наиболее эффективным способом являются программные средства подписи транзакций, устанавливаемые на смартфон или интегрированные напрямую в мобильное приложение банка.

PAYCONTROL – РЕШЕНИЕ ДЛЯ СОВРЕМЕННЫХ МОБИЛЬНЫХ СЕРВИСОВ

Классическим решением для безопасной и удобной замены SMS-паролей, обеспечивающим аутентификацию, визуализацию реквизитов платежа и подтверждение транзакций на смартфоне, является PayControl компании SafeTech. Оно совмещает удобство смартфона и безопасность MAC-калькулятора: реквизиты платежа (и даже PDF-документ) загружаются автоматически, удобно просматриваются на экране, а транзакция подтверждается усиленной неквалифицированной подписью.

PayControl позволяет защитить пользователей от всех известных на сегодняшний день атак, не снижая их мобильности и даже делая работу более удобной по сравнению с классическими «кодиками».

КРИПТОСЕРВИСЫ В «ОБЛАКАХ»

Новый импульс развитию дистанционных банковских (да и не только банковских) сервисов может придать синергия от сочетания мобильных и облачных технологий аутентификации и подписи транзакций. Хорошим примером служит комплексное решение на основе PayControl и облачного сервиса электронной подписи «КриптоПро DSS».

Решение передано на сертификацию в ФСБ России. Теперь банки с минимальными затратами смогут реализовать подтверждение платежных документов на мобильных устройствах квалифицированной подписью. Для клиентов это кардинально снизит порог использования квалифицированной электронной подписи за счет отсутствия аппаратных носителей ключей. Также это обеспечит полную мобильность при сохранении юридической значимости электронного документооборота. NBJ