Вторая международная конференция «Мобильная коммерция и платежи»
16-17 мая 2007г., г. Москва, Отель «Новотель»

infor-media Russia
Контакты. Информация. Решения.

Некоторые вопросы идентификации и аутентификации в мобильных платежных системах

Кирюшкин Сергей Анатольевич, к.т.н.
Генеральный директор ЗАО «АНК»
г. Санкт-Петербург, ул. Бабушкина д.3
Тел. +7 (812) 567-89-95; +7 (812) 567-38-56
Факс: +7 (812) 567-49-34
E-mail: ksa@ank-pki.ru

Цель доклада

- На качественном уровне **оценивание эффективности** внедрения технологий идентификации и аутентификации (ИА) в мобильных платежных системах **на основе инфраструктуры открытых ключей (PKI)**

Вопрос 1:

Зачем в МПП нужен PKI? Ведь и так все работает…

Предпосылки к рассмотрению вопроса

- **Федеральный закон от 7 августа 2001 г. N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем"** Статья 7. Обязанности организаций, осуществляющих операции с денежными средствами или иным имуществом

Вопрос:

Организации, осуществляющие операции с денежными средствами или иным имуществом, обязаны:

- **идентифицировать личность, которая совершает операции с денежными средствами** или иным имуществом, подлежащие обязательному контролю, либо открывает счет (депозитный вклад), по предъявляемым документам…

Как это сделать в электронной мобильной среде?

Предпосылки к рассмотрению вопроса

Ответ:

- **Изготовление сертификатов ключей подписей** осуществляется **на основании заявления участника информационной системы**, которое содержит сведения, указанные в статье 6 настоящего Федерального закона и необходимые для идентификации владельца сертификата ключа подписи и передачи ему сообщений. **Заявление подписывается собственноручно владельцем сертификата ключа подписи. Содержащиеся в заявлении сведения подтверждаются предъявлением соответствующих документов.**

ФЗ “Об ЭЦП” (Статья 9, п.2)

Предпосылки к рассмотрению вопроса

Ответ:

- **Сертификат ключа подписи** - документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы **для подтверждения подлинности электронной цифровой подписи** и **идентификации** владельца сертификата ключа подписи

ФЗ “Об ЭЦП” (Статья 3)

Предпосылки к рассмотрению вопроса

- Начиная с определенной “психологической” суммы мобильного платежа (например 1000 руб.)
  - абонент серьезно задумывается о “квитанции” подтверждающей факт платежа;
  - Оператору “квитанция” требуется (или желательна) для разбора потенциальных конфликтных ситуаций.

Вопрос:

Как получить квитанцию в электронной мобильной среде?

Предпосылки к рассмотрению вопроса

- Зачастую изменение условий обслуживания (предоставление новых сервисов, изменение тарифных планов и пр.) предполагают получение согласия со стороны абонента.

Вопрос:

Как это сделать не заставляя абонента прибывать в офис оператора?

Предпосылки к рассмотрению вопроса

Ответ:

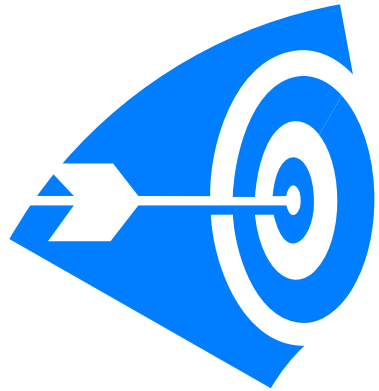
Электронная цифровая подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

ФЗ “Об ЭЦП” (Статья 4)

Вывод 1:

- Возможности предоставляемые инфраструктурой открытых ключей, в частности для ИА в мобильных платежных системах востребованы.



Вопрос 2:

Насколько это эффективно?

Опыт использования PKI

- Международный опыт, в том числе и в интересах мобильных платежных систем (Mobilkom Austria, Valimo);
- Российский опыт, в том числе практика реализации систем в соответствии с ФЗ «Об электронной цифровой подписи»

Требования к ИА для МПС

- Результативность
- Простота внедрения
- Простота применения

Результативность ИА

- Обеспечение требуемого уровня защищенности отношений субъект-объект доступа;
- Обеспечение юридической значимости ЭД;
- Обеспечение дополнительных сервисов

Простота внедрения

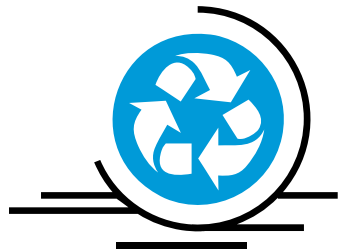
- Определяется:
  - Наличием технической и технологической базы решения;
  - Наличием базовой инфраструктуры для развертывания обслуживания;
  - Опытом внедрения сходных технологических решений.

Простота применения

- Определяется:
  - Техническим совершенствованием мобильных терминалов;
  - Унификацией пользовательских интерфейсов (для пользователя всё должно быть знакомо и понятно);
  - Базируется на знакомых принципах бумажного документооборота (для процессинга).

Вывод 2:

- Применение ИА на основе PKI в МПС эффективно



Спасибо за внимание!

Готов ответить на Ваши вопросы…

Кирюшкин Сергей Анатольевич, к.т.н.
Генеральный директор ЗАО «АНК»
г. Санкт-Петербург, ул. Бабушкина д.3
Тел. +7 (812) 567-89-95; +7 (812) 567-38-56
Факс: +7 (812) 567-49-34
E-mail: ksa@ank-pki.ru