Стандартизированные решения по использованию Российских криптоалгоритмов в платежных системах: вопросы безопасности

Елистратов Андрей Алексеевич

Часть I

НСПК

- АО «Национальная система платёжных карт» создано **23 июля 2014 года**.
- С **1 апреля 2015 года** платежи внутри России по всем пластиковым картам, включая Visa и MasterCard, проходят через НСПК.
- **15 декабря 2015 года** Банком России и НСПК было объявлено о начале эмиссии платёжных карт «Мир».

НСПК

1 мая 2017 Президент РФ подписал закон о переводе бюджетных выплат на карты «Мир».

Законом предусмотрены три этапа:

- **с 1 июля 2017 года** – для новых сотрудников государственных бюджетных учреждений и пенсионеров;
- остальные сотрудники бюджетных организаций получат карты «Мир» **до 1 июля 2018 года**;
- для пенсионеров предусмотрен постепенный переход на карты «Мир» до **1 июля 2020 года.**

НСПК

- В настоящее время НСПК функционирует с использованием закупленного оборудования иностранного производства.

- По сути взята инфраструктура одной международной платежной системы (МПС), которая была развернута и введена в эксплуатацию на территории Российской Федерации.

Требования по безопасности НСПК

- Положение Банка России 382-П
- Payment Card Industry Data Security Standard (PCI DSS)
  Последняя редакция данного документа – 3.2 – датирована 2016 годом
- EMV 4.3

Требования к криптографическим преобразованиям НСПК

- PCI DSS

  В PCI DSS в явном виде не приводится требований к криптографическим примитивам, которые должны использоваться для решения конкретных задач. При этом вводится понятие стойкой (сильной) криптографии (от англ. Strong Cryptography). Под стойким понимается некоторый набор криптографических примитивов (как симметричных так и асимметричных), минимальная стойкость которых оценивается 112 битами (данный уровень стойкости, по всей видимости, в первую очередь определяется не криптографическими, а эксплуатационными причинами).

Требования к криптографическим преобразованиям НСПК

- EMV 4.3

  Анализ решений, зафиксированных в спецификациях EMV 4.3, к настоящему моменту выявил ряд серьезных угроз, связанных с использованием зарубежных криптографических механизмов в данных решениях. Эти угрозы, являются следствием традиционной для зарубежных механизмов «старости» используемых подходов. История создания многих из используемых механизмов восходит к началу развития массовой криптографии (90-е годы XX века).

Требования к криптографическим преобразованиям НСПК

Итог

Иностранные криптографические решения для платежных систем имеют следующие недостатки:

-невозможность проведения оценки качества формируемых ключей;
- возможность использования слабых криптографических алгоритмов (TDES 112 бит, RSA и т.п.);
- отсутствие доказуемой стойкости криптографических решений.

-при сертификации HSM модулей по EMV сертификации подлежит только аппаратная часть и загрузчик. Программные модули, реализующие криптографические алгоритмы платежной системы не фиксируются.

Что делается в России

- С 2015 года в соответствии с планом мероприятий по внедрению СКЗИ с российскими криптографическими алгоритмами в банковской индустрии России ведется работа, направленная на обеспечение необходимого уровня безопасности в НСПК.
- Утвержден план мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации».

Что делается в России

- В программе «Цифровая экономика Российской Федерации»

05.02.009.004.004:

Разработка и утверждение рекомендаций по стандартизации, определяющих отечественные криптографические механизмы в компонентах платежной инфраструктуры, в том числе:

1. Отечественные криптографические механизмы в механизмах **EMV**, используемых в платежных картах;
2. Универсальное **API** для встраивания HSM в банковское ПО, POS и ATM и требований по проверкам корректности встраивания;
3. Дистанционную загрузку и смену ключевых последовательностей в устройствах самообслуживания (POS, ATM, мобильные терминалы);
4. Криптографические алгоритмы в «электронной торговле».

Что сделано в России

- На базе Технического комитета по стандартизации ТК26 был создан Подкомитет №3. В рамках деятельности указанного подкомитета разработан комплект методических рекомендаций (**8 базовых протоколов системы платежных карт**) аналогичных стандарту международных платежных систем EMV 4.3.
- Указанный комплект рекомендаций является достаточным для реализации в НСПК стандартного набора сервисов с спользованием российских криптографических алгоритмов.

Что делается в России

- **Росстандартом утверждены 6 рекомендаций по стандартизации** в сфере применения отечественных криптографических механизмов в национальной системе платежных карт:

  Документы вводятся в действие для применения в Российской Федерации

  с 1 июня 2018 г.

- Р 1323565.1.009-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах».;
- Р 1323565.1.007-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»;
- Р 1323565.1.010-2017 «Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения»;
- Р 1323565.1.008-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением»;
- Р 132365.1.011-2017 «Информационная технология. Криптографическая защита информации. Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN».
- Р 132365.1.013-2017 «Информационная технология. Криптографическая защита информации. Использование режимов алгоритма блочного шифрования в протоколе защищенного обмена сообщениями в процессе эмиссии платежных карт».

Что надо сделать

- Утвердить в Росстандарте оставшиеся 2 рекомендации по стандартизации.
- Обеспечить внедрение стандартов в процесс эмиссии и процессинг карт «МИР».

Что надо сделать

Разработать рекомендации:

- 1) формирование и имитозащиты сообщений при проведении операции по протоколу 3-D Secure (аналог MAC/HMAC для сообщений AAV/CAVV),
- 2) выработки одноразовых паролей (технологии CAP/DPA),
- 3) формирования подписи сообщений PARes закрытым ключом ACS,
- 4) установление TLS-соединений с взаимной аутентификацией сервера и клиента.

И утвердить их в Росстандарте.

Что надо сделать

Активные участники Подкомитета №3 ТК26 :

1. СПБ.
2. КриптоПро.
3. ИнфоТеКС.

Спасибо за внимание