Анализ развития PKI в России

«PKI - это не только электронная подпись» – С.М. Муругов

Сабанов А.Г., д.т.н., профессор ИУ-10 МГТУ им. Баумана
эксперт ISO/JTC1/SC27/WG5, ТК-362, ТК-122, ТК-26
Заместитель генерального директора
АО "Аладдин Р.Д."

Краткая история PKI-форумов

- Ноябрь **2003** Первая конференция PKI-форум – это секция в рамках выставки «Охрана и безопасность» на территории Ленэкспо. Около 30 участников, костяк составляют генеральные директора УЦ. Главная тема: как правильно построить УЦ?
- Ноябрь **2004** Первое участие наших польских коллег. Уже около 70 участников. Основной вопрос: окупаемость УЦ.
- Ноябрь **2005** Собралось 150 участников, среди них представитель ФАИТ А.Домрачев. Форум проходит в Ленэкспо, проживание - в «Прибалтийской». Тема: как убрать несовместимость средств ЭП?
- Ноябрь **2006** Форум переехал в «Балтиец» (Репино). Председатель оргкомитета и ведущий пленарного заседания с этого года - В.Г.Матюхин. Основные темы – трансграничное взаимодействие, OID.
- …
- Сентябрь **2010**. Более 300 участников. Число аккредитованных Минкомсвязью УЦ приблизилось к 160. Основные темы: организация работы уполномоченного федерального органа, федер. УЦ, PKI как основа электронного правительства, проблемы отчетности ФНС.
- …
- с 2009 по наст. время организатор – Медиа-группа Авангард. Прибалтийская, Москва, Прибалтийская, Азимут, Кортъярд – профессионалам все равно, где обсуждать самые актуальные вопросы PKI.

Краткая история развития PKI

До 2002г. ЭЦП уже применяется в системах «клиент – банк» и некоторых ЭДО - небольших системах с ограниченным числом участников.

2002г. Принят 1-ФЗ, МНС РФ вносит изменения в Налоговый кодекс. В 1-ФЗ определен «Уполномоченный федеральный орган (УФО)», но его функции были сильно заужены. Не было определено ЕПД ЭП и пути его создания.

2005-2010 Ведомства строят свои «сети доверия»: Приказ №346 ФНС – 2006г., Распоряжение №190 ПФР - 2007, приказ №19 ФСС-2010, Приказ №251 Росстат – 2010 и др. Для обеспечения взаимодействия 80 УЦ связываются кросс-сертификатами, которые обеспечивали проверку сертификатов КЭП до 2017г.

2009-2012 интенсивное строительство ЕПД ЭП. Появление TSL – списка доверенные УЦ МКС на основе Приказа МКС 41-2009 и Приказа ФАИТ 144 – 2009. В 2010 появился 210-ФЗ о госуслугах, портале госуслуг и СМЭВ. Число УЦ-160.

2012-2015 С выходом 63-ФЗ вся системы PKI заработали по-новому, хотя неготовность прикладного ПО и ИС заставили перенести ввод 63-ФЗ на год. ИС ГУЦ начал работу. Наступила первая стадия ЕПД ЭП и СКПЭП. Число УЦ-300.

2018 УЦ ГУЦ заработал в полной мере. Система УЦ перестроена на иерархию.

2019-2021 реформа системы УЦ в России: вместо 500 УЦ стало всего 3 +25 УЦ

PKI – это не только подпись

Инфраструктура открытых ключей (PKI - *Public Key Infrastructure*) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки **доверия к цифровым сертификатам** открытого ключа и решения различных криптозадач на основе **закрытого и открытого** ключей.

1.закрытый ключ должен быть известен **только его владельцу**;

2.удостоверяющий центр(УЦ) создает цифровой сертификат открытого ключа, удостоверяя факт того, что закрытый (секретный) ключ известен **только владельцу этого сертификата**, открытый ключ содержится и свободно передается в сертификате;

3.основу **доверия** составляет система удостоверяющих центров;

4.удостоверяющий центр подтверждает или опровергает **принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом,** что ключ не отозван и продолжает действовать (CRL).

Главный объект PKI - цифровые сертификаты

PKI нужна для обеспечения жизненного цикла цифровых сертификатов:

- **сертификат доступа**, подписывается корпоративным СА, ГОСТ Р ИСО/МЭК 9594-8-98 (простая и строгая аутентификация), алгоритм RSA
- **сертификат ключа проверки электронной подписи**, квалифицированный сертификат подписывается аккредитованным УЦ, 63-ФЗ, приказ ФСБ России № 795 – 2011, приказ ФСБ России № 31 от 29 января 2021
- **атрибутный сертификат** – пока не используется в РФ и никак не регулируется, ITU-T X.509 – 2011 (!), атрибутный сертификат применяется в Белоруссии с 2015г.

Где нужна PKI

PKI обеспечивает **доверенную** среду между субъектами информационного взаимодействия, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей и цифровых сертификатов.

Области применения:

- защищенное сетевое взаимодействие,
- удаленный доступ,
- отчетность в электронном виде,
- электронная почта,
- защищенный обмен информацией,
- ЭДО,
- электронная коммерция,
- службы обработки транзакций Web.

Доверие (assurance): Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности. Примечание – Результаты, получаемые в рамках обеспечения доверия, рассматриваются в качестве оснований для уверенности. [ГОСТ Р 58833–2020, пункт 3.15]

Изменения в N 63-ФЗ от 6.04.2011

Список изменяющих документов:

- от 01.07.2011 N 169-ФЗ
- от 10.07.2012 N 108-ФЗ
- **от 05.04.2013 N 60-ФЗ**
- от 02.07.2013 N 171-ФЗ
- от 02.07.2013 N 185-ФЗ
- **от 12.03.2014 N 33-ФЗ**
- **от 28.06.2014 N 184-ФЗ**
- **от 30.12.2015 N 445-ФЗ**
- от 23.06.2016 N 220-ФЗ

- **от 27.12.2019 N 476-ФЗ**
- от 08.06.2020 N 166-ФЗ
- от 08.06.2020 N 181-ФЗ
- **от 23.06.2020 N 183-ФЗ**
- от 24.02.2021 N 20-ФЗ
- **от 24.03.2021 N 50-ФЗ**

+34 нормативных акта

- Правительства РФ
- Федеральных органов ИВ
- ЦБ РФ

Как оценивать развитие PKI

Показатели

1. Уровень проникновения

Население 145 млн - 30 млн пенс. -17 млн школьн. - 4 млн студентов -…. Всего 72 млн занятых (Росстат)

Официальных данных по уровню проникновения PKI не имеется.

Оценки ФНС: около 8 млн. PKI+КЭП. Мои оценки: порядка 10 млн. используют PKI в задачах доступа

2. Области использования (перечислены на слайде 6)

3. Применение сервисов безопасности (кроме ЭП нужны штампы времени, аутентификация подписанта, проверка валидности сертификата, проверка полномочий, гарантированная доставка)

Критерии оценки развития PKI пока не определены.

Успехи PKI. Применение КЭП в органах гос. власти, ГИС и приложениях специальных операторов

- Госуслуги.ру
- ФНС России
- ЕГАИС (РАР, лес)
- ПФР
- ФТС
- Нотариат
- Росреестр
- ФСС
- РГС (например, mos.ru)
- Росстат
- Рособрнадзор и др.

Площадки и приложения спец.операторов:

- АО ПФ СКБ Контур
- ООО Компания Тензор
- АО Калуга Астрал
- ООО Такском
- АНО БЕЛИНФОНАЛОГ
- ООО КОРУС Консалтинг СНГ
- ООО РПЦ Партнер
- ООО Русь-Телеком
- …..

Всего в офиц. перечне на сайте ФНС 79 операторов

Успехи PKI. Торговые площадки

Федеральные торговые площадки (Госзакупки):

- Сбербанк-АСТ;
- Национальная электронная площадка;
- РТС-Тендер;
- Росэлторг;
- Zakaz-RF;
- РАД;
- Газпромбанк;
- ТЭК-Торг.

Коммерческие торговые площадки:

- B2B-Center;
- Фабрикант;
- Торги 223;
- Группа площадок «ОТС»
- и т.д. (более 100)

Площадки по реализации имущества (торги по банкротству):

- ruTender;
- Аукционный тендерный дом;
- Электронная торговая площадка (ETPRF);
- KARTOTEKA.RU
- и т.д.

Проблемы развития PKI в РФ

Нормативную базу пишут юристы без учета мнения «технарей» и экспертов.

Ведомственная раздробленность: в каждом ведомстве своя система УЦ, свои правила применения ЭП, исторически сложившаяся доменная структура (Novell, IBM, Microsoft). Подавляющая часть администраторов обучились в Microsoft.

Обязанность УЦ идентифицировать субъекта перед выдачей СКПЭП изначально была помещена в статью 18 (практически в конец) Федерального закона 63-ФЗ. 10 лет не было подзаконных актов о методах и методике идентификации субъектов. Следствия:

- определение личности владельца КЭП определялось так, как понимали УЦ;
- были УЦ, выдававшие СКПЭП по «скайпу», не заботясь об идентификации владельцев.

В процессе развития PKI менялась модель доверия системы УЦ – с кросс-сертификатов на иерархическую.

До сих пор появляются непродуманные с технической точки зрения решения. Примеры: МЧД, недавнее изменение формата сертификата.

Частые изменения в отдельные положения основных федеральных законов…???

Проблемы стандартизации

- Зоны ответственности поделены между ТК 22, ТК 26, ТК 362 и др.
- Основной стандарт PKI разрабатывается и совершенствуется экспертами МСЭ и ИСО с 1988г. – ITU-T **X.509**. В России имеется перевод МСЭ, датированный 2007г.
  - Служба каталога, структура сертификатов, атрибутных сертификатов, …
- Стандарт по сервисам ДТС **X.842** – официального перевода нет
  - Службы управления ключами и сертификатами, атрибутирования, персонализации, аутентификации, доставки, неотказуемости, штампов времени
- Стандарты по идентификации, аутентификации – идем почти в ногу с ИСО
- Стандарты по защите персональных данных – отставание 2:20
- Стандарты по криптографии – ТК 26
- Стандарты по применению ЭП в прикладном ПО – группа 17 стандартов CEN не адаптирована

Выводы

1. Единое пространство доверия к КЭП в России построено
2. Единое пространство доверия к электронным документам с ЭП пока не достигнуто. Остаются не совсем решенные проблемы:
   - Доверие к полномочиям (с помощью МЧД) пока не решена
   - Доверие к идентификации гражданина/представителя ЮЛ перед выдачей ему квалифицированного сертификата ключа проверки ЭП решена не полностью
   - Проблема доверия к результату аутентификации подписанта пока не решена (доступ к прикладному ПО в большей части по паролям)
   - Проблема доверия к поддержанию других сервисов безопасности, обеспечивающих юридическую силу электронному документу, решена не полностью
3. Нормативно-правовая база нуждается в продуманном и научно обоснованном совершенствовании
4. Стандарты существенно отстают от развития PKI в РФ.

Аладдин - будь собой в электронном мире!

Спасибо!

Алексей Сабанов

Заместитель генерального директора

АО "Аладдин"

8 (495) 223 0001

www.aladdin.ru

QR