International association
e-Signature Without Borders

X Международный PKI-Forum
г. Санкт-Петербург,
18 – 20 сентября 2012 г.

Реальные PKI-сервисы
и
экономика PKI-бизнеса

Анализ имеющейся практики использования PKI-сервисов.

Разнообразность практики использования PKI-сервисов в ЕЭС начинается **с носителей сертификатов и ключей подписи.**

По имеющимся данным:

1**. ID-КАРТЫ.**

- К началу марта 2012 **ID-карты** доступны в 11 странах (**Бельгия, Финляндия, Италия, Лихтенштейн, Литва, Португалия, Испания, Эстония, Хорватия, Германия** (с ноября 2010), **Швейцария** (с мая 2010)), и планируется ввести еще в 7 – **Польша** (начало или середина 2013), **Франция** (в 2010 приняла законопроект о защите личности, который предполагает введение ID-карты, но сроки не определены до сих пор), **Греция** (планировала введение ID-карты в 2011, но до сих пор данных о внедрении карт нет), **Латвия** (выдача электронных ID-карт по плану начнется с 1 Апреля 2012), **Румыния** (2014), **Мальта** (середина 2012), **Словакия** (конец 2012).
- В 2010 году после формирования нового правительства Великобритания присоединилась с списку из одиннадцати стран, которые **не планируют** выпуск ID-карт, и в феврале 2011 года объявила об уничтожении Национального идентификационного регистра.
- ID-карты выдаются государством (в 7 странах) или уполномоченными частными структурами (6 стран) и обеспечивают создание квалифицированных подписей.
- Среди стран, не входящих в ЕС, электронные ID-карты представлены: **Албания** (с декабря 2009), **Армения** начала выпуск ID-карт с середины 2012 года, **Грузия** начала выпуск ID-карт с 1 августа 2011. **Украина** заявляет о технической готовности для внедрения ID-карт (сроки не известны). В России ситуация непонятная, т.к. внедрение Универсальных Электронных Карт (УЭК) отложила до 2013 года и буквально в последнее время рассматриваются альтернативные варианты универсальной идентификационной карты, вплоть до введения нового вида документа.

International association

e-Signature Without Borders

2. СПЕЦИАЛЬНЫЕ СМАТР-КАРТЫ

Сектор специфических смарт-карт, используемых в PKI-сервисах для ограниченного круга пользования или в специфической области применения (банковские, карты социального обеспечения, здравоохранения, а так же карты госслужащих).

В период с конца 2010 по начало 2012 в дополнение к смарт-картам, представленным в 9 странах, добавились:

-**Германия** представила электронные карты врача, электронные медицинские карты пациента, электронные разрешения для иностранцев (2011),

- **Франция** ввела электронные карты для полицейских (2011),

- **Эстония** представила карту вида на жительство иностранца, проживающего на территории Эстонии на основании вида на жительство и не являющегося гражданином ЕС (2011).

- **Польша** планирует с 2013 выдавать электронные карты пациента.

- **Болгария**. Частная компания объявила о начале выпуска смарт-карт для доступа к картам-здоровья военных и членов их семей (2010),

- **Италия** представила смарт-карты для беременных (2010).

- **Словакия** планирует выдавать электронные карты здоровья с 2013.

Крипто-токены присутствуют в 22 странах, программные сертификаты – в 18. Выпускаются эти средства частными компаниями.

Только единственной стране ЕС (Эстония) обеспечивается функция электронной печати организации.

Мобильные подписи доступны сейчас всего в 7 странах (**Финляндия, Литва, Норвегия, Польша, Эстония**). **Австрия** представила мобильные подписи с декабря 2009, спустя два года активация мобильной подписи обеспечивается всеми налоговыми департаментами на бесплатной основе.

Основные сферы использования

Взаимодействие с государством посредством PKI-сервисов в ЕС сводятся в основном к госзакупкам, здравоохранению, юстиции, налоговой отчетности, социальному обеспечению, торговле, получению госуслуг.

Госзакупки. В дополнение к 15 реально работающим приложениям, в 2011-2012 были представлены:

-**Швейцария** (2011) к товарам и услугам добавила строительный сектор для размешения закупок в электронном формате,

- **Франция.** С начала 2012 участники процедур госзакупок обязаны принимать предложения цены в электронном виде для всех закупок стоимостью от 90 000 евро.

- **Греция** провела презентацию электронных аукционов в начале 2011.

- **Мальта** в середине 2011 перевела тендерные документы по госзакупкам в электронный вид, в октябре 2011 представила полностью электронные аукционы.

- **Дания** представила систему электронных госзакупок для всех государственных структур с начала 2012.

- **Финляндия** приступила к переходу на электронные госзакупки со второй половины 2011.

- **Швеция** планирует представить законченное решение по электронным госзакупкам к осени 2012.

Из этих приложений на квалифицированных сертификатах основаны 6, на расширенных на базе квалифицированных – 2, на расширенных – 6, и только 1 – на простой подписи.

Из этих приложений только три **(Ирландия, Дания и Словакия**) не имеют ограничений по юрисдикции заявителя, да и то в **Ирландии** в этом сервисе PKI не используется, а все сведено к «он-лайн» регистрации.

в **Словакии** используются сертификаты расширенной подписи, высылаемые по э-майлу.

Дания перешла на единую электронную подпись NemID в середине 2011.

В еще двух странах (**Австрия и Норвегия**) допустимо использование ЭЦП из узкого круга стран. В остальных случаях этими приложениями могут пользоваться только свои резиденты.

International association

e-Signature Without Borders

Здравоохранение

За период с конца 2010 по начало 2012 электронная запись к врачу была представлена в: **Германии**, Берлин (конец 2011), **Македонии** (январь 2012), **Чехии** (январь 2012).

Дигитальные рецепты введены в следующих странах: **Эстония** (в 2010 г.), **Польша** (середина 2011 – пилотный проект), **Португалия** (август 2011), **Финляндия** (2010), **Норвегия** (октябрь 2011), **Нидерланды** (январь 2012), **Хорватия** (2011).

Электронные медицинские карты пациента внедрены в **Румынии** (2010 – пилотный проект), **Польша, Словакия и Дания** планируют введение электронных медицинских карт в ближайшие два года. **Латвия** представила медицинские услуги на портале электронного Правительства с сентября 2010. **Великобритания** объявила о запуске электронной системы здравоохранения в тюремных и исправительных учреждениях в апреле 2011. **Болгария** запустила сервис электронной регистрации новорожденных с начала 2012. **Италия** представила сервис е-Здоровья на вебсайте Министерства Здравоохранения в августе 2011.

Из всех реально работающих приложений 7 используются для защищенного обмена информацией, остальные три – к узко специфическим сферам.

Есть проблемы с определением роли подписантов.

Возможность трансграничного использования PKI-сервисов в этой сфере практически отсутствует (в середине 2011 **Польша и Германия** провели первое трансграничное телемедицинское сотрудничество. В конце декабря 2011 **Еврокомиссия** объявила о создании e-Health Network (Сети электронного Здоровья) с целью объединения национальных медицинских сервисов). Но, справедливости ради, надо отметить, что и потребность в этом – так же невелика, т.к. взаимодействие осуществляется, как правило, в пределах одной страны.

Система права.

Реально работают 7 приложений. Но и тут имеются проблемы с верификацией юридической роли лиц (нотариусы, судьи, адвокаты и т.п.). 5 приложений работают в области судебного производства и управления (**Ирландия, Италия, Польша, Португалия, Эстония**), 4 – связаны с регистрацией компаний (**Хорватия, Германия, Эстония, Польша** (с 1 июля 2011)), 3 - относятся к службам нотариальных архивов (**Австрия, Словения, Эстония**).

Относительно типов сертификатов, то 4 основаны на квалифицированных сертификатах (**Австрия, Германия, Польша, Эстония**), и по одному – на расширенной, основанной на квалифицированных сертификатах (**Словения**), расширенной (**Португалия**) и простой (**Ирландия**).

Возможность трансграничного использования реализована только в **Эстонии**, и в отношении узкого круга стран и между Финляндией, Литвой, Бельгией, Португалией и Испанией (с начала 2010).

В июле 2011 Запущен Европейский Портал Электронного Правосудия (https://e-justice.europa.eu).

О ВАЛИДАЦИИ

- Особо нужно отметить проблему валидации (проверки) ЭЦП. Если в 2007 году сервис валидации существовал только в Испании и Эстонии, то к концу 2010 добавились всего 4 страны (**Польша, Австрия, Германия и Норвегия**). С начала 2012 года Испанская платформа ЭЦП @firma обеспечивает сервис проверки ЭЦП и электронных сертификатов со следующими странами: **Австрия, Бельгия, Эстония и Португалия**. В феврале 2011 **Польша и Норвегия** подписали двустороннее соглашение об электронных подписях с целью проверки и валидации ЭЦП на основе электронных идентификаторах (eID) от более чем 300 провайдеров по всей Европе.
- Несколько проектов по валидации ЭЦП проводятся под руководством Еврокомиссии: STORK (Secure Identity Across Borders Linked), PEPPOL (Pan-European Public Procurement Online), SPOCS (Simple Procedures Online for Cross-border Services). В 2011 году в ходе реализации проектов были достигнуты некоторые успешные результаты: в марте 2011 первый электронный инвойс был отправлен, получен, подтвержден и оплачен и первые два виртуальных досье компаний (Virtual Company Dossiers) были созданы и отправлены с применением решений PEPPOL; в апреле 2011 Норвегия присоединилась к инфраструктуре PEPPOL; в марте 2011 Греция стала первой страной-членом ЕС, использующей Open e-PRIOR (открытая платформа электронных госзакупок, соединенная с PEPPOL); в мае 2011 Великобритания отправила Европейской Комиссии первые два электронных инвойса, использую инфраструктуру PEPPOL; в ноябре 2011 Италия приступила к использованию решений PEPPOL; в марте 2012 была представлена новая версия Open e-PROIR, включающая WEB-портал для электронных инвойсов, который позволяет крупным и мелким компаниям и индивидуальным предпринимателям отправлять электронные инвойсы клиентам, у которых установлено ПО Open e-PRIOR. В октябре 2010 были запущены 6 пилотных проектов STORK для обеспечения трансграничного взаимодействия электронных документов в Европе, и в январе 2012 был запущен новый проект STORK 2.0.

International association

e-Signature Without Borders

- К сожалению, география возможности проверки валидности ЭЦП в этих проектах весьма узка - как по организационным причинам, так и по причинам техническим и технологическим, о которых говорилось выше.
- Кроме этого, существенную проблему создает и использование несовместимых идентификаторов (например, регистрационного номера, VAT-номера и т.п.) как части подписи, а так же ролей подписанта.
- Из общего количества заявленных приложений «э-Правительств» только 69 можно оценить как способные создать эффективное использование ЭЦП (на всех видах сертификатов ЭЦП).

- Как видно, несмотря на значительные достижения в этой области, еще необходимо приложить массу усилий для расширения возможностей использования PKI-технологий для обеспечения эффективного взаимодействия.

International association

e-Signature Without Borders

Экономика PKI-бизнеса

на примере Эстонии.

- Услуги на базе PKI начинают свою историю с 2002 года. При этом впервые идея создания услуг на базе PKI и ID-card появилась в конце 1997 года. За это время были разработаны и реализованы технические идеи и приведена в соответствии с заявленными целями правовая база.
- С конца 2001 года населению стала предлагаться идентификационная карта (ID-card). До 2008 года получение ID-card была добровольной процедурой. Позднее – обязательной для всех лиц, старше 14 лет. В 2006 года населению было выдано 20 тыс. ID-card. На 18 сентября 2011 года действует 1.163.917 **активных** ID-card. Население Эстонии составляет 1,350,000 человек.

ID-card + личный код = ОСНОВА

- ID-card представляет собой пластиковую карту формата аналогично банковской карте, на которой в защищенном режиме напечатаны фотография и необходимые личные данные, а также имеется встроенный чип, на котором в защищенном от копирования режиме записаны открытый и закрытый ключи, сертификат и личная информация, дублирующая напечатанную. В ближайшее время планируется записывать и биометрическую информацию.
- ID-card имеет статус национального удостоверения личности. Выдается органами МВД. В соответствии с законом, запрещено требовать предъявления какого–либо другого документа для удостоверения личности. Действует на всей территории Эстонии, а так же признается и в других государствах ЕС.

ID-card + личный код = ОСНОВА

- В качестве основного признака идентификации используется личный код *(11-значное число, содержащее: пол, год, месяц, дату рождения, регион регистрации и две учетных цифры)*. Личный код, в отличие от фамилии и имени – остается неизменным на весь период жизни (пребывания) в Эстонии. Личный код имеет любой человек (в том числе и дипломаты), находящийся на территории Эстонии легально на любом основании, кроме визы.
- Госпошлина за получение ID-карты – около €**20**. Для молодежи и пенсионеров – может выдаваться **бесплатно**.
- Срок действия ID-card и сертификатов – 5 лет.
- Замена сертификатов происходит бесплатно для пользователя, но УЦ, обновивший сертификат получает от государства дотацию в размере около €**1,20**. При утрате ПИН-кодов для использования ID-карты замена кодов производится без проблем в Департаменте гражданства и миграции или в любом отделении любого банка. Услуга бесплатная при обращении в орган МВД, и платная при оформлении через банк (€**1,92).**

International association

e-Signature Without Borders

Техническая составляющая для пользователя

- Для использования ИД-карты на компьютере пользователя должно быть установлено программное обеспечение (имеется для большинства видов компьютерных платформ и операционных систем). ПО скачивается **бесплатно** с сайта головного УЦ Эстонии. ПО регулярно обновляется.
- Так же используется считыватель ИД-карты (более 10 типов, стоимость в розничной продаже около €**6,00**, при оформлении некоторых услуг (например, открытие счета в банке) – выдается клиенту **бесплатно**.
- Использование ID-карты в совокупности со считывателем и ПО обеспечивает авторизацию в электронной среде государственных и частных структур и создание электронной подписи.

Mobil-ID – следующий шаг в развитии PKI-сервисов

- С 2009 года параллельно с ID-картой в качестве средства идентификации в электронной среде и электронной подписи стала активно использовать система Mobil-ID. Основой системы является SIM-карта, на которой, помимо обычных для любой SIM-карты свойств, имеются криптопроцессор, ключи. ID-SIM жестко привязана к личности человека. Может быть получена в любом представительстве любого из трех мобильных операторов Эстонии на основании договора. Но ID-SIM может быть активирована **только при использовании ID-карты** (для исключения мошенничества на уровне оформления ID-SIM). Получение ID-SIM **бесплатно**. Обслуживание в части услуг Mobil-ID – **€6,35** в месяц. Функциональность и надежность работы Mobil-ID обеспечивается созданным на базе DigiDoc-сервиса взаимодействием: запрашивающего услугу человека + предоставляющего услугу лица (например, банка) + мобильного оператора + УЦ.
- Основным достоинством Mobil-ID является отсутствие необходимости иметь на используемом компьютере какого-либо ПО и считывателя ID-карты. В настоящее время выявлено всего 6 определенных моделей мобильных телефонов (устаревшего образца), которые НЕ поддерживают работу с Mobil-ID.
- Mobil-ID без проблем работает в роуминге, и это не влечет дополнительных затрат.

Экономика PKI-сервисов. Идентификация.

- **Идентификация личности** в электронной среде осуществляется бесплатно для пользователя. За услугу достоверной идентификации, которую оказывает УЦ, платит проверяющая сторона – структура, оказывающая услугу (государственная или частная структура). Стоимость этой услуги зависит от желаемого пакета (10 вариантов), который гарантирует количество обращений и скорость их обработки. Стартовый (пробный) можно получить **бесплатно на 6 месяцев**. При этом гарантируется обработка **8.000 обращений** со скоростью не менее 1 в секунду. Цена минимального стандартного пакета (**4000 обращений в месяц**, скорость обработки 1/сек) – дает стоимость **0,048 EUR/запрос;** максимального (**750.000 обращений**, скорость 30/сек) – **0,007 EUR/запрос**. Кроме стандартных пакетов при необходимости обработки более 750.000 запросов можно оформить и персональный пакет, по договорной цене.
- Для государственных структур для оплаты услуг валидности сертификата предусмотрены бюджетные деньги.

International association
e-Signature Without Borders

PKI-сервисы. Подпись.

- **Подпись документов** осуществляется в он-лайн режиме, т.к. в соответствии с требованиями «Закона об ЭЦП» (пункт 2 третьего абзаца § 2): *"Цифровая подпись вместе с использующей ее системой должна позволять точно установить время цифрового подписывания"*. Штамп времени и услуга подтверждения действительности являются самыми эффективными инструментами определения времени подписания. Просто добавления времени подписания документа недостаточно, поскольку его легко фальсифицировать. Поэтому использование внешнего штампа времени является необходимым условием подписания электронного документа.

PKI-сервисы. Подпись.

- Подписать документ можно двумя способами:
- 1) с использованием установленного на компьютере пользователя ПО «DigiDoc Client» - пользовательское программное обеспечение, позволяющее дигитально подписывать документы, проверять подлинность дигитальных подписей, открывать/сохранять файлы в формате Digidoc, шифровать и дешифровать данные. Для личного пользования можно создать до 10 подписей в месяц. При большем количестве или для использования в коммерческих целях – взимается небольшая плата около **€0,10**.
- 2) с использованием портального сервиса DigiDoc – с любого компьютера, подключенного к Итернету, для входа на этот портал необходимо авторизоваться по ID-card или Mobil-ID. Функциональность такая же, но без шифрования плюс хранение документов и разграничение доступа для ознакомления на основании личных сертификатов. Плата за пользования – аналогично «DigiDoc Client».
- Для подписи по обоим вариантам можно использовать как ID-card, так и Mobil-ID. Один документ может содержать несколько подписей, проставленных разными способами.
- Подписание документа происходит бесплатно.

International association
e-Signature Without Borders

PKI-сервисы. Подпись.

- Перед подписанием документа в открывающемся окне подписант **самостоятельно** определяет свою роль (необязательное поле!) и только потом документ подписывается. Проверить правомерность определенной подписантом роли можно **бесплатно** через соответствующие регистры (например, Коммерческий). В случае недостоверности указанной роли всю ответственность за это несет подписант. При подписании документа обоими упомянутыми средствами (внутреннее ПО DigiDoc Client и портал DigiDoc) формируется контейнер по типу PKCS#7 (в новой версии PKCS#11) и создается файл с расширением «*.ddoc» (в новой версии «*bdoc»). Контейнер можно пересылать любым способом. А в портальном сервисе DigiDoc документ можно оставлять на портале с указанием личного кода тех, кто может ознакомиться с документом и подписью.
- На базе системы DigiDoc можно интегрировать поддержку электронной подписи практически в любую информационную систему или программное приложение. Именно на этой системе и построены все сервисы электронных услуг и электронного взаимодействия в Эстонии.

PKI-сервисы.
Электронная печать.

- С конца 2009 года в «Закон об ЭЦП» внесены изменения, легализующие цифровую печать. Цифровая печать, по сути, является подписью **юридического** лица, которой оно может удостоверять роль **физического** лица, выступающего от имени юридического. Это исключает необходимость каждый раз проверять через регистры правомочность подписанта при определении им своей роли, а так же снимает проблему «ВрИО» и «ВрИД» (когда одно лицо в фирме или госструктуре на основании внутреннего приказа временно замещает другое), т.к. на подпись подписанта накладывается цифровая печать, а, следовательно, ответственность за достоверность указанной роли несет юридическое лицо, чья электронная печать использовалась. Так же цифровая печать может использоваться и без подписи физического лица (например, банки или регистры).
- Сертификат ключа цифровой печати действителен **один год**. Стоимость сертификата (на токине) – около **125 EUR**. Не смотря на новизну этой услуги за 2011 и 2012 год выдано более 2000 «электронных» печатей.

International association

e-Signature Without Borders

- По состоянию на 18 сентября 2011 года в Эстонии с населением 1.350.000 человек действуют 1.163.917 активных карт, создано 62.459.055 электронных подписей, произведено 105.258.898 электронных идентификаций личности.
- Количество активных пользователей электронными услугами на март месяц достигло 500 тысяч – то есть половина дееспособного населения страны.

Индикаторы информационного общества–он-лайн начало 2012 г.:

- - **94% - школьников пользуется системой е-Школа**. Эта система является частной разработкой, оплачена государством. 75% школ покрыта этой системой. Обеспечивает контроль посещаемости, успеваемости, замечаний, планирования занятий, и т.п. Является основным инструментов в планировании и осуществленнии образовательной деятельности. За 4 года обеспечило 100% компьютерную грамотность учителей.
- **- 99% - банковских платежей**. Хотя все банки Эстонии принадлежат скандинавам, но эстонская система более продвинута чем у «родителей». Внутренний платеж, совершенный через Интернет стоит **€**0,16..0,38. Платеж, оформленный в бумажном виде в банке стоит **€2,00.**
- **- 94% - налоговых деклараций.** Система автоматизирована и для заполнения декларации необязательно иметь уровень бухгалтера. Возврат налогов происходит в течение недели.
- **- 24% - голосов на выборах.** Выборы происходят через Интернет. Была успешно использована в пяти выборах в местное самоуправление и парламент. Присутствующие наблюдатели никаких претензий и нарушений не выявили. Доступна для граждан и неграждан. В настоящее время клонирована в Швейцарии.
- - **40% - истории болезни через Интернет.** Обеспечивает доступность информации о пациенте для любого врача, независимо от статуса лечебного учреждения (государственное или частное). При обращении к данным, хранящимся в другом лечебном учреждении, при авторизации врача требует санкционирование пациента.
- **- 85% - рецептов оформляется в электронном виде и доступны в 100% аптек.** Исключает злоупотребления лекарствами и полную прозрачность. NB! В первый период использования был сбой – люди кинулись покупать лекарства одновременно, после зарплаты. И система слегка «захлебнулась». Проблема устранена.
- **- 97% - госуслуг для граждан**. Большинство услуг – замкнутого цикла, когда решение принимается системой **немедленно**, путем сопоставления заявляемых требований с правообладанием. Например – ходатайство о повышении пенсии, получении родительского пособия, заказ новых документов.
- **- 99% - услуг для бизнеса.**

Мировые рекорды

- Интернет-голосание – 24,3%
- Перепись населения – 66%
- Основание фирмы – 18 минут. Доступна для Бельгии, Финляндии, Литвы и Португалии.

International association
eSWB
e-Signature Without Borders

ФИНАНСЫ.

- Расходы в госсекторе намного ниже любой страны.
- Регистры и БД подсоединяются в общую систему легко, и практически не зависят от платформы внутренней информационной системы. Дополнительные требования для работы в X-ROAD минимальные, фактически сводятся к установке сервера, выполняющего функнции выходного шлюза и безопасности.
- Все системы самостоятельны, но они дублируются на Госпортале – в «едином окне».
- В Эстонии – на ИТ тратится 1% от госбюджета в течение 10 лет. Все средства осваивались на основе тендеров.

International association

e-Signature Without Borders

БЛАГОДАРЮ ЗА ВНИМАНИЕ !!!

Международная Ассоциация

«e-Signature Without Borders»

Николай Ермаков, член правления

www.e-swb.com nick@e-swb.com