International association

e-Signature Without Borders

The EuropeanID Interoperability Concepts and Compliance Conference

«Cross-border service provision supporting national eIDs»

27-29/03/2012

Biel, Switzerland

The authenticity in electronic interaction “Without Borders".

Problems and solutions.

As it works.

International association

e-Signature Without Borders

Безусловно, развивая в рамках одной страны какую-то технологическую тему, которая в перспективе может стать объектом международного взаимодействия, было бы разумным сначала разработать единые международные стандарты, и уже после этого строить локальную систему.

Однако, история показывает, что как правило, происходит наоборот: сначала создаются локальные системы, а потом начинаются попытки их сопряжения с другими аналогичными локальными системами.

Классическими иллюстрациями такого положения являются существующие ныне :

- лево- и правосторонее движение;
- железнодорожная колея 1520 (Россия), 1435 мм (Европа), 1668 мм (Португалия и Испания);
- 220 и 110 вольт в бытовой электросети;
- PAL, SECAM и NTFS системы цветного изображения в ТВ;

И так далее…

International association
e-Signature Without Borders

Тема PKI и аутентичности в электронном взаимодействии также не является исключением из исторической закономерности возникновения разногласий и различий.

Достаточно обратиться к поверхностному сравнению условий признания иностранных сертификатов и ЭЦП, определенных в локальных законодательствах. И это при том, что существуют международные стандарты и рекомендации, которые, по идее, должны были бы быть учтены при разработке локальных правовых актов.

Особо следует обратить внимание на существенные различия даже внутри групп юрисдикций (ЕС, СНГ, ЕврАзЕС, ШОС, ТС), внутри которых существуют свои согласованные и утвержденные рекомендации.

ECE/TRADE/C/CEFACT/2010/14
Рекомендация № 37: Рекомендация в отношении функциональной совместимости подписанных цифровых документов:

«В результате проверки подписанного цифрового документа проверяющая сторона должна, как минимум, получить четкое представление о:

- ***параметрах подписей (дате, месте, виде обязательства);***
- ***целостности подписанного контента;***
- ***целостности и действительности сертификатов подписантов;***
- ***надежности провайдеров сертификационных услуг.»***

Беларусь

Статья 30.

- **Признание иностранного сертификата открытого ключа**

Иностранный сертификат открытого ключа, соответствующий требованиям законодательства иностранного государства, в котором этот сертификат издан, признается на территории Республики Беларусь в случаях и порядке, определенных международным договором Республики Беларусь, предусматривающим взаимное признание сертификатов открытых ключей или другой способ придания юридической силы иностранным электронным документам.

Сертификат открытого ключа, изданный поставщиком услуг иностранного государства, аккредитованным в Государственной системе управления открытыми ключами, признается на территории Республики Беларусь.

Узбекистан

Статья 19.

Использование сертификатов ключей электронных цифровых подписей иностранных государств

Использование сертификатов ключей электронных цифровых подписей иностранных государств осуществляется в порядке, установленном законодательством.

Украина

Статья 17.

Признание иностранных сертификатов ключей

Иностранные сертификаты ключей, удостоверенные в соответствии с законодательством тех государств, где они выданы, признаются в Украине действующими в порядке, установленном законом.

Россия (2011 г.)

Статья 7.

Признание электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами.

Электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют на основании настоящего Федерального закона.

Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права.

Казахстан

Статья 13.
Признание иностранной электронной цифровой подписи

Иностранная электронная цифровая подпись, имеющая иностранное регистрационное свидетельство, признается электронной цифровой подписью на территории Республики Казахстан в соответствии с ратифицированными Республикой Казахстан международными договорами или после внесения в регистр регистрационных свидетельств

Эстония

Статья 40.

Признание иностранных сертификатов

Сертификаты, выданные иностранными учреждениями и лицами, оказывающими услуги по сертификации, признаются наравне с сертификатами, выданными действующими на основании настоящего Закона учреждениями и лицами, оказывающими услуги по сертификации, в случае выполнения как минимум одного из следующих условий:

1) иностранное учреждение или лицо, оказывающее услуги по сертификации, соответствует согласно решению ответственного обработчика регистра требованиям, установленным настоящим Законом и изданными на его основании правовыми актами;

2) гарантии в отношении сертификатов, выданных иностранным учреждением или лицом, оказывающим услуги, предоставляются одним из действующих на основании настоящего Закона учреждений или лиц, оказывающих услуги по сертификации, принявшим на себя ответственность за достоверность данных, содержащихся в сертификатах;

3) сертификаты, выданные иностранным учреждением или лицом, оказывающим услуги по сертификации, признаются на основании международного договора Эстонской Республики.

Германия

Параграф 15.
Сертификаты, выданные другими государствами.

(1) *Цифровые подписи, подлинность которых можно проверить (подтвердить) сертификатом открытого ключа подписи в другом государстве-члене ЕС или другом государстве-члене Соглашения об ЕЭЗ, должны считаться эквивалентным цифровым подписям, определяемых в данном Акте, так как они предоставляют такой же уровень безопасности.*

(2) *Пункт (1) выше также должен применяться к другим государствам, если были заключены соответствующие межгосударственные или внутригосударственные соглашения.*

International association
e-Signature Without Borders

Более подробно с различием в условиях признания иностранной ЭЦП и сертификатов ключа подписи в различных юрисдикциях можно ознакомиться в нашей подборке, опубликованной по адресу:

http://www.e-swb.com/?o=docs&id=551&mod=full&mid=2

Особо необходимо отметить существенные различия в условиях даже внутри одной группы юрисдикций (ЕС, СНГ, ЕврАзЭС, ШОС).

Если провести даже поверхностный анализ условий признания иностранных ЭЦП в различных юрисдикциях, то можно выделить следующие основные условия:

1. *Аккредитация иностранных УЦ в своей юрисдикции (обязательная или добровольная).*
2. *Соответствие иностранного УЦ или сертификата внутренним требованиям. (зачастую не указано кто определяет соответствие?).*
3. *Наличие соответствующих межгосударственных соглашений или нахождение в определенной юрисдикции (например, в ЕС).*
4. *Поручительство резидентного УЦ за валидность иностранной ЭЦП.*
5. *Безоговорочное признание.*

Указанные условия в различных сочетаниях могут использоваться как И, так и ИЛИ.

Не надо так же не замечать и абстрактные условия – «в соответствии с действующим законодательством»….

Основы проблем трансграничного взаимодействия

Возможность трансграничного использования ЭЦП сильно ограничивается следующими факторами:

- Различиями в терминологиях и определениях. Неполнота правовой базы.
- Локальные нормативные базы содержат требования, не соответствующие иностранным решениям.
- Возможность многозначного толкования европейской нормативной базы, например, различие в концепциях квалифицированных сертификатов и в особенности может ли квалифицированный сертификат быть выдан юридическому лицу; надзора за УЦ («соответствующий!»), что на практике подразумевает от простого уведомления до проведения детальных процедур сверки и оценки); понятие устройства создания безопасных подписей (SSCD).
- Отсутствие в нормативной базе явного предпочтения квалифицированной ЭЦП. При этом, если требования к Кв-ЭЦП хоть как-то определены (выпускаются сертифицированными УЦ; удовлетворяют общим требованиями; соответствие отслеживается госорганами), то к другим видам подписи эти требования весьма расплывчаты, а следовательно проблема их совместимости обостряется уже на внутригосударственном уровне, не говоря уже об уровне ЕС.
- Очевидно, что в отношении совместимости подписей, не основанных на квалифицированных сертификатах, невозможно рассчитывать на какой-то прогресс, так как не было определено никаких основных критериев определения надежности подобных решений. Препятствие работе над этими решениями на европейском или ином трансграничном уровне делает маловероятным возможность существования более или менее приемлемой совместимости между ними.

- Недостаточно определены на уровне ЕС требования к услугам Третьей Доверенной Стороны (штамп времени, долгосрочная архивация, идентификация и авторизация). Все это развивается исключительно в рамках национальных законодательств, а следовательно изначально закладывается проблема совместимости при попытке использования этих услуг в трансграничном режиме.
- Широкое распространение решений, не основанных на PKI.
- Неоднообразное использование атрибутов сертификатов: нет общепринятого стандарта для атрибутов, который можно было бы использовать для определения роли подписанта, а так же единого мнения по поводу значений, которые атрибут может содержать, в том числе и языковые различия (например, lawyer, advocaat, Rechtsanwalt).
- Большинство из перечисленных выше приложений может использовать КквЭЦП, выпущенные на сертификатах ограниченного круга УЦ, определенного доверительным списком.
- Использование в упомянутых приложениях различных видов подписей: PKCS#7, XMLDSig, XAdES, CAdES и т.д.. , а так же алгоритмов. Например, в Германии с 1 января 2010 года использование SHA-1 для функции хэширования в квалифицированного сертификате – недопустимо. Но это только в Германии, а в других странах этот алгоритм вполне приемлем.
- Практически все упомянуты приложения предполагают проверку валидности ЭЦП через тот УЦ, который выдал сертификат ключа подписи, и который находится в одной юрисдикции с владельцем приложения.

- **<u>Юридическая сторона так же не является беспроблемной.</u>**
- Например, понятие «защищенной ЭЦП» не имеет одинакового толкования, т.к. не определено на уровне ЕС. Например, в Австрии зЭЦП относится к классу квалифицированной, а в Польше и Литве – к расширенной. Совершенно ясно, что такое различие толкований создает риски возникновения беспорядка на общеевропейском уровне. Многие термины и понятия являются уникальными для каждой страны.
- Всего в 13 странах имеются специальные акты «е-правительства» (в мае 2011 Греция приняла закон об Электронном Правительстве). . В них так же имеются серьезные различия. Но объединяет их одно: возможность гражданам и предприятиям общаться в органами государственной власти в электронном виде, а так же обратную возможность – взаимодействия органов государственной власти между собой и с гражданами. При этом, существуют разные правила взаимодействия – от не делающих никаких различий в использовании ЭЦП (Эстония), до сугубо специальных правил (13 стран).
- По разному решен и вопрос стимуляции использования ЭЦП во взаимодействии лиц и государства. Только немногие из этих актов учитывают проблемы возможности использования национальных ЭЦП в трансграничном режиме даже внутри ЕС.

Анализ имеющейся практики использования ЭЦП и СПК

- Разнообразность практики использования ЭЦП в ЕЭС начинается **с носителей сертификатов ключей подписи.**
- **По имеющимся данным:**
- 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 планирует выпуск ID-карт на начало-середину 2012 года, Грузия начала выпуск ID-карт с 1 августа 2011, Азербайджан планирует введение ID-карт (сроки не известны), Украина заявляет о технической готовности для внедрения ID-карт (сроки не известны). Россия отложила внедрение Универсальных Электронных Карт (УЭК) до 2013 года.

- Сектор специфических смарт-карт (используемых 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. Частная компания Болгарии 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. Латвия представила мобильные подписи в 2010 году.

- **Основные сферы использования** в сфере взаимодействия с государством посредством ЭЦП в ЕС сводятся к госзакупкам, здравоохранению, юстиции, налоговой отчетности, социальному обеспечению, торговле.
- **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, во Франции 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 ЭЦП 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.

- **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: 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 ЭЦП 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.

International association
e-Signature Without Borders

- **<u>Система права.</u>** 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 подписи, то 4 основаны на квалифицированных ЭЦП (Австрия, Германия, Польша, Эстония), и по одному – на расширенной, основанной на квалифицированных сертификатах (Словения), расширенной (Португалия) и простой (Ирландия).
- Возможность трансграничного использования ЭЦП реализована только в Эстонии, и в отношении узкого круга стран и между 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.

- 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

Как видно из всего вышесказанного, на сегодняшний день практическое применение ЭЦП и сертификатов для трансграничного электронного взаимодействия в условиях такого технологического и правового «хаоса» -

невозможно!!!

И пока чиновники пытаются договориться, бизнес несет потери.

В первую очередь это касается таких направлений как внешнеэкономическая деятельность и электронная торговля, в том числе и по программе государственных закупок PEPPOL (в Европе) и 94-ФЗ (в России).

Потенциальные пути решения

Есть разные пути устранения таких противоречий.

1. **Обеспечения единообразия для всех существующих PKI-систем и правовой базы, на которых они базируются.**

Но эти системы уже созданы! И что? Тем кто не впишется во вновь созданные единые правила надо будет отказаться от всего, что создано?

Аналогия:

насколько перспективны попытки договориться о замене всех бытовых электросетей в Европе на 110 вольт, или в Америке и Японии – на 220. Или введении везде 185 вольт ?

International association
eSWB
e-Signature Without Borders

Но есть и другой путь!

И именно этим путем решены многие, имеющиеся на сегодня технические противоречия.

Надо оставить каждому свое, пусть будут и 110, и 220 вольт, и 50 и 60 Гц.

Нужно просто создать

А Д А П Т Е Р Ы!!

И именно для решения PKI-проблемы «адаптерными методами» в мае 2008 года была учреждена

Международная Ассоциация «e-Signature Without Borders»

www.e-swb.com

International association
e-Signature Without Borders

К настоящему моменту нами создана методика, технология и опытные образцы компонентов системы универсального обеспечения проверки валидности ЭЦП и СКП, независимо от используемых технологий, стандартов и алгоритмов, а так же юрисдикций автора и получателя электронного документа – **PKI-АДАПТЕР.**

International association
eSWB
e-Signature Without Borders

БАЗОВЫЕ ПРИНЦИПЫ НАШЕГО ПОДХОДА К РЕШЕНИЮ ПРОБЛЕМЫ

Одним из вариантов решения проблем PKI-трансграничности, широко обсуждаемыми чиновниками от PKI, является создание

«Пространства Доверия».

Но, на наш взгляд - «Доверие» понятие абстрактное.

Для возникновения доверия можно выдвинуть самые разные условия, в доверии можно отказать в любой момент.

Поэтому мы считаем, что было бы логичнее говорить о создании

ПРОСТРАНСТВА ОТВЕТСТВЕННОСТИ !!

А во-вторых, мы считаем, что при использовании PKI-технологий в трансграничном режиме необходимо исходить из того, что помимо обеспечения однозначной и надежной идентификации личности, проверки валидности его сертификата, целостности и неизменности полученного документа, конечной целью должно быть обеспечение

НЕОТКАЗУЕМОСТИ !

Пространство ответственности

Формируется за счет:

A) соответствующих правовых отношений, прав и обязанностей участников процесса проверки (устав Ассоциации, договора и соглашения);

B) использования в процессе проверки сертификатов и средств подписи, которым участники проверки однозначно доверяют (полученных от заинтересованного участника проверки).

C) Ассоциация e-SWB выступает гарантом легитимности и достоверности проверки. Гарантия обеспечивается страхованием собственной ответственности Ассоциации и ее членов, участвующих в каждой отдельно взятой проверке.

Обеспечение неотказуемости

В случае попытки подписанта отказаться от действия, совершенного на основании сертификата, (в том числе и от ЭЦП), и доведения спора до суда, исходя из существующей судебной практики, в суд целесообразней представлять не заключения экспертов, а показания свидетелей, в качестве которых выступают участники проверки. И каждое свидетельство подтверждается документально – в виде запросов и квитанций, заверенных ЭЦП, легитимной в своей юрисдикции.

В этом случае, исходя из того что каждый этап проверки был легитимным в своей юрисдикции, то и вся проверка может считаться легитимным.

Более подробно с разработанной нами
«Методикой обеспечения аутентичности в трансграничном взаимодействии»
можно ознакомиться по адресу:
http://e-swb.com/methodics.pdf

ХЕШ и Конфиденциальность

При проверке ЭЦП мы принципиально не работаем с подписанным документом, а осуществляем проверку только в отношении хеш-функции от документа, которая и представляется проверяющей стороной для проверки.

Тем самым обеспечивается защита личных данных и конфиденциальность информации.

В случае действительности ЭЦП в отношении представленного хеша, окончательное решение о приемлемости вывода о действительности ЭЦП в отношении всего документа принимает проверяющая сторона, исходя из того насколько она доверяет используемому алгоритму хеширования.

Как это работает

на примере Россия (НУЦ) и Эстония (SK)

1. Создание документа, подписанного на СКП SK

Клиент (EE)

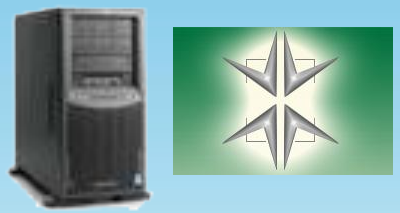
Клиент (РФ)

International association
e-Signature Without Borders

2. Документ отправляется в адрес получателя (РФ)

3. Формируется запрос на проверку подлинности документа.

4. Запрос отправляется в адрес НУЦ



Клиент
(ЕЕ)

Клиент
(РФ)

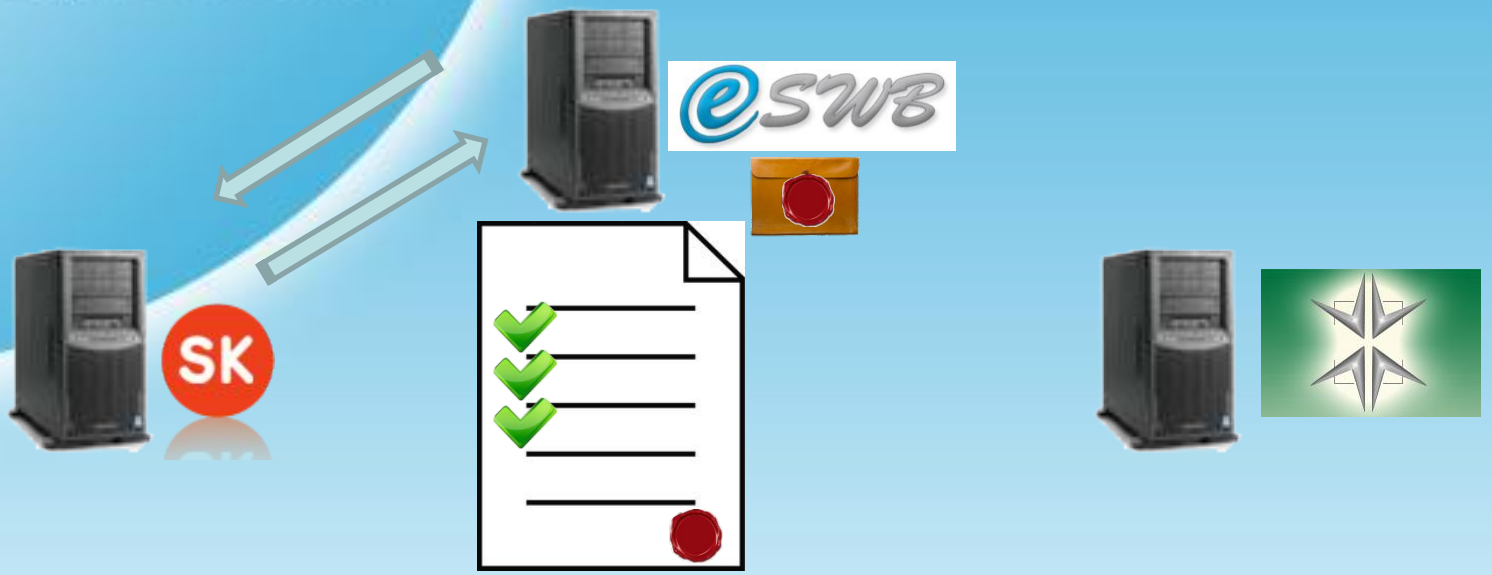
5. Запрос отправляется в адрес НУЦ

6. НУЦ формирует запрос на проверку ЭЦП в адрес e-SIGN VS.

Клиент
(ЕЕ)

Клиент
(РФ)

Проверка Запроса и формирование квитанции

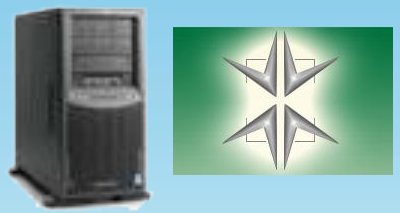


8. Проверка ЭЦП, использованной для подписи документа
9. Проверка ЭЦП, использованной для подписи Запроса

Клиент (ЕЕ)

Клиент (РФ)

10. Отправка квитанции в адрес НУЦ



Клиент (ЕЕ)

Клиент (РФ)

10. Отправка квитанции в адрес НУЦ

11. Проверка квитанции на стороне НУЦ

12. Формирование квитанции клиенту

13. Пересылка квитанции клиенту

Клиент (ЕЕ)

Клиент (РФ)

Реальные итоги

Представленная схема взаимодействия опробована на практике.

В настоящий момент при взаимодействии с членами Ассоциации, и в первую очередь Национальным Удостоверяющим Центром (НУЦ) из России и SK из Эстонии проведены успешные испытания по проверке валидности ЭЦП, выработанных на сертификатах России, Эстонии, Финляндии, Литвы, Австрии, Бельгии, Португалии в интересах субъектов взаимодействия из этих юрисдикций.

Испытания прошли успешно, что подтверждается соответствующими протоколами, опубликованными на нашем сайте по адресу :

……..

Перспективы

В стратегии своего развития мы исходим из того, что все взаимодействие при проверке должно осуществляться исключительно между Ассоциацией e-SWB и УЦ, и именно УЦ должны осуществлять взаимодействие с конечным пользователем.

Однако, не исключаем и возможности предоставления сервиса по проверки и через соответствующий собственный WEB-портал.

Кроме того, разрабатывается и другая модель обеспечение проверки валидности ЭЦП, когда подписанный документ будет попадать к конечному пользователю уже с квитанцией о проверке, заверенной ЭЦП обслуживающего его «родного» УЦ.

International association

e-Signature Without Borders

ЗАКЛЮЧЕНИЕ

По нашему мнению, при наличии благоприятных условий (доброй воли, понимания и финансирования), развитие представленной концепции обеспечения аутентичности в трансграничном электронном взаимодействии способно в самые сжатые сроки и сравнительно недорого обеспечить достижение желаемого результата – беспроблемного взаимодействия между собой в различных сочетаниях граждан, частного бизнеса и государственных организаций из различных юрисдикций.

Что, в свою очередь даст новый импульс для полноценного и эффективного развития трансграничных проектов в области электронной торговли, государственных закупок, внешнеэкономической деятельности, предварительном информировании, и таких проектов как PEPPOL, STORK, SPOCS.

БЛАГОДАРЮ ЗА ВНИМАНИЕ !!!

Международная Ассоциация
«e-Signature Without Borders»

Николай Ермаков, член правления

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