International association

e-Signature Without Borders

Конференция «Единое Окно»
7-8 апреля 2011 г.
г. Москва, Россия

Проблемы и решения в обеспечении аутентичности в трансграничном электронном документообороте

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.

International association
e-Signature Without Borders

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

International association
e-Signature Without Borders

Россия-2011

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.

- Разнообразность практики использования ЭЦП в ЕЭС начинается **с носителей сертификатов ключей подписи.**
- В первом полугодии ID-карты были доступны только в 10 странах (Бельгия, Финляндия, Италия, Лихтенштейн, Литва, Португалия, Испания, Эстония, Хорватия, в конце прошлого года началось в Германии), и планируется ввести в течение 2 лет еще в 5 – Мальта, Норвегия, Польша (2011) и Румыния (2011). Одиннадцать стран вообще не планируют выпуск ID-карт.
- ID-карты выдаются государством (в 7 странах) или уполномоченными частными структурами (6 стран) и обеспечивают создание квалифицированных подписей.
- Специфические смарт-карты (используемые для ограниченного круга пользования или в специфической области применения) имеются в 9 странах (банковские, карты социального обеспечения, здравоохранения, а так же карты госслужащих).
- 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 6 странах (Финляндия, Литва, Норвегия, Польша, Эстония).

- **Юридическая сторона так же не является беспроблемной.**
- 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 12 странах имеются специальные акты «е-правительства». 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 (12 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.

- **Основные сферы использования** в сфере взаимодействия с государством посредством ЭЦП в ЕС сводятся к госзакупкам, здравоохранению, юстиции, налоговой отчетности, социальному обеспечению, торговле.
- **Госзакупки.** Реально работают только 15 приложений. Из них на квалифицированных сертификатах основаны 6, на расширенных на базе квалифицированных – 2, на расширенных – 6, и только 1 – на простой подписи.
- Из этих 15 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, а в Дании и Словакии используются сертификаты расширенной подписи, высылаемые по э-майлу.
- В еще двух странах (Австрия и Норвегия) допустимо использование ЭЦП из узкого круга стран.
- В остальных 10 случаях этими приложениями могут пользоваться только свои резиденты.
- **Здравоохранение**. Всего 8 реально работающих приложений и 2 в пилотной и проектной стадии. Из них 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 полностью отсутствует. Но, справедливости ради, надо отметить, что и потребность в этом – так же невелика, т.к. взаимодействие осуществляется, как правило, в пределах одной страны.

- **<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), 3 – связаны с регистрацией компаний (Хорватия, Германия, Эстония), 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.

International association

e-Signature Without Borders

- 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). Причем, география возможности проверки валидности ЭЦП весьма узка. Существенную проблему создает и использование несовместимых идентификаторов (например, регистрационного номера) 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).

Возможность трансграничного использования ЭЦП сильно ограничивается следующими факторами:

- Различиями в терминологиях и определениях. Неполнота правовой базы.
- Нормативная база содержит 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 кЭЦП, 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.

Как видно из всего вышесказанного, решить проблему практического применения ЭЦП для трансграничного ЭДО обычными методами в условиях такого технологического и правового «хаоса» - невозможно.

И именно для решения этой проблемы нестандарными методами в мае 2008 года была создана

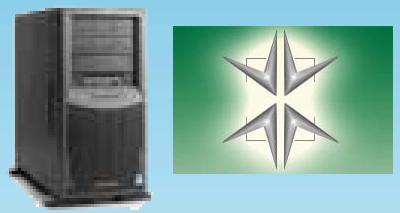
Международная Ассоциация

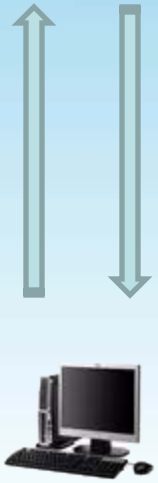
«e-Signature Without Borders»

www.e-swb.com

К настоящему моменту нами создана технология универсального обеспечения проверки валидности ЭЦП, независимо от используемых технологий, стандартов и алгоритмов, а так же юрисдикций автора и получателя электронного документа.

1. Создание документа, подписанного на СКП SK





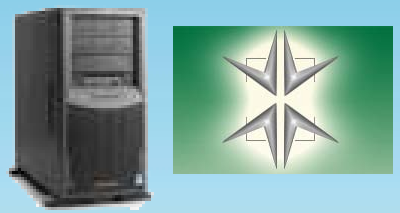
Клиент (ЕЕ)

Клиент (РФ)

2. Документ отправляется в адрес получателя (РФ)

3. Формируется запрос на проверку подлинности документа.

4. Запрос отправляется в адрес НУЦ



Клиент (ЕЕ)

Клиент (РФ)

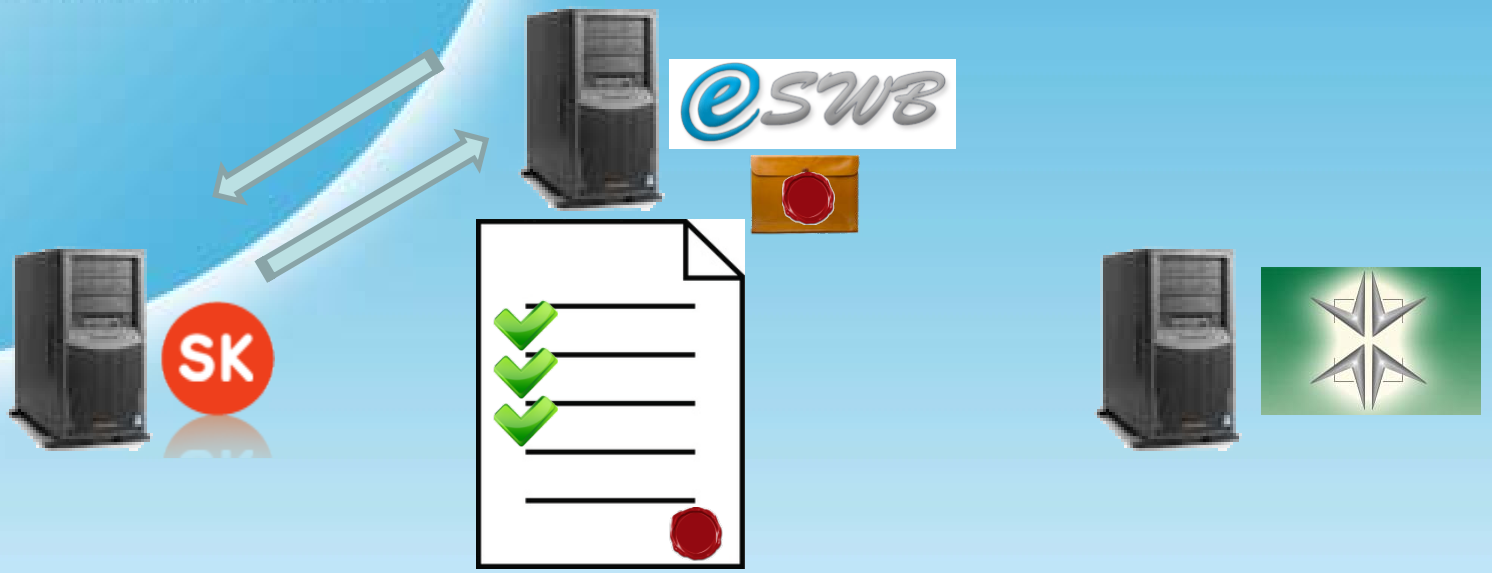
4. Запрос отправляется в адрес НУЦ

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

Клиент (ЕЕ)

Клиент (РФ)

Проверка Запроса и формирование квитанции

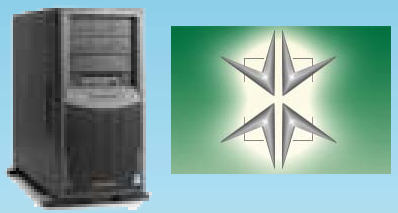


8. Проверка ЭЦП, использованной для подписи Запроса

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)

International association

e-Signature Without Borders

БЛАГОДАРЮ ЗА ВНИМАНИЕ !!!

ГОТОВ ОТВЕТИТЬ НА ВОПРОСЫ.

Международная Ассоциация
«e-Signature Without Borders»

Н.Е. Ермаков, вице-президент

www.e-swb.com

nick@e-swb.com