СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ, ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ И АУТЕНТИФИКАЦИИ В ИХ ВЗАИМОСВЯЗИ

КОМИСАРЕНКО В.В.
ЗАМЕСТИТЕЛЬ ГЕНЕРАЛЬНОГО ДИРЕКТОРА
ЗАО «БЕЛТИМ СБ»

1.Развитие сервисов инфраструктуры открытых ключей

1.1 Тренды 2012-2013

1.2 Новые компоненты

1.3 Оценка безопасности

1.4 Качество предлагаемых продуктов

1.Развитие сервисов инфраструктуры открытых ключей.

1.1 Тренды 2012 – 2013:

- Выход на активные продажи услуг УЦ
- Статус тренда «множественность алгоритмов ЭЦП» не изменился
- Новые разработчики не появляются

1.Развитие сервисов инфраструктуры открытых ключей

1.2.Новые компоненты:

- сервисы валидации по OCSP протоколу (validation)
- сервисы, связанные с восстановлением ключей шифрования (key recovery)
- сервисы управления работой с клиентами (CRM)

1.Развитие сервисов инфраструктуры открытых ключей

1.3.Оценка безопасности:

- Зарубежная практика: оценка защищенности решений по Common Criteria (EAL 4)
- Россия, Беларусь, Украина: оценка защищенности на соответствие специфическим национальным требованиям

1.Развитие сервисов инфраструктуры открытых ключей

1.3.Оценка безопасности. Республика Беларусь:

ПОЛОЖЕНИЕ о порядке криптографической защиты информации № 62 от **30.08.2013** :

Системы защиты информации информационных систем, системы безопасности КВОИ и системы электронных документов ГИС должны включать в себя СКЗИ … , а также комплекс средств обеспечения безопасности СКЗИ.

Программные СКЗИ и программное обеспечение аппаратных СКЗИ должны соответствовать требованиям, установленным СТБ 34.101.27-2011 "Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации",

а программно-аппаратные и технические СКЗИ – требованиям, установленным СТБ П 34.101.43-2009 "Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации".

2.Электронная подпись в «облаках»

Взаимодействие напрямую

2.Электронная подпись в «облаках»

Взаимодействие через «облако»

2.Электронная подпись в «облаках»

Ключи и средства подписи в «облаке»

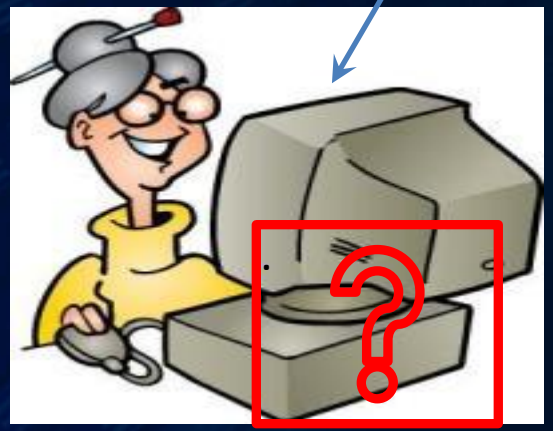
2.Электронная подпись в «облаках»

Требования законодательства (на примере России и Беларуси)

1.При использовании усиленных электронных подписей участники электронного взаимодействия обязаны обеспечивать конфиденциальность ключей электронных подписей, в частности, не допускать использование принадлежащих им ключей электронных подписей без их согласия.

2.Владелец личного ключа обязан хранить в тайне личный ключ.

2.Электронная подпись в «облаках»



1.Безопасность среды

2.Электронная подпись в «облаках»

2.Сильная аутентификация

2.Электронная подпись в «облаках»

3.Сильная авторизация

3.Сервисы ДТС в «облаках» !

Взаимодействие через «облако»

3.Сервисы ДТС в «облаках» !

Проверка подписи в облаке

3.Сервисы ДТС в «облаках» !

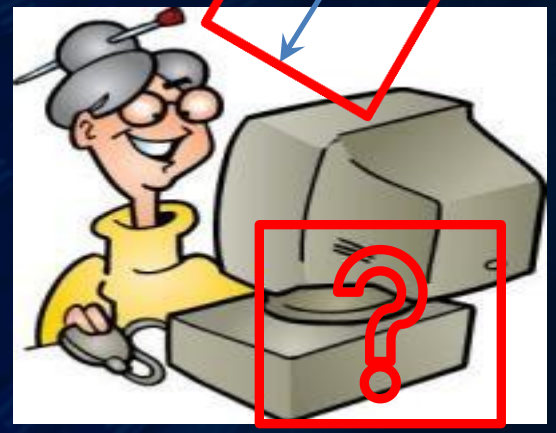
Проверка подписи в облаке

3.Сервисы ДТС в «облаках» !

Формально юридическая значимость подписи и электронного документа обеспечивается. Вопрос в безопасности технологии

3.Сервисы ДТС в «облаках» !

Формально юридическая значимость подписи и электронного документа обеспечивается. Вопрос в безопасности технологии



4. Единые серверы идентификации и аутентификации (Single sign-on)

4.1 Необходимость поддержки различных методов аутентификации и уровней защищенности

4.2 Прикладная система взаимодействует только с сервером идентификации-аутентификации

4.3 Тренд: переход к трехфакторной аутентификации

5.Трансграничное взаимодействие с использованием юридически значимых электронной подписи и электронных документов

5.1 Работы продолжаются

5.2 Достигнуто понимание вопроса обеспечения безопасности на уровне ДТС-ДТС

5.3 Тестирование реализаций форматов и протоколов на базе программно-технических платформ России, Казахстана и Беларуси

5.Трансграничное взаимодействие с использованием юридически значимых электронной подписи и электронных документов. Республика Казахстан

С целью реализации требований статьи 10 «Соглашения о применении информационных технологий при обмене электронными документами во внешней и взаимной торговле на единой таможенной территории Таможенного союза», утвержденного Правительствами государств от 21 сентября 2010 года, в Республике Казахстан создана Доверенная третья сторона и принято постановление Правительства Республики Казахстан от 12 марта 2013 года № 227 «Об утверждении Правил подтверждения подлинности иностранной электронной цифровой подписи доверенной третьей стороной Республики Казахстан»

5.Трансграничное взаимодействие с использованием юридически значимых электронной подписи и электронных документов. Республика Казахстан

7. ДТС РК на основе полученных запросов осуществляет их проверку, при этом перенаправляет запросы в соответствующий ДТС иностранного государства, в котором было выпущено проверяемое регистрационное свидетельство.

8. На основании полученного ответа от ДТС иностранного государства ДТС РК формирует ответ в виде квитанции DVC, являющиеся необходимой и достаточной для подтверждения подлинности иностранной ЭЦП на территории Республики Казахстан.

9. Подтверждение подлинности иностранной ЭЦП ДТС РК осуществляется в круглосуточном онлайн-режиме на бесплатной основе через интернет-ресурс.

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ТЕХНОЛОГИЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ, ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ И АУТЕНТИФИКАЦИИ В ИХ ВЗАИМОСВЯЗИ

КОМИСАРЕНКО В.В.
ЗАМЕСТИТЕЛЬ ГЕНЕРАЛЬНОГО ДИРЕКТОРА
ЗАО «БЕЛТИМ СБ»