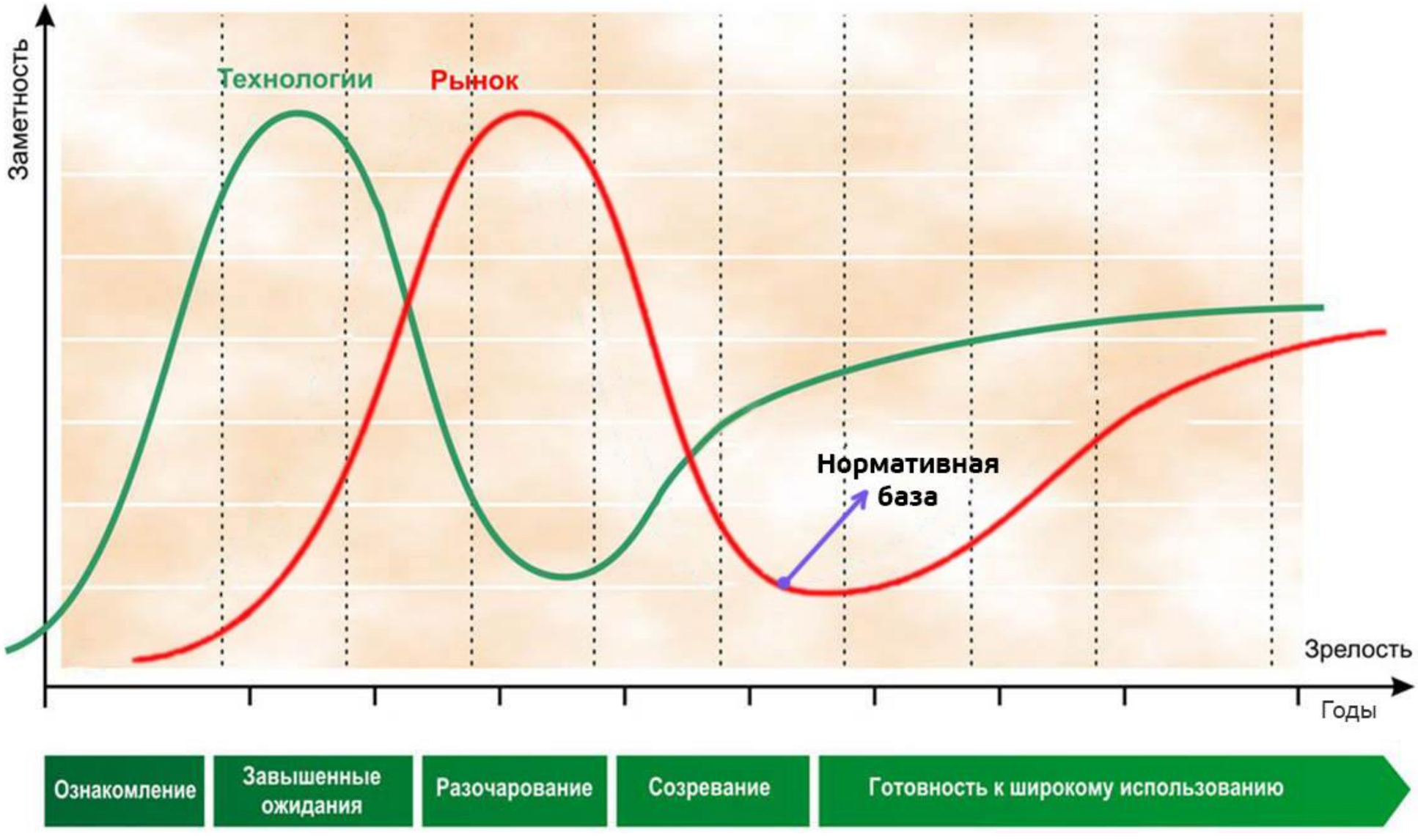
Доверие к инфраструктуре открытых ключей и решениям на ее основе

PKI-форум 15-17 сентября 2015 г.

Алексей Сабанов, к.т.н.,

Доцент МГТУ им.Н.Э.Баумана

Роль нормативно-правовой базы



Доверенные ИС – необходимость 2015

Доверенная информационная система

	доверие к разработке	доверие к интеграции	доверие к функционированию	уровень строгости требований
доверие к ИС	требуется	необходимо	необходимо	высокий
доверие к бизнес-процессам ИС	требуется	необходимо	необходимо	высокий
доверие к продукту	требуется	возможно	требуется	высокий
доверие к процессу	требуется	требуется	требуется	средний
доверие к среде	требуется	требуется	требуется	низкий
уровень сложности	низкий	средний	высокий	низкий

ГОСТ Р 54583-2011/ISO/IEC/TR 154443-3:2007.Информационная технология. Меры и средства обеспечения безопасности.М.: Стандартинформ.2013.

Доверенная среда

- Доверенная среда как основа создания и функционирования доверенной ИС может иметь как микроскопические размеры (например, чип), так и практически неограниченное физическими размерами пространство.
- Виды доверенной среды: аппаратная, программно-аппаратная, с участием операторов (наличие человеческого фактора).
- Доверенную среду создать гораздо проще, чем доверенный продукт и уж тем более доверенные бизнес-процессы.

Доверие к продукту (сервису)

Цель обеспечения доверия - создание уверенности в надёжном функционировании продукта (сервиса) в заданных условиях.

Определяется оценкой риска и/или политикой организации, при этом пользователь должен быть уведомлён об остаточном риске.

Менеджмент риска учитывает неопределённость, которая исходит от множества факторов, таких, как недостаточное знание всех аспектов функционирования, допусков при измерениях и т.д.

При применении мер повышения уровня доверия и усиления функций применяемых средств безопасности связанная с указанными факторами неопределённость уменьшается, что сказывается на снижении величины остаточного риска.

ГОСТ Р 54583-2011/ISO/IEC/TR 154443-3:2007.Информационная технология. Меры и средства обеспечения безопасности.М.: Стандартинформ.2013.

Доверие к PKI и решениям на ее основе

- *функциональная надёжность*, т.е. степень готовности к выполнению заданных функций в определенных условиях, пригодность к восстановлению в случаях сбоев и ошибок, безотказность, степень достоверности результатов вычислений, контролируемость их получения;

- *функциональная устойчивость*, т.е. способность ИС противостоять деструктивным воздействиям];

- *информационная безопасность* ИС, т.е. выполнение условий поддержания заданного уровня конфиденциальности, доступности и целостности информации, хранимой, передаваемой, принимаемой и обрабатываемой ИС в процессе её работы.

Особеннности систем с числом пользователей порядка 10^7

- Модели угроз, нарушителя и привычные средства защиты информации нуждаются в совершенствовании;
- Начинают проявляться законы больших чисел;
- Сервисы безопасности необходимо проектировать с применением методов исследования систем массового обслуживания;
- Вероятностный характер результатов в отличие от полной определенности для локальных ИС;
- Необходимость введения уровней доверия.

Доверие к идентификации

- Основной критерий – Качество идентификации – отличие одного субъекта от другого путем сравнения предъявленных идентификаторов с занесенными в БД.
- Имеются ошибки первого (не идентифицирован) и второго рода (злоумышленник идентифицирован как легальный user).
- Требует уровней доверия к результатам сравнения в зависимости от числа идентификаторов и механизмов сравнения. Требует протоколирования результатов для разбора конфликтных ситуаций.

Доверие к аутентификации

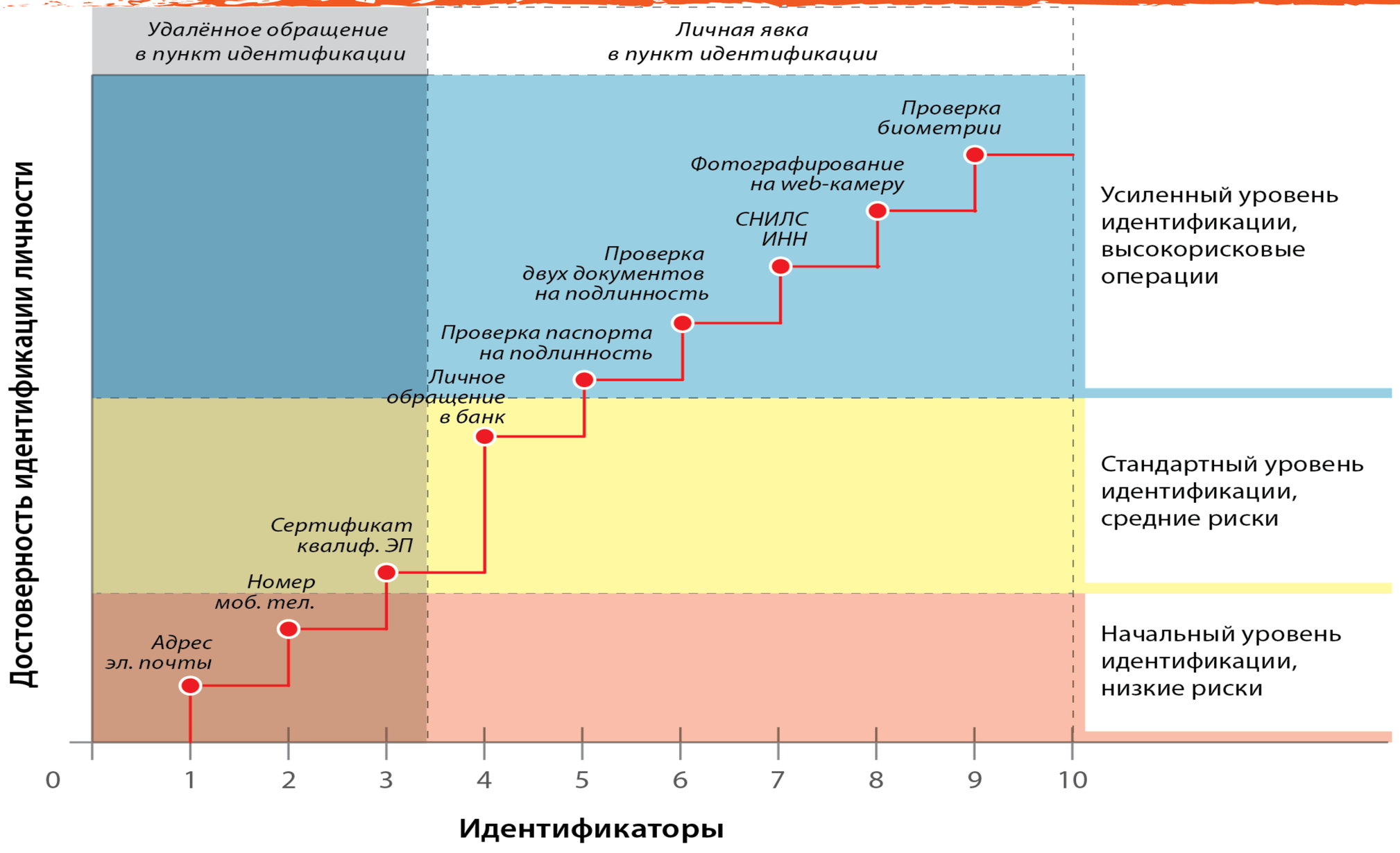
- Только аутентификация доказывает привязку идентификаторов и аутентификатора к конкретной личности. Самая безопасная и надежная аутентификация основана на сертификате доступа с механизмом аутентификации в виде квалифицированной электронной подписи.
- Основной критерий – качество (безопасность и надежность) аутентификации.
- Необходимо ввести уровни доверия к аутентификации.
- Основная нерешенная проблема – трансляция доверия.

Определение достоверности

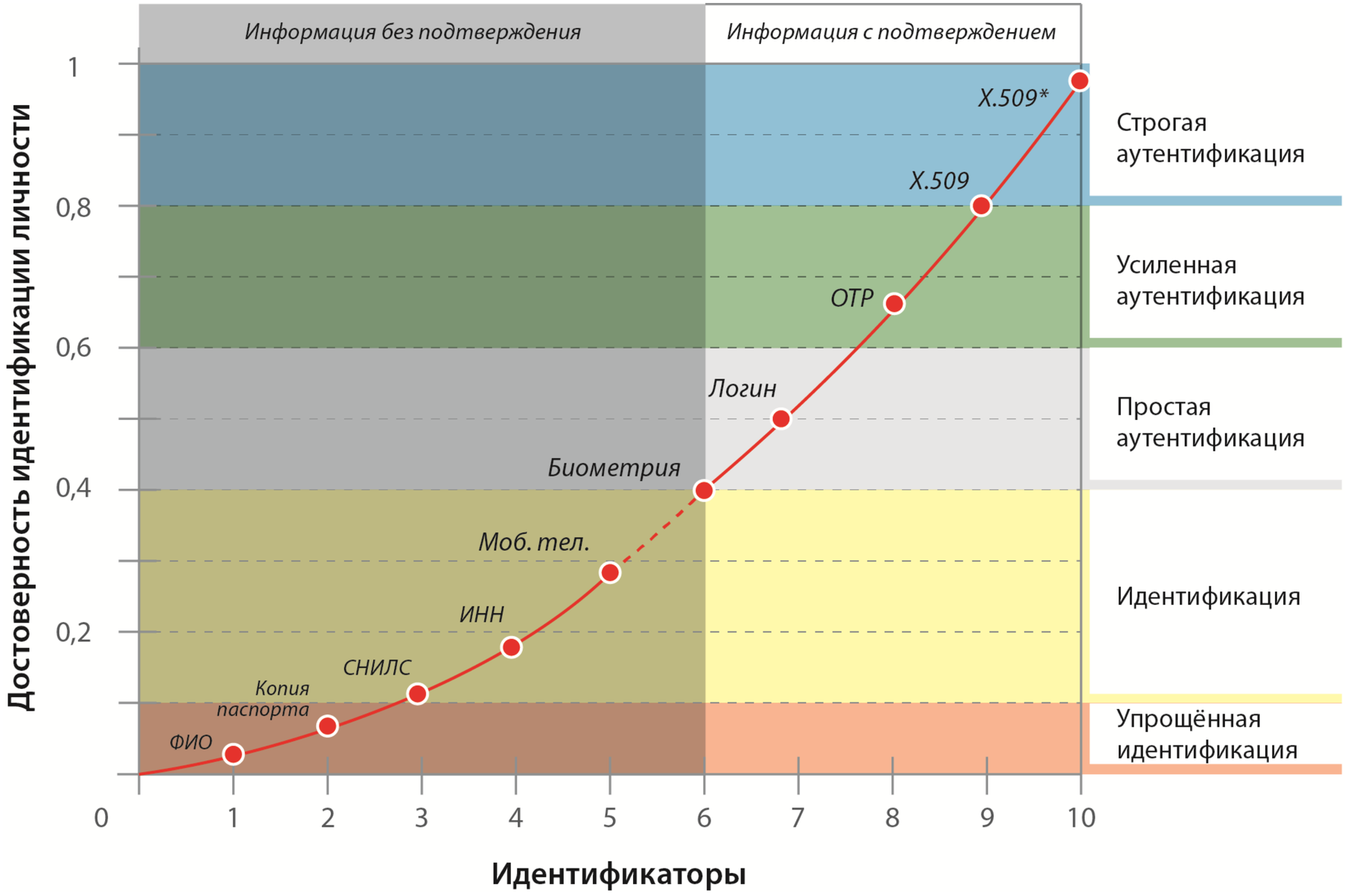
Достоверность информации - общая точность и полнота информации. Достоверность информации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Достоверность идентификации и аутентификации (ИА) определим как меру доверия к результатам идентификации и аутентификации при условии безошибочности выполнения процедур идентификации и аутентификации. Поскольку безошибочность может иметь уровни точности ее определения, также как и мера доверия к результатам ИА, то и мера доверия (то есть достоверность) может иметь уровни достоверности, называемые в западных нормативных источниках уровнями гарантий.

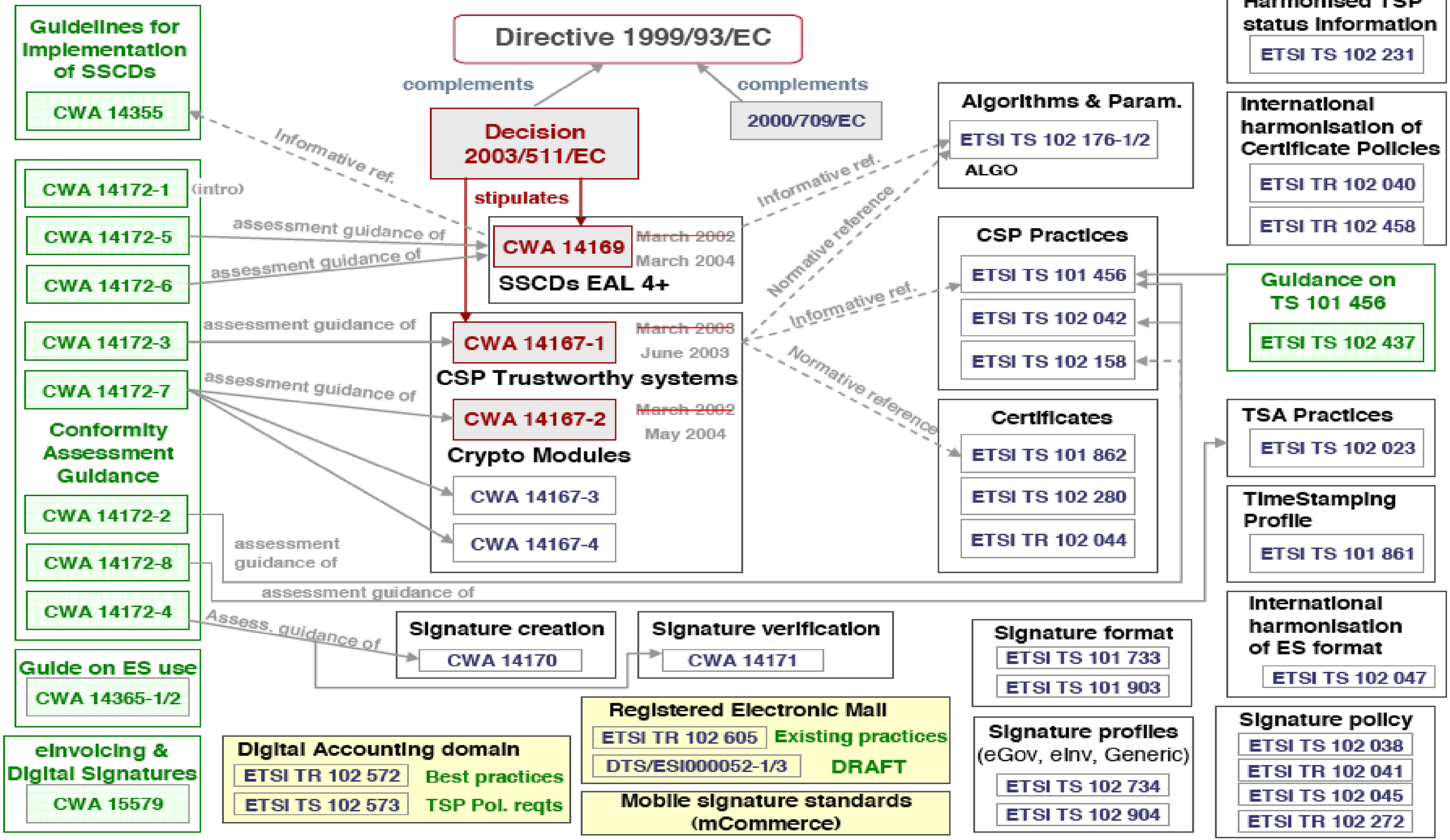
Достоверность можно накапливать



Достоверность идентификации



EU eSignature Standardisation Work overview



Краткая история

- Существенным толчком к решению задач доверия к идентификации явилось 11 сентября 2001г.
- Совет Безопасности ООН принял резолюцию 1373, направленную на усиление мер против фальсификации паспортов
- США: разработаны требования на основе работ НИСТ, стандарт FIPS PUB 201-1 - 2006, биопаспорта введены с 2004г.
- ISO/IEC 24760-1:2011, 24760-2:2015; ISO/IEC 29115: 2013
- Положение и регламент Regulation 910/2014

Норвегия

Имеется 3 системы идентификации граждан:

- Государственная Min ID (MyID - для граждан с 13 лет), использует национальный Id, возможна первичная идентификация по номеру мобильного телефона с OTP, который приходит по SMS. Доступ к онлайн-сервисам более 50 госуслуг.
- Банковская – более высокий уровень гарантий, чем Min ID. Использует набор механизмов безопасности, включая смарт-карты и ЭП на SIM. На июнь 2010г. охвачено более 2,5 млн. из 4.7 млн населения
- BuyPass. Использует смарт-карты и мобильные телефоны

Положения Regulation 910/2014

(14) В Регламенте должны быть определены некоторые условия в отношении того, какие средства электронной идентификации должны быть признаны, и как должно осуществляться уведомление об этих схемах.

(15) Обязательство признавать средства электронной идентификации относится только к тем средствам, уровень доверия установления личности который соответствует равному или более высокому, чем уровень, требуемый для доступа к услуге, о которой идет речь.

(16) Уровни доверия должны характеризовать степень уверенности в способности средств электронной идентификации устанавливать идентичность лица таким образом, чтобы обеспечить гарантию, что лицо, заявившее об определенной идентичности, действительно является тем лицом, которому данная идентичность была назначена.

Положения Regulation 910/2014

(19) Безопасность схем электронной идентификации является ключом к заслуживающему доверия трансграничному взаимному признанию электронных средств идентификации. В этом контексте страны - члены ЕС должны сотрудничать в вопросах обеспечения безопасности и совместимости схем электронной идентификации на уровне ЕС.

(20) Сотрудничество стран - членов ЕС должно служить технологической совместимости заявленных схем электронной идентификации, с тем чтобы способствовать высокому уровню доверия и обеспечению безопасности, соответствующей степени риска.

(21) Настоящий регламент должен также установить общую законодательную базу для использования доверенных электронных служб.

Положения Regulation 910/2014

(30) Страны - члены ЕС должны назначить надзорный орган или надзорные органы для осуществления надзорной деятельности в соответствии с настоящим Регламентом.

(31) Надзорные органы должны сотрудничать с органами защиты данных, например путем информирования их о результатах аудита квалифицированных поставщиков доверенных служб, в тех случаях, когда, предположительно, были нарушены правила защиты персональных данных. Предоставленная информация, в частности, должна отражать инциденты безопасности и факты нарушений безопасности персональных данных.

(37) Настоящий Регламент устанавливает ответственность для всех поставщиков доверенных служб. В частности, он устанавливает режим ответственности, в соответствии с которым все поставщики доверенных служб должны нести ответственность за ущерб, причиненный любому физическому или юридическому лицу в результате несоблюдения обязательств в соответствии с настоящим Регламентом.

Регламент 910/2014, ст.6

Когда электронная идентификация, использующая средства электронной идентификации, и аутентификации определены к использованию национальным законодательством или административной практикой для доступа к службе, обеспечиваемой в онлайн-режиме организацией государственного сектора, в одной стране – члене ЕС, средства электронной идентификации, выпущенные в другой стране – члене ЕС, должны признаваться в первой стране – члене ЕС для целей трансграничной онлайн-аутентификации в этой службе, при соблюдении следующих условий:

(a) такие средства электронной идентификации выпущены в соответствии со схемой, которая включена в список, опубликованный Комиссией в соответствии со Статьей 9;

(b) уровень гарантии этих средств электронной идентификации соответствует уровню гарантии, равному или более высокому, чем уровень гарантии, требуемый соответствующей организацией государственного сектора для онлайн-доступа к этой службе в первой стране – члене ЕС, при условии что уровень гарантии этих средств электронной идентификации соответствует существенному уровню гарантии или более высокому

(c) соответствующая организация государственного сектора использует существенный уровень гарантии или более высокий в отношении онлайн-доступа к этой службе.

Регламент 910/2014, ст.8

Уровни доверия электронных схем идентификации

1. Электронная схема идентификации, заявленная в соответствии со Статьей 9, должна указывать уровни гарантии низкий, существенный и/или высокий для электронных средств идентификации, выпущенных по этой схеме.

2. Уровни доверия– низкий, существенный и высокий – должны удовлетворять следующим критериям соответственно:

(a) низкий уровень доверия должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает ограниченную степень уверенности в заявленной или утвержденной подлинности лица и описывается ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является уменьшение риска ненадлежащего использования или изменения подлинности.

(b) существенный уровень доверия должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает существенную степень уверенности в заявленной или утвержденной подлинности лица и характеризируется ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является существенное уменьшение риска ненадлежащего использования или изменения подлинности.

(c) высокий уровень доверия должен характеризовать средства электронной идентификации в контексте схемы электронной идентификации, которая обеспечивает более высокую степень уверенности в заявленной или утвержденной подлинности лица, чем электронные средства идентификации с существенным уровнем гарантии, и характеризируется ссылкой на технические спецификации, стандарты и процедуры, к ней относящиеся, включая технические средства управления, назначением которых является предотвращение ненадлежащего использования или изменения подлинности..

Анализ изменений 1999/93 vs 910/2014

1. Требования SSCD (Security Signature Creation Device) сменились на QSCD (Qualified Signature Creation Device). Теперь все устройства генерации закрытого ключа электронной подписи должны быть в списке квалифицированных, который утверждается Комиссией ЕС
2. Однозначно прописаны уровни доверия к идентификации и аутентификации.
3. Доверенные сервисы должны поставляться и поддерживаться квалифицированными поставщиками доверенных служб (УЦ).
4. Для аутентификации Web-сайтов необходимо выпускать квалифицированный сертификат доступа, в котором идентифицируется владелец сайта. Выпускать такие сертификаты может только квалифицированный поставщик доверенных служб.

Оценка перспектив

1. Имеется два подхода к решению представленных задач по регулированию электронной идентификации: быстро и правильно
2. Правильно (на федеральном уровне) задачи будут решены не скоро. Нет стратегии построения пространства доверия к аутентификации.
3. Быстро требования к идентификации и аутентификации можно выработать на уровне предприятия.
4. На отраслевом уровне решения появятся не скоро.

Промежуточные выводы

1. Вопросы безопасности и надежности процессов идентификации и аутентификации в отличие от развитых стран практически не регулируются, что не позволяет проводить оценку качества, безопасности и надежности сервисов идентификации и аутентификации.
2. Необходимо введение уровней достоверности идентификации и аутентификации.
3. Сформулированные выводы должны найти отражение в нормативной базе Российской Федерации по ИБ.

Выводы

1. При создании информационных систем, сервисов и прикладного программного обеспечения на базе PKI вопросам обеспечения доверия следует уделять должное внимание.
2. Необходимо вводить уровни доверия на только к аутентификации, но и к базовым сервисам PKI (штамп времени, валидация, актуальность реестров,...).
3. Нормативно-правовая база нуждается в совершенствовании, при этом следует использовать международные стандарты и рекомендации, в том числе Положение и регламент Regulation 910/2014.

Спасибо за внимание!

asabanov@mail.ru