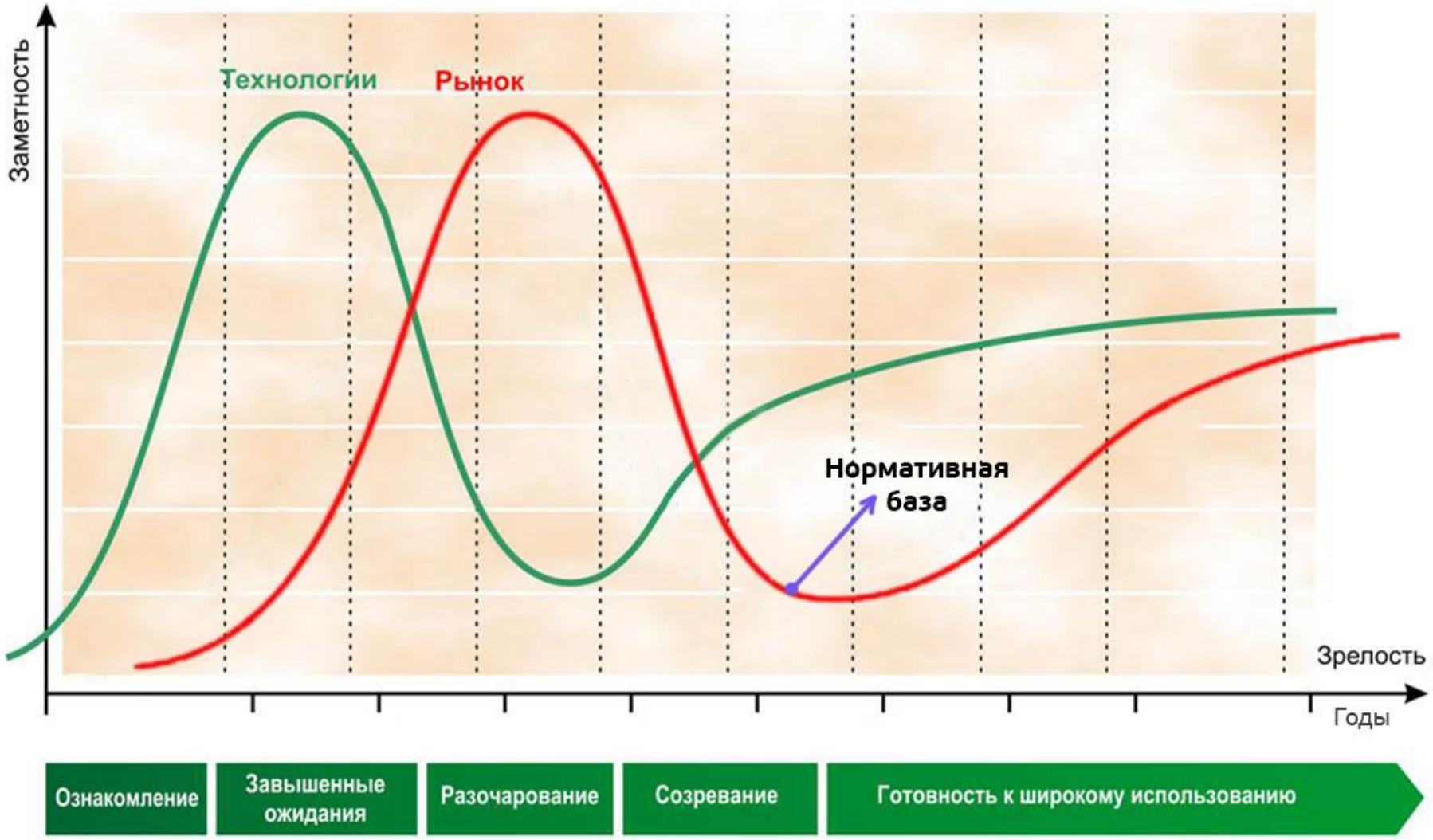
Аладдин РД

Актуальные проблемы регулирования развития PKI

Алексей Сабанов, к.т.н.,
Заместитель генерального директора

18 сентября 2013г.

Технологии и их внедрение



Электронная подпись: цели документов

- Директива 1999/93/ЕС «Об общих условиях использования электронных подписей» (1999г.) – унификация **правил использования** ЭП и формулировка условий, необходимых для признания юридической равнозначности собственноручной и ЭП
- Проект Регламента ЕС об электронной идентификации и доверенных службах на внутреннем рынке (2012г.) - необходимость **совершенствования законодательства** для исполнения в странах ЕС в системах электронной идентификации, аутентификации и подписи для **повышения доверия** к защищенным сервисам

Директива 1999/93/EC: Квалиф. X.509

- Квалифицированный сертификат (Qualified Certificate, QC) - сертификат, удовлетворяющий требованиям, сформулированным в Приложении I, созданный провайдером сертификационных услуг, удовлетворяющим требованиям, сформулированным в Приложении II Директивы.
- Провайдер сертификационных услуг (Certification-Service-Provider, CSP) - организация (entity), либо юридическое или физическое лицо, которая выпускает сертификаты либо обеспечивает другие сервисы, связанные с электронной подписью.
- Защищённое устройство создания подписи (Secure-Signature-Creation Device, SSCD) - сконфигурированное программное или аппаратное устройство создания подписи, которое удовлетворяет требованиям, сформулированным в Приложении III Директивы.

Директива 1999/93/ЕС: Квалиф. ЭП

a) сертификат является **квалифицированным** (удовлетворяет требованиям Приложения I Директивы);
b) провайдер служб сертификатов (по нашему – УЦ) **удовлетворяет требованиям** Приложения II Директивы;
c) **технология**, использованная для **формирования** подписи, является **безопасной** (удовлетворяет требованиям Приложения III Директивы);
d) **верификация подписи** выполнена в соответствии с **требованиями Приложения IV** Директивы (в частности, проверено, что в сертификате указана политика QC + SSCD и данные для формирования подписи хранятся в устройстве SSCD).

№63-ФЗ: равнозначность подписей

«Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе». В ст. 11 №63-ФЗ приведены условия признания квалифицированной электронной подписи.

Пункт 4 №63-ФЗ

- «Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и двум дополнительным признакам:
- 1) ключ проверки электронной подписи указан в квалифицированном сертификате;
  2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом».

В европейских документах неквалифицированная электронная подпись это усиленная, но не квалифицированная, а согласно приведённому выше определению из ФЗ, усиленная и неквалифицированная электронная подписи совпадают, причём квалифицированная электронная подпись является частным случаем неквалифицированной электронной подписи

Проект Регламента- 2012г.

- **Аутентификация** — электронный процесс, позволяющий проверить идентификационные данные лица, а также происхождение и целостность электронных данных
- **Квалифицированная электронная подпись** — усиленная электронная подпись, созданная с помощью устройства создания квалифицированной электронной подписи и подкрепленная квалифицированным сертификатом электронной подписи
- **Усиленная электронная подпись** — электронная подпись, которая:
- однозначно привязана к подписывающему лицу и позволяет идентифицировать его;
- создана с использованием данных электронной подписи, которые может использовать только подписывающая сторона, и;
- связана с подписываемыми данными так, что любое изменение таких данных будет заметно.
- **Устройство создания квалифицированной электронной подписи** — устройство создания электронной подписи, соответствующей требованиям Приложения II.

Важность аутентификации в мире

- “is a key element for the delivery of any e-services.”
  - European Commission COM(2008) 798 final (28 Nov. 2008)

- “is a critical component of . . . national and global economic, governmental and social activities [which] rely more and more on the Internet.”
  - OECD, The Role of Digital Identity Management in the Internet Economy (June 2009)

- “is a one of the most important security service of e-commerce and e-government”

  APEC Guidance for E-commerce (December 2005)

IDENTITY, CREDENTIAL, & ACCESS MANAGEMENT

Since its creation in fall 2008, the Identity, Credential, and Access Management (ICAM) program has focused on addressing challenges, pressing issues, and design requirements for digital identity, credential, and access management and defining and promoting consistency across approaches for implementing ICAM programs as reflected in the FICAM Roadmap & Implementation Guidance (FICAM Roadmap). The FICAM Roadmap was developed to outline a common framework for ICAM within the Federal Government and to provide supporting implementation guidance for federal agencies as they plan and execute a segment architecture for ICAM management programs. Much of the work accomplished under the FICAM program is driven by the Identity, Credential, and Access Management Subcommittee (ICAMSC).

Документы

- 04.2006 - NIST Special Publication 800-63 Version 1.0.2 Electronic Authentication Guideline | Download
- Backend Attribute Exchange (BAE) Governance | Download
- Backend Attribute Exchange (BAE) Overview | Download
- Federal ICAM Identity Scheme Adoption Process | Download
- Federal ICAM Privacy Guidance for Trust Framework Assessors and Auditors | Download
- Federal ICAM Trust Framework Provider Adoption Process for Levels of Assurance 1, 2, Non-PKI 3 | Download
- Federated Physical Access Control System (PACS) Guidance | Download
- FICAM Roadmap and Implementation Guidance | Download
- Fingerprint Exception Handling Guidelines | Download
- GSA Memorandum Acquisitions of Products and Services for Implementation of HSPD-12 | Download
- GSA Memorandum Federal Child Care Center Workers Facility Access Credentialing | Download
- GSA Technical Supplement in support of OMB issued memorandum M-05-05 | Download
- Identity, Credential, and Access Management (ICAM) Roadmap Snapshot | Download
- Modernizing Federal Logical Access Control Systems (LACS) Brochure | Download
- Modernizing Federal Physical Access Control Systems (PACS) Brochure | Download
- NIST SP800-63 E-Authentication Guideline | Download
- OMB M-04-04 E-Authentication Guidance for Federal Agencies | Download
- OMB Memorandum dated October 6, 2011 Requirements for Accepting Externally-Issued Identity Credentials | Download
- OMB Memorandum M-05-05 Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services | Download
- Password/PIN Entropy Tool | Download
- SAML Identifier and Protocol Profiles for BAE | Download
- SAML Metadata Profile for BAE | Download
- Security Assertion Markup Language (SAML) Web Browser Single Sign-on (SSO) Profile | Download
- Trust Framework Provider Assessment Package Application | Download
- Источник: http://www.idmanagement.gov/identity-credential-access-management

Выполнение Директивы 12 Президента

- **HSPD-12 PURCHASING**
- Through HSPD-12 Purchasing, Government approved products and services are made available to federal agencies through GSA Schedules. The resources available on the GSA Schedules have pre-approved vendors and pre-registered rates.
- **SCHEDULE 70 & SINS**
- IT Schedule 70 is an acquisition vehicle under the Multiple Award Schedule (MAS) program that gives agencies direct access to commercial experts who are able to address the needs of the government IT Community through a series of Special Item Numbers (SINs). These SINs cover most of the general purpose commercial IT hardware, software, and services and should be used by agencies as needed to meet their mission objectives as well as ICAM initiatives.
- Special Item Number Series 132 6x is reserved for product lines needed to authenticate an individual for purposes of physical and logical access control, electronic signature, performance of e-Business transactions and delivery of Government services. Pursuant to Section 211 of the E-Gov Act of 2002, Cooperative Purchasing provides authorized State and local government entities access to information technology items offered through GSA's Schedule 70 and the Corporate contracts for associated special item numbers.
- **QUALIFICATION REQUIREMENTS**
- Qualification Requirements and Evaluation Procedures for Special Item Number 132 6x Series:
- Special Item No. 132 60 A-F Access Certificates for Electronic Services (ACES) Program.
- Special Item No. 132 61 Public Key Infrastructure (PKI) Shared Service Provider Program.
- Special Item No. 132 62 HSPD-12 Product and Service Components.
- **SIN 132-62**
- The Special Item Number (SIN) 132-62 has been established for products and services to implement the requirements of HSPD-12, FIPS 201, and associated NIST special publications. Vendors providing offers on SIN 132-62 must meet the qualification requirements for the category of product and service being offered. Vendors should follow evaluation procedures outlined in the CONOPS document when submitting qualification packages to: Daryl Hendricks, (703) 306-6367, daryl.hendricks@gsa.gov.
- **QUALIFICATION RESOURCES**
- Qualification requirements are established for the following HSPD-12 system components and categories on SIN 132-62:
- PIV Enrollment and Registration Services and Products.
- PIV Systems Infrastructure Services and Products.
- PIV Card Management and Production Services and Products.
- PIV Card Activation and Finalization Services and Products.
- PIV System Integration Services and Products.
- Additional forms needed for the qualification process:
- Evaluation Cover Sheet From Vendor submits as part of the application package.
- Failure Review Form Vendor submits when in disagreement

Первоисточники

- Б.Шнайер. Прикладная криптография. – М.: Издательствоо ТРИУМФ, 2003 – 816с.
- FIPS 196, "Entity authentication using public key cryptography," Federal Information Processing Standards Publication 196, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997. (Аутентификация субъекта на основе криптографии открытых ключей).
- ISO/IEC 9798-1: 1997, Information technology– Security techniques- Entity authentication- Part 1: General. (Аутентификация субъекта. Часть1).
- ISO/IEC 9798-3: 1997, Information technology – Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques. (Аутентификация субъекта. Часть 3. Механизмы, использующие технологии цифровой подписи).
- RFC 3163. R. Zuccherato (Entrust Technology), M.Nystrom (RSA Security). ISO/IEC 9798-3 Authentication SASL Mechanism. August 2001.
- NIST SP-800-33 Технические модели, лежащие в основе безопасности информационных технологий. Дек.2001.

Нормативная база

- Declaration on Authentication for Electronic Commerce 7-9 October 1998
- CWA 14365 Guide of use of Electronic Signature. Jan.2003
- OMB Memorandum M-04-04 E-Authentication Guidance for Federal Agencies December 16, 2003 & OMB Circular A-130 2003
- Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004
- ISO/IEC 10181-2, ITU-T Rec/x.811 Теоретические основы аутентификации. 2004
- NIST Special Publication 800-63 April 2006 (РД по использованию е-аутентификации)
- OECD Recommendation on Electronic Authentication/2007
- FIPS PUB 201-1 Personal Identity Verification (PIV) of Federal Employees and Contractors. March 2006, FIPS PUB 201-2. March 2011
- ETSI draft SR 000 000 v0.0.2 Rationalised Framework for Electronic Signature Standardization August 2011 & ETSI TS 1, 103173,…

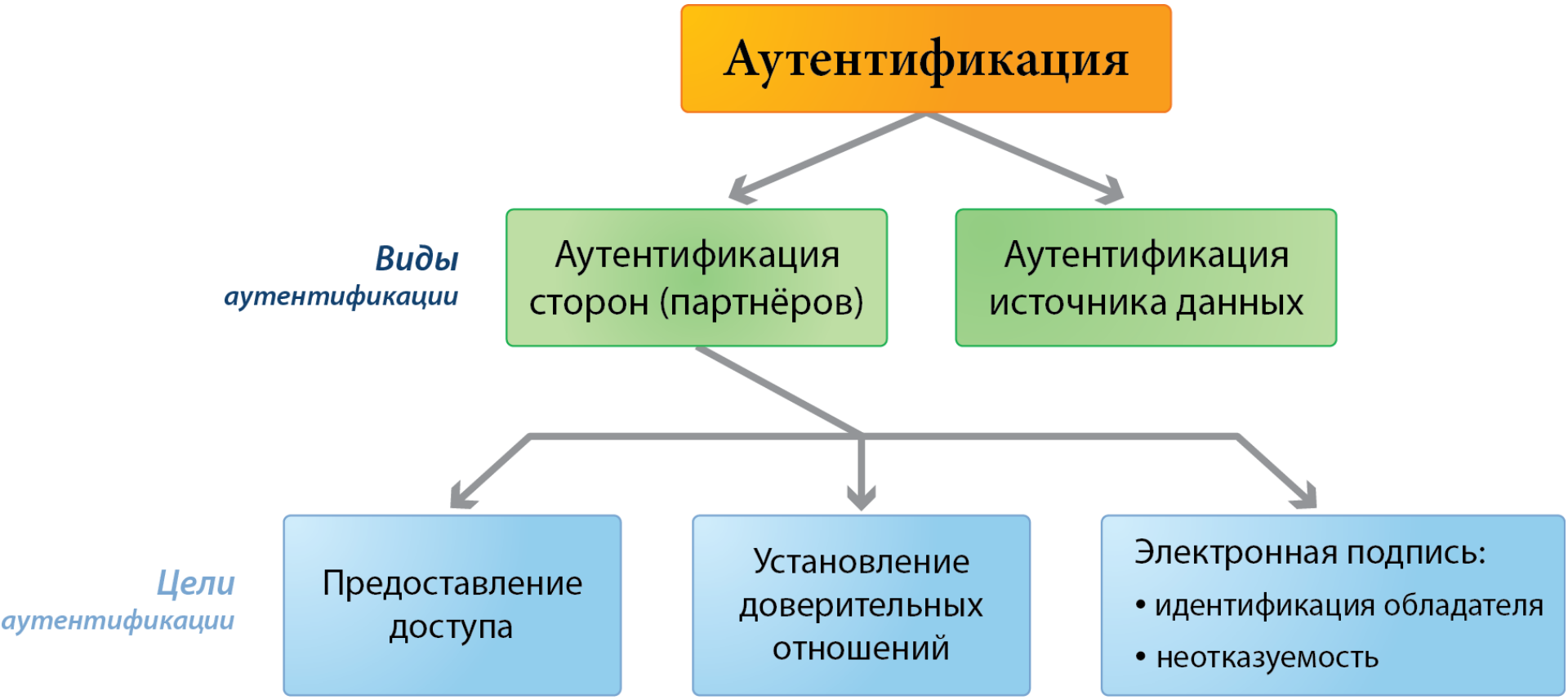
Работа над источниками

год	название	коротко суть
1997	FIPS 196, "Entity authentication using public key cryptography," Federal Information Processing Standards Publication 196, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 1997. (Аутентификация субъекта на основе криптографии открытых ключей).	стандарт рекомендован к применению во всех федеральных ведомствах для несекретной информации. Может применяться во всех коммерческих организациях. Аутентификация на основе криптографии с открытыми ключами может применяться во всех приложениях, когда стороны аутентифкации не имеют сведений о существовании друг друга. Протоколы аутентификации (односторонний и двухсторонний), описанные в данном стандарте, можно использовать с другими системами на основе PKI.
1997	ISO/IEC 9798-1: 1997, Information technology – Security techniques - Entity authentication - Part 1: General. (Аутентификация субъекта. Часть 1. Общие подходы)	даны определения и определены общие подходы к идентификации и аутентификации
1997	ISO/IEC 9798-3: 1997, Information technology – Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques. (Аутентификация субъекта. Часть 3. Механизмы, использующие технологии цифровой подписи)	определены пять различных протоколов для односторонней и двусторонней аутентификации с использованием криптографических алгоритмов с открытым ключом
1998	Министерская декларация об аутентификации для элеткронной коммерции. ODCE. Оттава 1998	учитывая необходимость обеспечения конфиденциальности данных пользователей в электронной коммерции признается необходимость развития аутентификации. При этом должно быть отсутствие дискриминационных подходов к механизмам и средствам эл.аутентфикации, принятых в других странах. Правительства призываются быть промоутерами e-commerce и эл.аутентификации.
2001	RFC 3163. R. Zuccherato (Entrust Technology), M.Nystrom (RSA Security). ISO/IEC 9798-3 Authentication SASL Mechanism. Aug 2001. (Механизм аутентификации SASL по ИСО/МЭК 9798-3)	определяется механизм аутентификации SASL (Simple Authentication and Security Layer, простой уровень аутентификации и безопасности), основанный на стандартах аутентификации субъекта ИСО/МЭК 9798-3 и FIPS PUB 196. одностороняя и взаимная(ЭЦП)
2001	NIST SP-800-33 Технические модели, лежащие в основе безопасности информационных технологий. Дек.2001	системное исследование компьютерной безопасности. Основано на рассмотрении сервисов безопасности (К-конфиденц., Ц-целостность, Д- доступн., надежность, возможность учета действий пользователей, гарантии. Показано, что гарантии выполнения основных задач ИБ (КДЦ) зависят от реализации задач К, Ц, учета.картинки.

Классификация средств идентификации и аутентификации

с точки зрения применяемых технологий

Классификация аутентификации по видам и целям

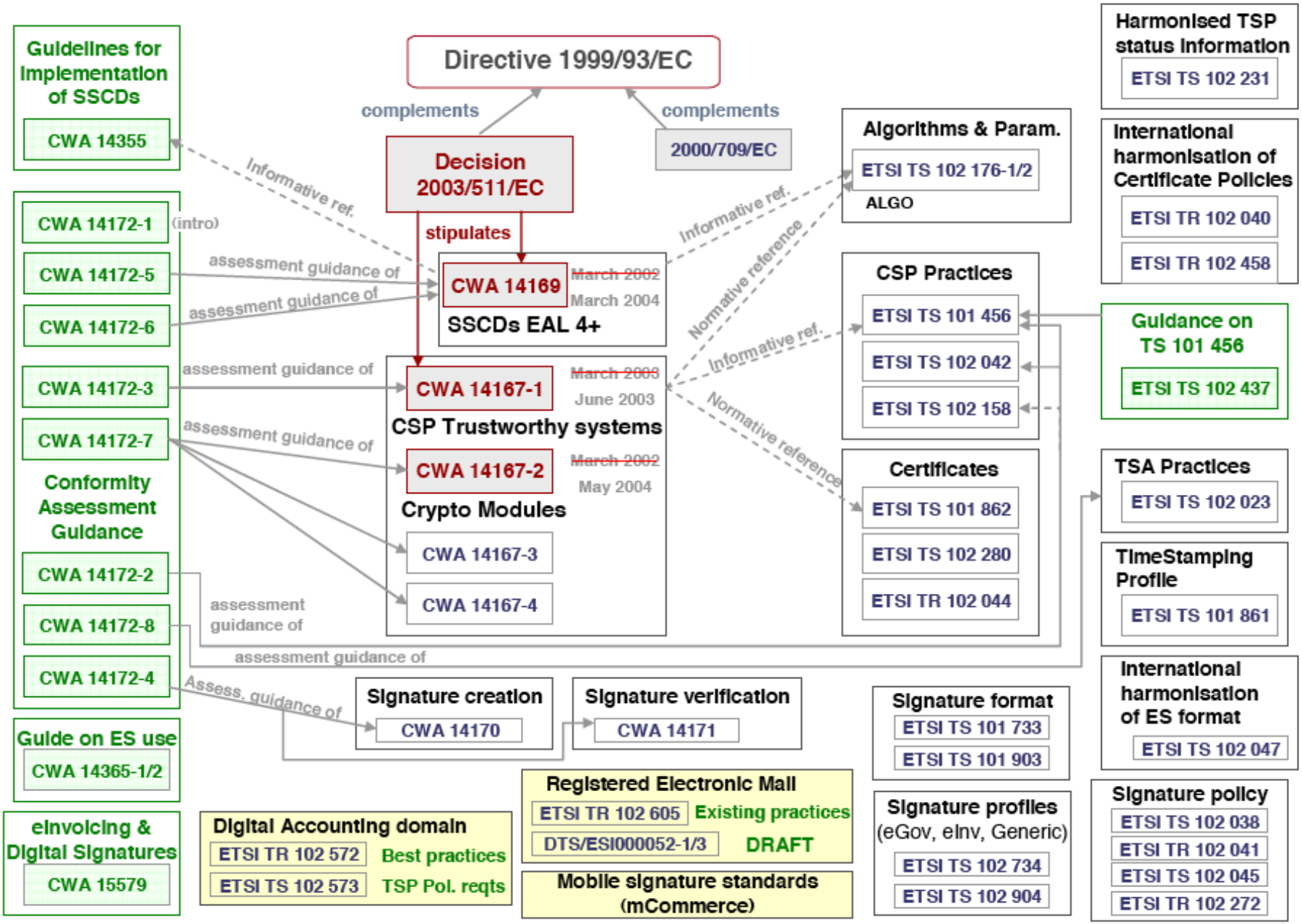


Три вида секрета, три типа аутентификации

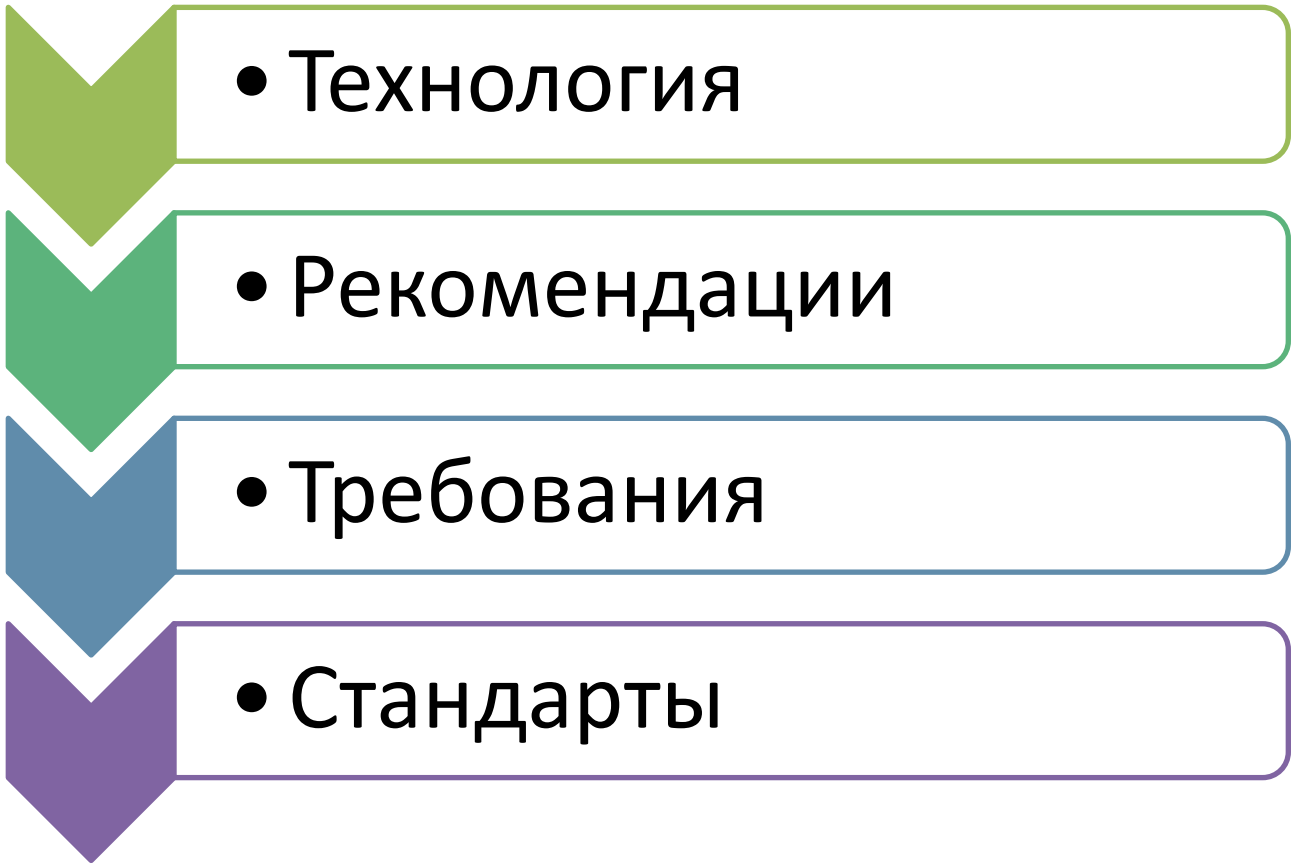
Учетная запись пользователя	Секрет (аутентификатор)	Тип аутентификации
логин	пароль	простая
логин/ поля неквалифицированного сертификата	одноразовый пароль (технология OTP)/ закрытый ключ	усиленная
заданные поля сертификата X.509, сформированного аккредитованным удостоверяющим центром для доступа пользователя	закрытый ключ (в терминах №1-ФЗ)	строгая

Классификация аутентификации

EU eSignature Standardisation Work overview



Диалектика развития стандартов

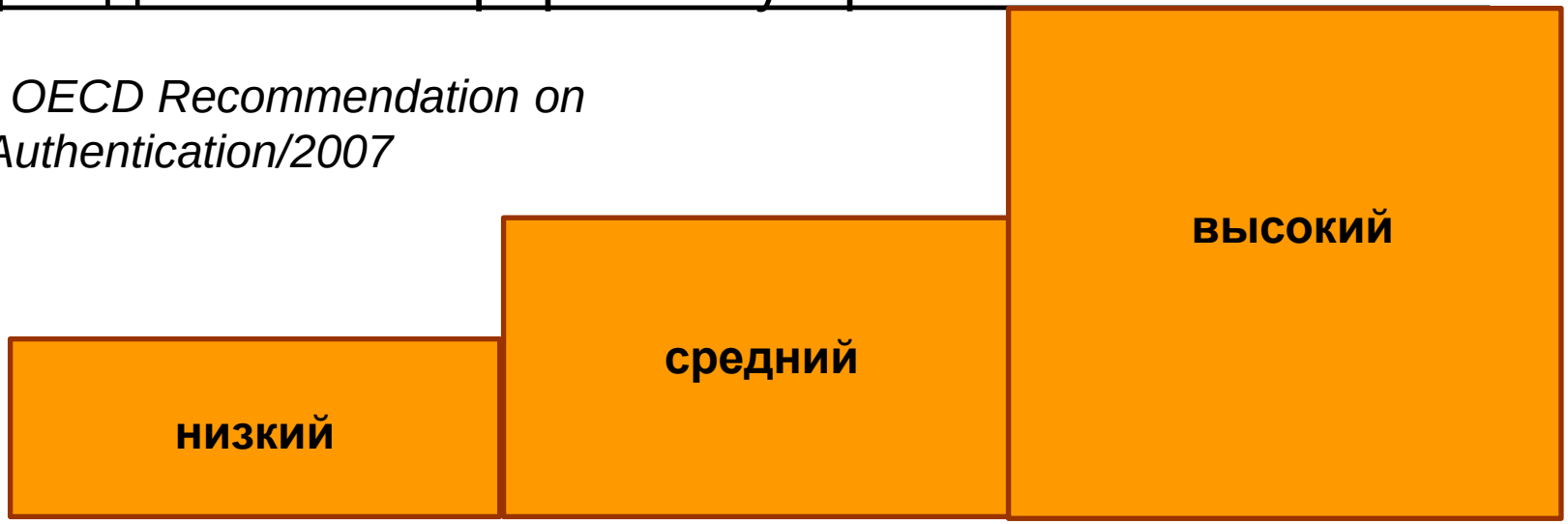


ОЭСР(OECD): Уровни последствий ошибок ААА

Применение средств ААА должно быть приведено в соответствие с потребностями и уровнем риска

- Физические лица – как минимум, пара «логин/пароль»
- Организации (бизнес) - OTP + Защищенные ключевые носители
- Государственные органы – строгая аутентификация, секрет должны генерировать устройства класса SSCD

Источник: OECD Recommendation on Electronic Authentication/2007



4 уровня гарантий аутентификации в США

Административно-бюджетное управление при Президенте США для федеральных ведомств и NIST разработали уровни минимальных технических требований к:

- токенам (аутентификаторам);
- Процессам подтверждения подлинности, регистрации, изданию и передаче цифровых удостоверений, связыванию
- Механизмам удаленной аутентификации (комбинация из цифровых удостоверений, токенов и протоколов аутентификации)
- Механизмам подтверждения, используемой для передачи результатов удаленной аутентификации другим сторонам)

Проблемы глоссария

Аутентификация	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности	Руководящий документ «Защита от НСД к информации. Термины и определения», Утверждено решением председателя Гостехкомиссии России от 30.03.1992 г.
Аутентификация отправителя данных	Подтверждение того, что отправитель полученных данных соответствует заявленному	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 15 февраля 2008 г.
Аутентификация участников информационного взаимодействия (в ЕСИА)	Проверка принадлежности участнику информационного взаимодействия введенного им идентификатора, а также подтверждение подлинности идентификатора	Постановление Правительства РФ от 28.11.2011 г. № 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"
Аутентификация сведений об участниках информационного взаимодействия (сведений об их информационных системах)	Проверка, в том числе с использованием квалифицированных сертификатов ключей проверки электронных подписей, принадлежности участнику информационного взаимодействия или его информационной системе введенного им идентификатора, а также подтверждения подлинности идентификатора;	Постановление Правительства РФ от 10.07.2013 г. № 584 «Правила использования федеральной государственной информационной системы "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"»

Выводы

- Анализ зарубежного опыта показывает, что исторически первыми требования к аутентификации разработаны в США. Канада, Австралия и ряд других стран повторяют и лишь локализуют американские требования, которые являются наиболее проработанными.
- Российская нормативная база существенно отстает от развитых стран. Необходимо сократить это отставание нормативного регулирования на основе анализа зарубежных разработок
- Самой большой проблемой существующей и планируемой к опубликованию российской нормативной базы является полная независимость от технологий.
- Представленный подход может лечь в основу научной основы разработки нормативных требований к созданию надежных и безопасных систем аутентификации.

Аладдин РД

Спасибо за внимание!

a.sabanov@aladdin-rd.ru