Перспективы стандартизации доверенных сервисов на базе PKI

06 сентября 2017 г.

XV Юбилейный PKI-форум

Алексей Сабанов, к.т.н.,

ЗАО "Аладдин Р.Д."

Зачем необходима система доверия и система стандартов доверенных сервисов

1. Неуклонный рост мошенничеств и злоумышленных действий в киберпространстве.
2. Отсутствие общепризнанных понятий и требований к безопасности, надежности и качеству доверенных сервисов, технически обеспечивающих юридическую силу (ЮС) электронным документам и сообщениям.
3. Выбор технологий и средств обеспечения юридической силы электронных документов кроме сервиса ЭП отдан на откуп владельцам ИС и разработчикам.
4. Актуальность проблем обеспечения доверия к удалённому электронному взаимодействию в мире непрерывно повышается (внедрение eIDAS -EC, USA Strategy, e-Authentication Австралия и др.)

ЮС: Минимальный набор сервисов безопасности

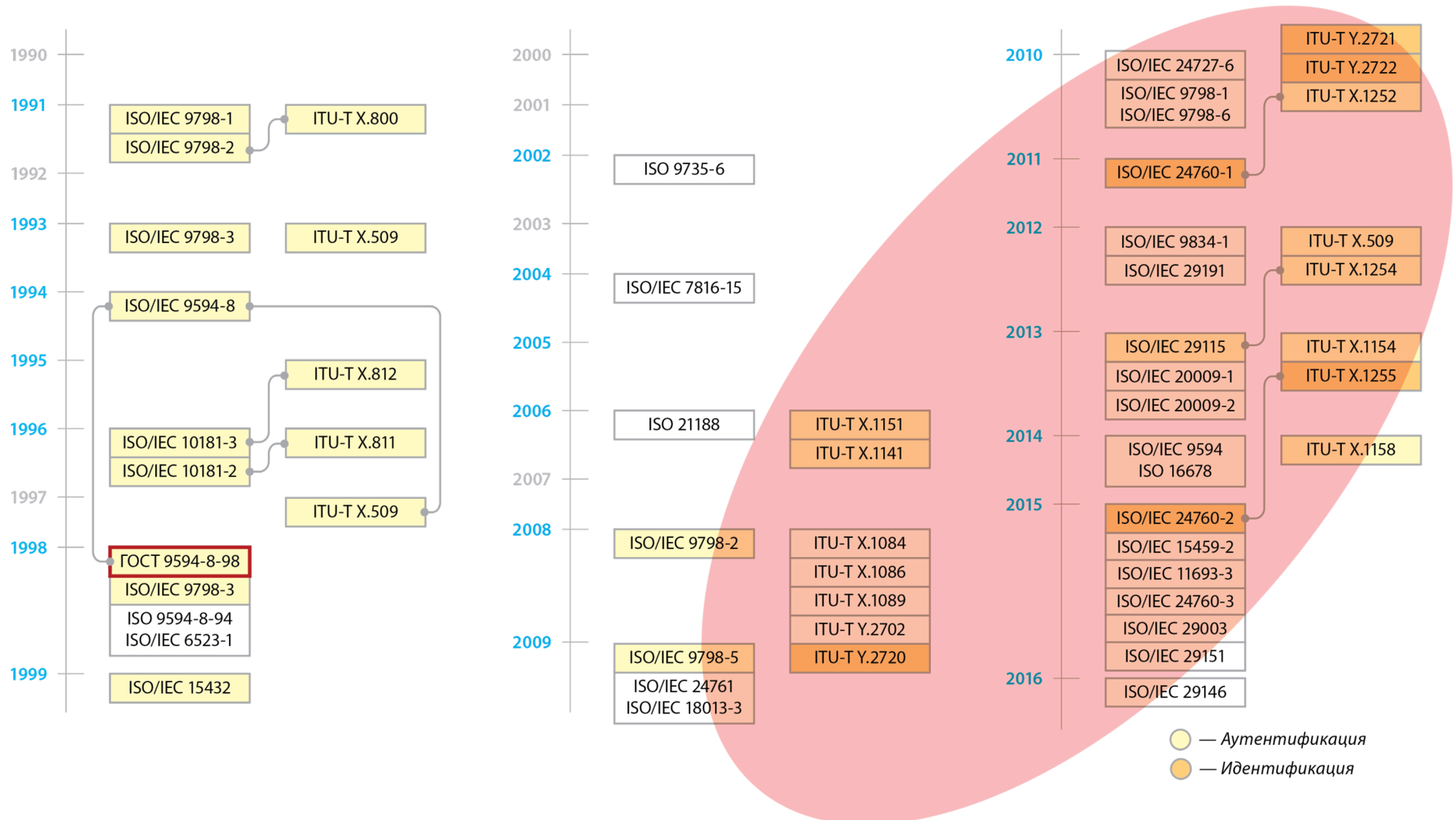
- Идентификация и аутентификация подписанта
- Электронная подпись (63-ФЗ, ГОСТ Р 34.10-2012 ГОСТ 34.11-2012)
- Метка доверенного времени (RFC 3161 «Time-Stamp Protocol (TSP)»
- Валидация сертификата ключа проверки подписи и сертификата доступа (RFC 2459)
- Проверка полномочий подписанта

Уровни доверия к сервисам должны быть сбалансированы!

Сервис аутентификации

- обеспечение доказательства подлинности предъявленного идентификатора (ISO/IEC 10181-2:1996, 9798-3:1998);
- доказательство принадлежности аутентификатора, с помощью которого производится доказательство подлинности, конкретному субъекту (ISO/IEC 24760-2: 2015);
- аутентификация сторон – подтверждение того, что взаимодействующая сторона является той, за которую себя выдает (ISO 29115: 2013).

Идентификация и аутентификация



Что нового внесено в проект ГОСТ по ИА

1. Введено понятие первичной и вторичной идентификации
2. Дано новое определение аутентификации
3. Введено понятие электронного удостоверения (ЭУ) = цифровой сертификат доступа, изданный УЦ (ДТС)
4. Предложены три основных вида аутентификации: простая, усиленная, строгая
5. Введено понятие аутентификационной информации (АИ) для строгой аутентификации. АИ=закрытый ключ и соотв. ему ЭУ. Впервые в НПА введён неизвлекаемый закрытый ключ (п.7.12.3) – повышенная защищённость от клонирования.

Функции электронной подписи

- аутентификация источника данных – подтверждение подлинности источника полученных данных (ISO 7498-2);
- обеспечение целостности данных, означающее, что данные не были модифицированы или уничтожены неавторизованным образом (ISO 7498-2);
- невозможность отрицания авторства – сервис защиты от отрицания автором факта создания или отправления им сообщения (ISO/IEC 13888-1).

Стандарты электронной подписи

- №63-ФЗ Об электронной подписи
- ГОСТ Р 34.10-2012 (пока еще действует ГОСТ Р 34.10-2001) - средство ЭП
- ГОСТ Р 34.11-2012 (пока еще действует ГОСТ Р 34.11-2001) – вычисление хэша

Руководство по встраиванию СКЗИ пока не разработано и не опубликовано. Разработчики СКЗИ составляют и распространяют этот документ самостоятельно.

Метка доверенного времени

- ITU-T X.842 (10/2000) Guidelines for the use and management of trusted third party services // ISO/IEC TR 14516:2002 Информационные технологии. Методы защиты. Руководящие указания по использованию и управлению службами доверенной третьей стороны
- ITU-T X.843 (10/2000) Specification of TTP services to support the application of digital signatures // ISO/IEC 15945:2002 Информационные технологии. Методы защиты. Спецификация служб TTP для поддержки применения электронных подписей
- ISO/IEC 18014-1: 2008-09-01, Time-stamping services - Part 1: Framework (2nd edition)
- ISO/IEC 18014-2: 2009-12-15, Time-stamping services - Part 2: Mechanisms producing independent tokens (2nd edition)
- ISO/IEC 18014-3: 2009-12-15, Time-stamping services - Part 3: Mechanisms producing linked tokens (2nd edition)
- ISO/IEC 18014-4: 2015-04-15, Time-stamping services - Part 4: Traceability of time sources(1st edition)

Сервис валидации. Функции

1) Проверка формата сертификата ЭП:
•проверяется по формальным признакам (формат и структура файла (нотация));
•проверяется наличие и содержание обязательных полей и дополнений.
2) Имеется ли политика валидации для проверки сертификата ЭП, определяющая требования к проверке сертификата КС, сертификатов ЦС и криптографическим алгоритмам.
3) Срок действия сертификата не истек на момент осуществления проверки.
4) Сертификат не отозван, и информация об отзыве удовлетворяет требованиям к актуальности.
5) Сформирована цепочка сертификации.
6) Срок действия сертификатов ЦС не истек.
7) Ни один из сертификатов ЦС не отозван.
8) Сертификаты ЦС соответствуют требованиям (ограничения по длине и проч.).
9) Криптографическая проверка сертификата КС
•Криптографическая проверка требований к длине ключа проверки ЭП, целостности полей сертификата КС, требований к используемым криптографическим алгоритмам.

Протоколы:

- Data Validation and Certification Server Protocols (DVCS) с квит. сервера (RFC 3029)
- On-line Certificate Status Protocol - OCSP (RFC 2560)
- Validation of Public Key Certificates (VPKC)

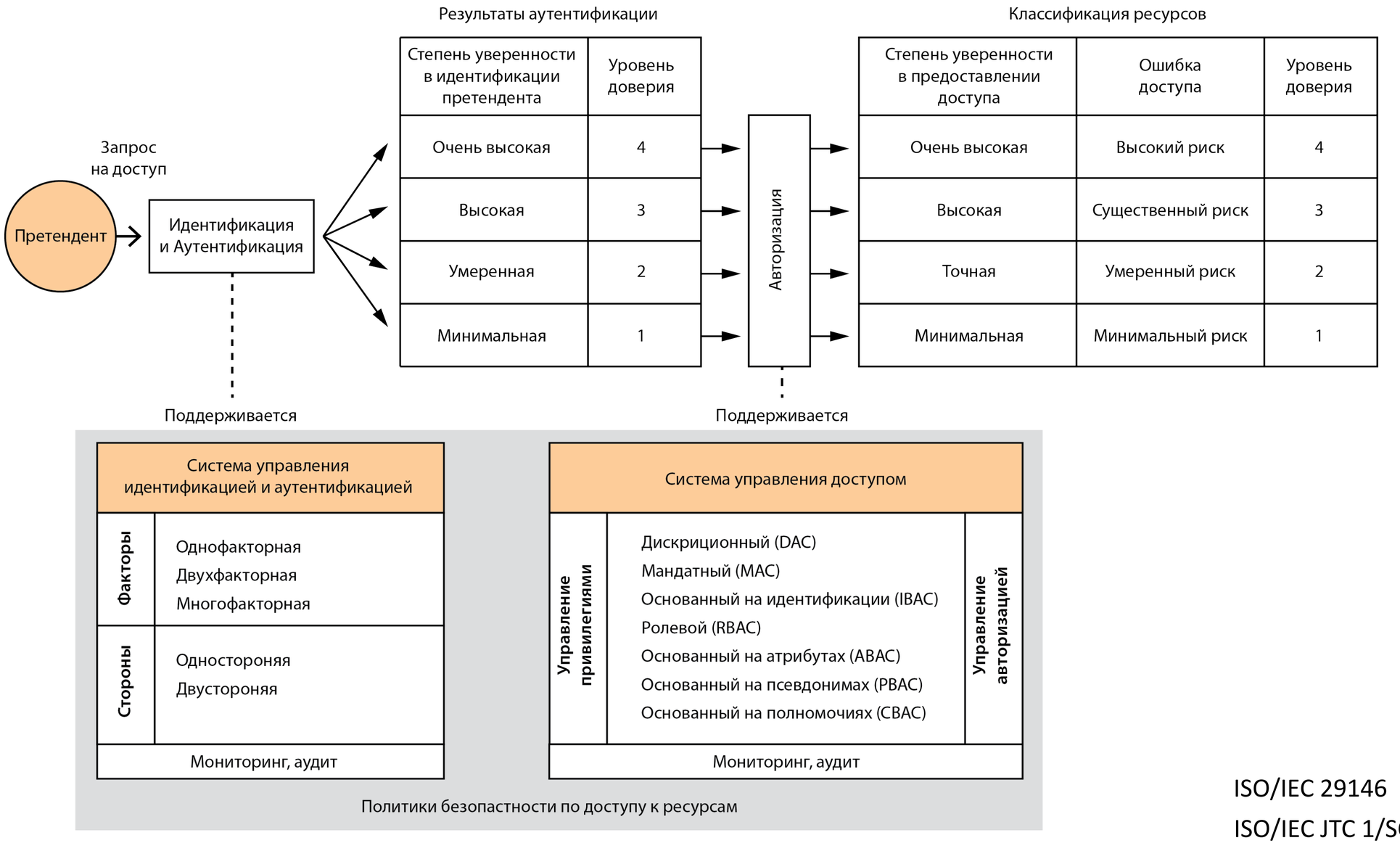
На основе RFC 2459

Валидация. Стандарты

ITU-T X.509 (10/2016) | ISO/IEC 9594-8: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
ETSI TS 119 102-1 V1.0.1 «Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation», 2015.
ETSI TR 119 100 V1.1.1 «Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for signature creation and validation», 2016.
ETSI TS 119 101 V1.1.1 «Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation», 2016.

certificate validation -286 упоминаний на сайте ITU-T.org

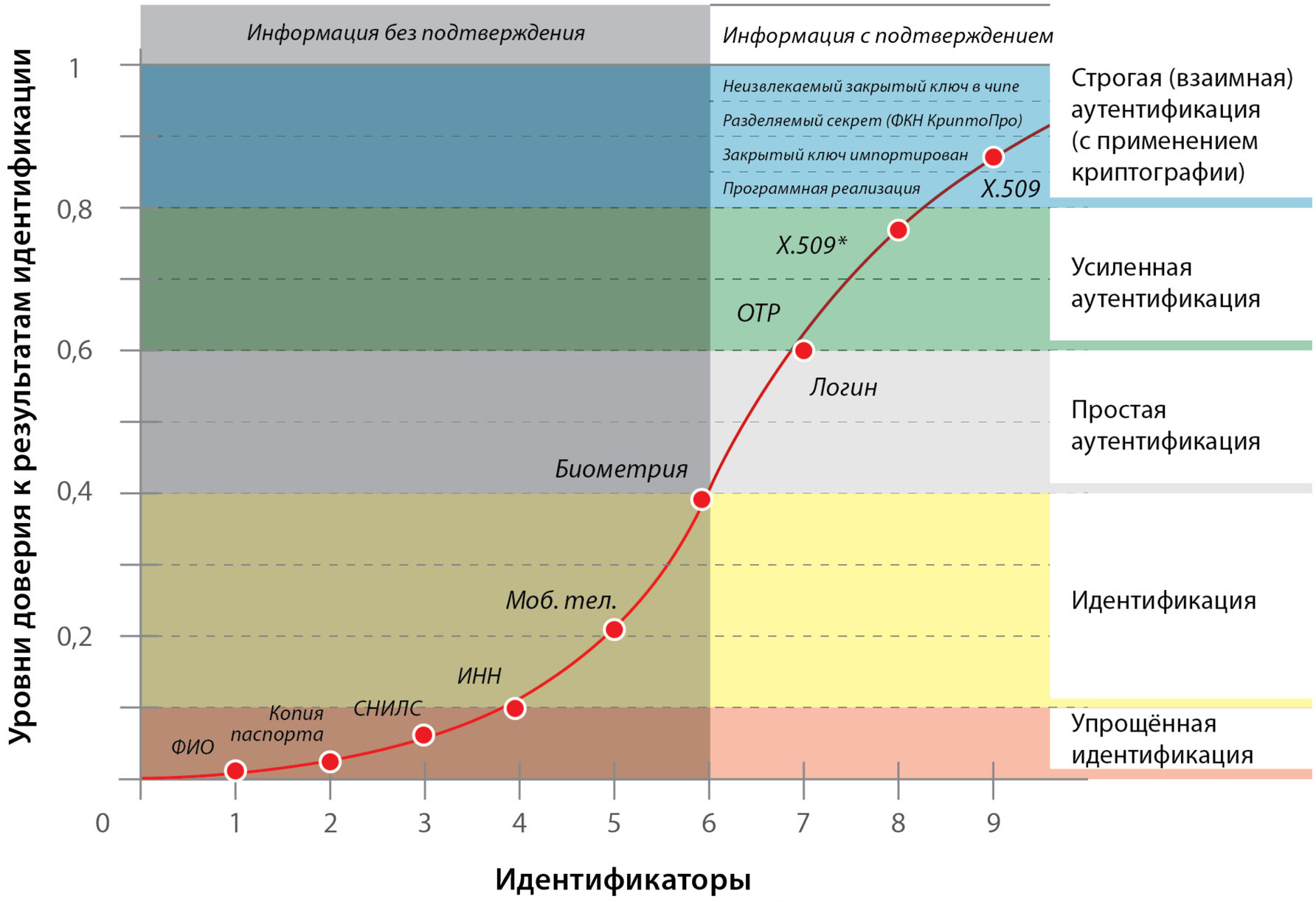
Современный взгляд на управление доступом



ISO/IEC 29146

ISO/IEC JTC 1/SC27/WG 5

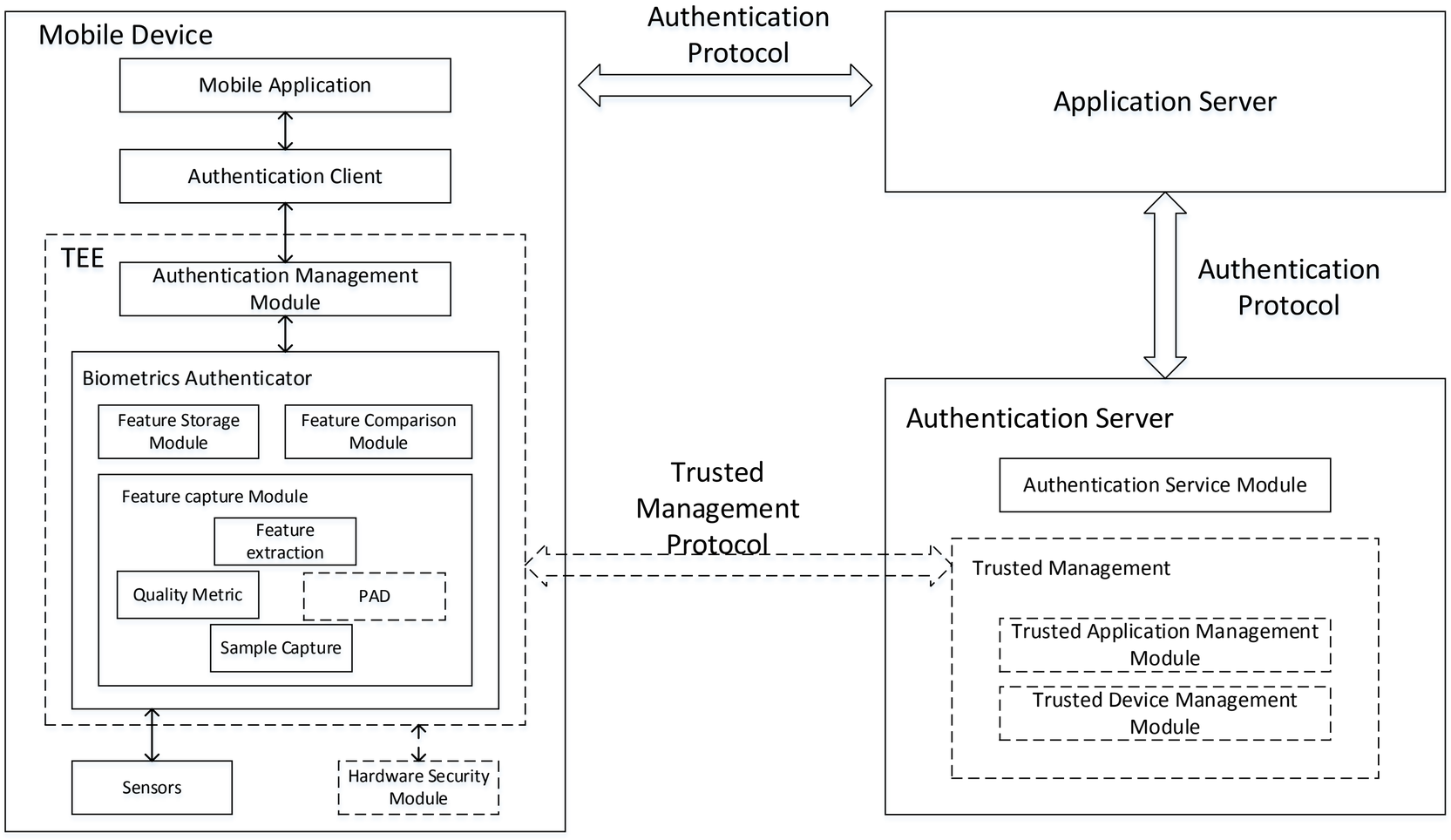
Уровни доверия к идентификации



Пример. Телебиометрия на мобильных устройствах, отчёт ISO/ПК27/WG5 2017г.

- Мобильная аутентификация разделяется на локальную и удалённую (на сервере аутентификации).
- Локальная аутентификация более защищена: отсутствие утечек при передаче аутентификцаионной информации.
- При удалённой аутентификации биометрические данные, как правило, остаются в мобильном устройстве, поскольку при передаче они могут подвергаться атакам. Существуют комбинированные методы, при этом применяется строгая аутентификация с использованием токена и двухфакторной аутентификации, биометрия применяется только для разблокирования токена для передачи информации на сервер аутентификации.
- Основное внимание уделяется согласованию уровней доверия к результатам локальной аутентификации с уровнями доверия к резульататам аутентификации на сервере аутентификации и сервере приложений.

Предлагаемая схема аутентификации



Планы развития стандартов

Концепция национальной стандартизации

Распоряжение Правительства РФ от 24 сентября 2012 г. N 1762-р

1. Одобрить прилагаемую Концепцию развития национальной системы стандартизации Российской Федерации на период до 2020 года.

2. Федеральным органам исполнительной власти учитывать положения Концепции, указанной в пункте 1 настоящего распоряжения, при проведении работ в области технического регулирования и стандартизации.

Председатель Правительства
Российской Федерации Д. Медведев

Москва
24 сентября 2012 г. N 1762-р

Концепция
развития национальной системы стандартизации Российской Федерации на период до 2020 года
(одобрена распоряжением Правительства РФ от 24 сентября 2012 г. N 1762-р)

I. Введение

Настоящая Концепция содержит систему взглядов на развитие национальной системы стандартизации в Российской Федерации и формирует цели, задачи и направления ее развития на период до 2020 года.

Национальная система стандартизации представляет собой взаимосвязанную совокупность организационно-функциональных элементов, документов в области стандартизации, определяющих в том числе правила и процедуры стандартизации для осуществления деятельности по установлению требований и характеристик в целях их добровольного многократного использования. Документы в области стандартизации направлены на достижение упорядоченности в сферах производства и обращения продукции, повышение конкурентоспособности продукции (работ, услуг) и реализацию иных целей и задач стандартизации.

Стандартизация является одним из ключевых факторов, влияющих на модернизацию, технологическое и социально-экономическое развитие России, а также на повышение обороноспособности государства.

Национальная система стандартизации включает в себя комплекс общетехнических стандартов и стандартов по отраслям экономики, стандарты безопасности труда и охраны здоровья, стандарты безопасности при чрезвычайных ситуациях и другие подсистемы стандартизации, а также участников работ по стандартизации, в том числе по стандартизации оборонной продукции (работ, услуг), и документы по стандартизации такой продукции. Документы по стандартизации оборонной продукции (работ, услуг) увязаны с национальными стандартами за счет комплексности стандартизации, обеспечивающей проведение работ по стандартизации взаимосвязанных объектов. Деятельность по стандартизации оборонной продукции (работ, услуг) обеспечивается в том числе за счет взаимосогласованных процедур планирования, разработки, принятия, пересмотра и отмены документов по стандартизации оборонной продукции (работ, услуг), а также национальных стандартов и общероссийских классификаторов технико-экономической и социальной информации, применяемых при разработке, производстве, эксплуатации и утилизации оборонной продукции (работ, услуг) и внесения в них изменений.

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНКОМСВЯЗЬ РОССИИ)

ПРИКАЗ

18.04.2014 №86

Москва

О совершенствовании системы стандартизации в области телекоммуникаций

В целях реализации Концепции развития национальной системы стандартизации Российской Федерации на период до 2020 года и совершенствования системы стандартизации в области телекоммуникаций
ПРИКАЗЫВАЮ:

1. Одобрить прилагаемую «Программу стандартизации в области телекоммуникаций на период до 2020 года» (далее - Программа стандартизации).

2. ДРРСС (Степаненко), ДИП (Телков), Россвязь (Духовницкий) организовать доработку проекта Программы стандартизации в области телекоммуникаций на перспективу до 2020 года с учетом предложений, высказанных на заседании Правительственной комиссии (протокол от 4 марта 2014 г. № 1), а также согласовать Программу стандартизации с Минпромторгом России, Росстандартом и другими заинтересованными федеральными органами исполнительной власти и представить ее на рассмотрение рабочей группой по вопросам совершенствования системы стандартизации в области телекоммуникаций при Правительственной комиссии по связи.
Срок: 15 октября 2014 г.

3. ДМС (Исмаилов) организовать работу по анализу международного опыта и представить предложения по участию Администрации связи Российской Федерации и представителей Администрации связи Российской Федерации в международных и региональных организациях по стандартизации, а также представить обобщенные предложения в целях их рассмотрения рабочей группой по вопросам совершенствования системы стандартизации в области телекоммуникаций при Правительственной комиссии по связи.
Срок: 2 квартал 2014 г.

4. Возложить контроль за исполнением настоящего приказа на заместителя Министра Д.М. Алхазова.

Министр Н.А. Никифоров

http://minsvyaz.ru/ru/documents/?words=%D0%9F%D0%A0%D0%98%D0%9A%D0%90%D0%97+18.04.2014

Планы развития стандартов. Росстандарт

- Ср. 13 сентября 2017

Официальный сайт

Федеральное агентство по техническому регулированию и метрологии

РОССТАНДАРТ

- Электронные услуги
- Техническое регулирование
- Стандартизация
- НДТ
- Метрология
- Подтверждение соответствия
- Информационные системы

- Деятельность
- Планы работ

Основные задачи Федерального агентства по техническому регулированию и метрологии на 2017 год

План внутреннего финансового аудита на 2017 год

Ведомственный план Федерального агентства по техническому регулированию и метрологии по реализации Концепции открытости федеральных органов исполнительной власти на 2017 год

Презентация по Ведомственному плану Федерального агентства по техническому регулированию и метрологии по реализации Концепции открытости федеральных органов исполнительной власти на 2017 год.

План снижения объемов и количества объектов незавершенного строительства по Федеральному агентству по техническому регулированию и метрологии

В соответствии с порядком и критериями ежегодного согласования Правительственной комиссией по координации деятельности открытого правительства планов и отчетов федеральных органов исполнительной власти по расходованию средств на информационное сопровождение своей деятельности, включая расходы подведомственных организаций, одобренными протоколом заседания Правительственной комиссии по координации деятельности открытого правительства от 17 декабря 2015 г. № 8 Федеральное агентство по техническому регулированию и метрологии публикует:

План по расходованию средств на информационное сопровождение деятельности федерального органа исполнительной власти Таблица № 1.1. Общие сведения о целях и задачах информационного сопровождении деятельности федерального органа исполнительной власти на плановый период

План по расходованию средств на информационное сопровождение деятельности федерального органа исполнительной власти Таблица № 1.2. Сведения об основных направлениях информационного сопровождения деятельности ФОИВ

Приказом Росстандарта № 469 от 26 апреля 2016 г. утвержден План информатизации Федерального агентства по техническому регулированию и метрологии на 2016 год и плановый период 2017-2018 годы

Приказом Росстандарта № 302 от 22 марта 2016 г. утвержден План информатизации Федерального агентства по техническому регулированию и метрологии на 2015 год и плановый период 2015-2017 годы

Ведомственный план Росстандарта по реализации Концепции открытости федеральных органов исполнительной власти на 2016 год с учетом «Горизонта планирования» до 2018 года

План работы Федерального агентства по техническому регулированию и метрологии на I квартал 2016 г.

План работы Федерального агентства по техническому регулированию и метрологии на II квартал 2016 г.

План работы Федерального агентства по техническому регулированию и метрологии на III квартал 2016 г.

План работы Федерального агентства по техническому регулированию и метрологии на IV квартал 2016 г.

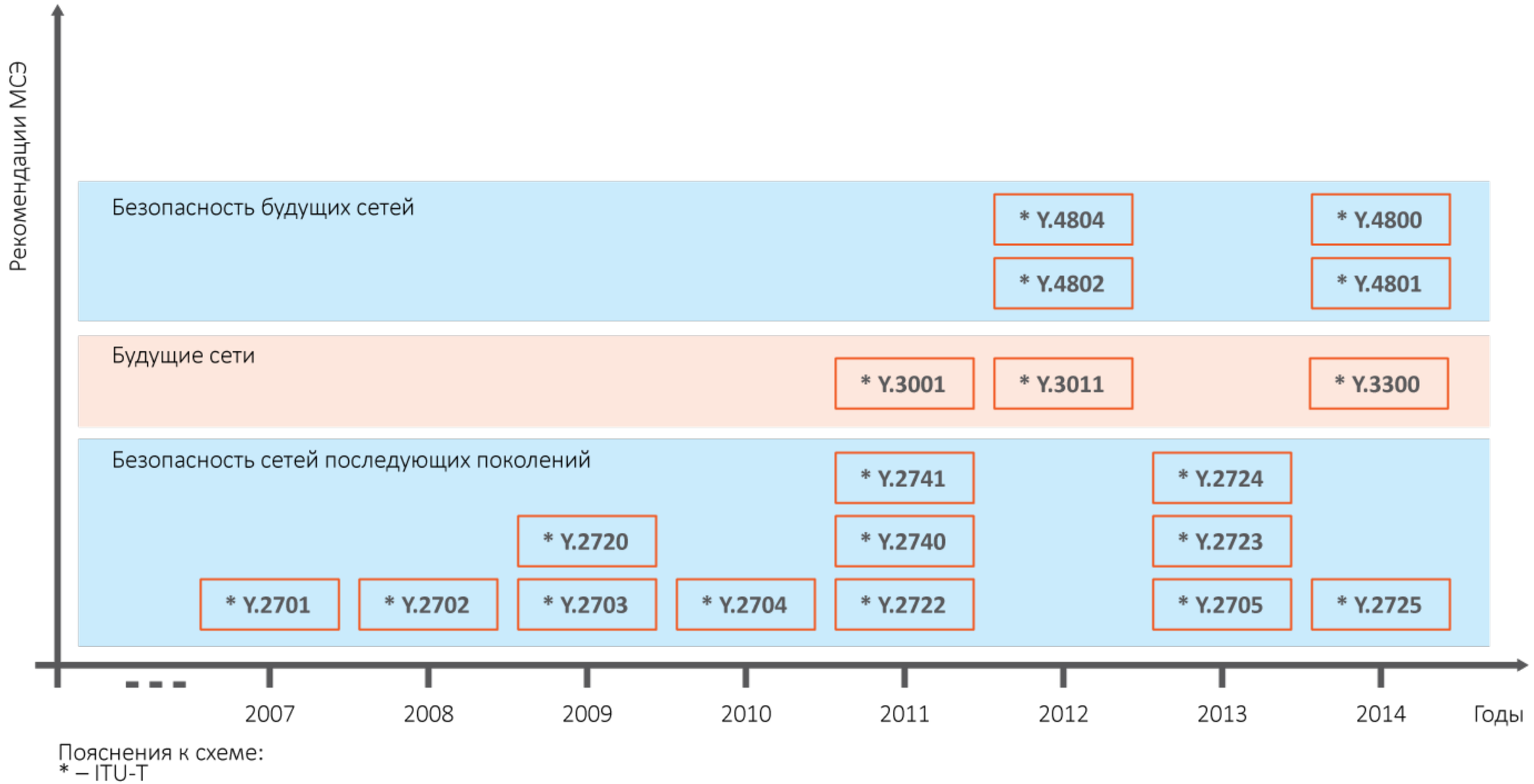
ПЛАН РАБОТЫ Федерального агентства по техническому регулированию и метрологии на 2015 год по обеспечению реализации основных задач, одобренных на заседании коллегии Федерального агентства 11 февраля 2015 года по вопросу «Об итогах деятельности Федерального агентства по техническому регулированию и метрологии в 2014 году и задачах на 2015 год»

Планы Росстандарта

Шифр задания Программы НС / Программы МГС / Код ОКП / Код ОКС	Наименование проекта национального стандарта РФ (межгосударственного стандарта, международного стандарта) Вид работы	Наименование технического регламента или федерального закона, в обеспечение которого разрабатывается стандарт / Наименование приоритетных направлений стандартизации	Сроки (месяц, год)		Наименование организации - головного разработчика, организаций соисполнителей	Источники финансирования разработки
			Направления в Ростехрегулирование уведомления о начале / завершении разработки ГОСТ Р или ГОСТ	Направления в Ростехрегулирование окончательной редакции проекта ГОСТ Р или ГОСТ, отчета о разработке проекта МС		
				утверждения ГОСТ Р	Институт-эксперт	Источники финансирования экспертизы и подготовки к утверждению
				отправки проекта ГОСТ в МГС		
1	2	3	4	5	6	7
ТК 002 Зерно, продукты его переработки и маслосемена						
2 Межгосударственная стандартизация						
1.7.002-2.002.15	Тритикале. Технические условия Разработка ГОСТ	О безопасности зерна (ТР ТС)		02.2016	ФГБГНУ "ВНИИЗ"	Средства разработчика
97 1180		Конкурентоспособность		06.2016		Средства разработчика
67.060				04.2016		
1.7.002-2.003.15	Просо. Технические условия Разработка ГОСТ	О безопасности зерна (ТР ТС)		03.2016	Конкурс	Федеральный бюджет
97 1510		Конкурентоспособность		11.2016		Федеральный бюджет
67.060				07.2016		
1.7.002-2.005.15	Мука и отруби. Метод определения зольности Пересмотр ГОСТ 27494-87	О безопасности пищевых продуктов (ТР ТС)		02.2016	Конкурс	Федеральный бюджет
		Защита прав потребителя Конкурентоспособность		11.2016		Федеральный бюджет
67.060				06.2016		

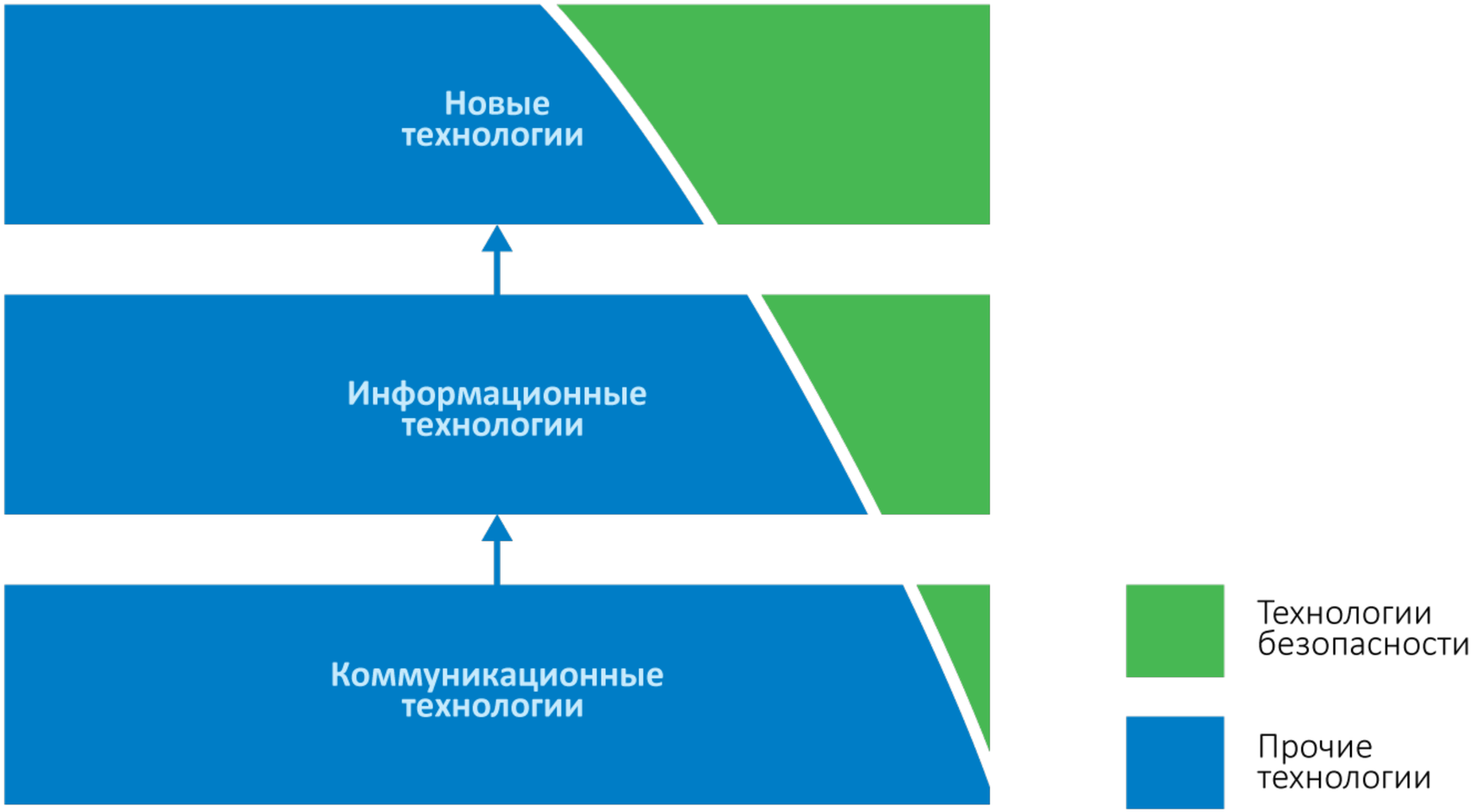
http://www.gost.ru/wps/portal/pages.ConceptionOfNationalStandartisation

Взгляд в будущее. Стандарты по связи

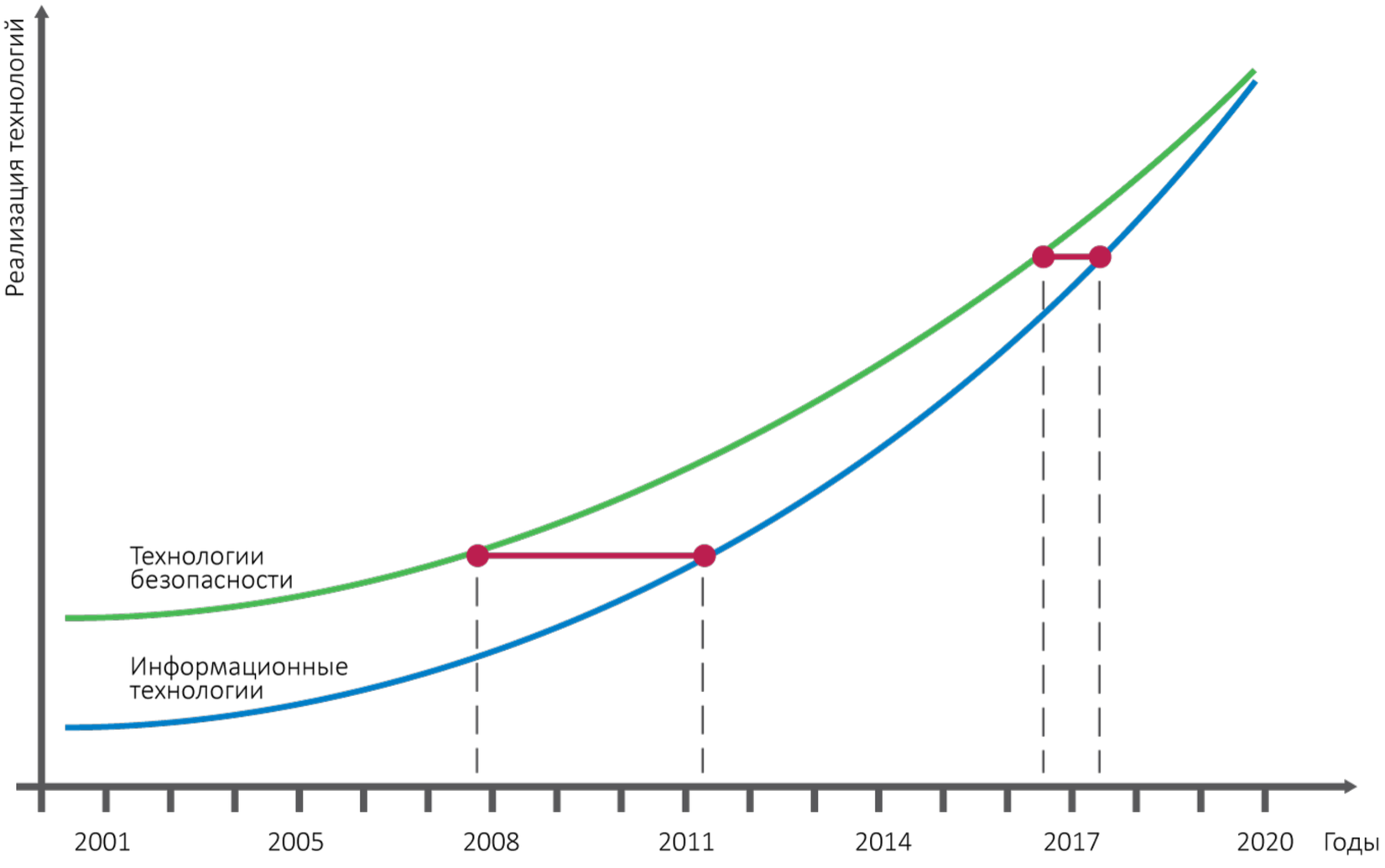


Пояснения к схеме:
* – ITU-T

Связь стандартов ИТ и ИБ



Перспективы стандартизации



Выводы

1. Международные стандарты по ИБ развиваются интенсивно, отставание стандартов по безопасности от появления новых информационных технологий сократилось с 3-5 лет до 1 года.
2. Запаздывание появления стандартов РФ по ИБ от международных стандартов недопустимо велико для развития новых технологий и цифровой экономики.
3. Имеется необходимость появления единого центра управления и комплексного подхода к разработке системы национальных стандартов по доверенным сервисам безопасности.
4. Одним из возможных путей решения указанных проблем может быть передача ряда функций по планированию системы стандартов по доверенным сервисам, технически обеспечивающим юридическую силу электронным документам, саморегулируемой организации при взаимодействии с уполномоченными государственными органами.

Спасибо за внимание!

a.sabanov@aladdin-rd.ru