Проблемы стандартизации в области PKI и ЭП

Алексей Сабанов, д.т.н.,
эксперт ISO/JTC1/SC27/WG5,
член ТК-362, ТК-122, ТК-26,
эксперт РОСЭУ,
профессор кафедры МГТУ им. Баумана,
зам. ген. директора ЗАО "Аладдин Р.Д .",
Академик МАС

Проблемы планирования стандартов

- Отсутствие стратегического планирования с четко обозначенными целями и задачами
- Планы идут от технических комитетов снизу, Росстандарт утверждает представленные ими планы
- Нерешенный вопрос: нужна ли нам сейчас гармонизация с системой международных стандартов?

Аладдин

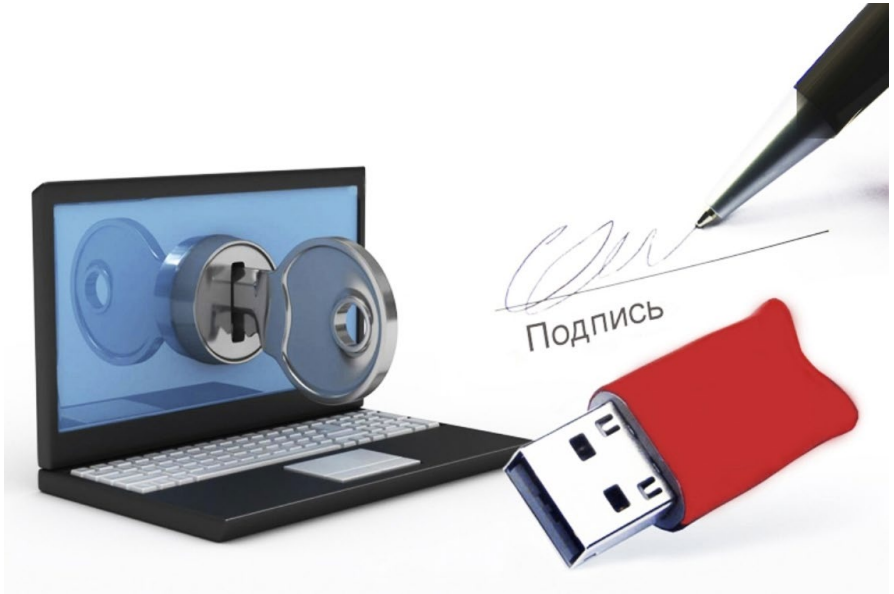
Стандарты на подпись и функцию хэширования

ГОСТ Р 34.10–2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

ISO/IEC 10118-3:2018 IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions.

Ведутся разработки постквантовой подписи и постквантовой выработки общего ключа



Источник: https://tc26.ru/news/

Стандарты на сервисы безопасности PKI в ТК 26

Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе штампов времени (TSP)» 1 редакция. 17.01.2022.

Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации» 1 редакция

Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509. 14.01.2021.

Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML». 27.01.2020.

Источник: https://tc26.ru/discussions/

Аладдин

Стандарты на сервисы безопасности PKI в ТК 362

Приказ от 05 августа 2022 г. N 740-ст Об утверждении национального стандарта ГОСТ Р 70262.1-2022 "Защита информации. Идентификация и аутентификация. Уровни доверия идентификации"

Разработка проекта национального стандарта ГОСТ Р "Защита информации. Идентификация и аутентификаци[illegible]. ***Уровни доверия аутентификации"***				
27	Рассмотрение организациями-членами ТК 362 проекта национального стандарта	апрель 2022 г.	замечания и предложения	Организации-члены ТК 362
29	Доработка проекта национального стандарта по результатам совещания СРГ 1, и направление на согласование с председателем ПК 2	июль 2022 г.	проект национального стандарта, сводка отзывов	АО "Аладдин Р.Д." (организация-разработчик)
34	Направление на издательское редактирование и подготовку к утверждению проекта национального стандарта	декабрь 2022 г.	проект национального стандарта, комплект сопроводительных документов	АО "Аладдин Р.Д." (организация-разработчик)

Приказ от 10 апреля 2020 г. N 59-ст Об утверждении национального стандарта ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация. Общие положения"

Источник: https://fstec.ru/tk-362/

Аладдин

Стандарты на сервисы безопасности PKI в ТК 22

ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции

ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы

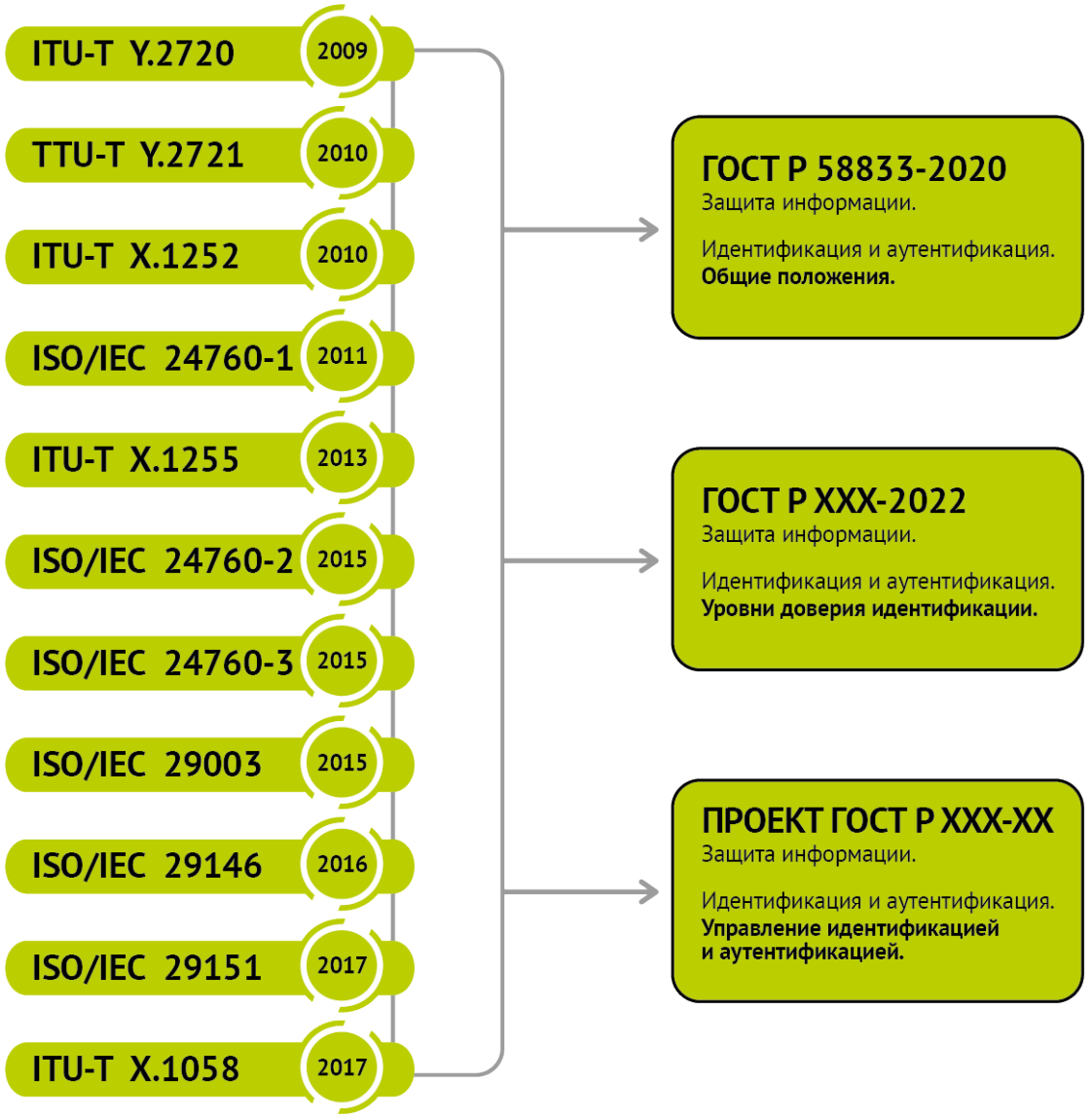
ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом

ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности

ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования

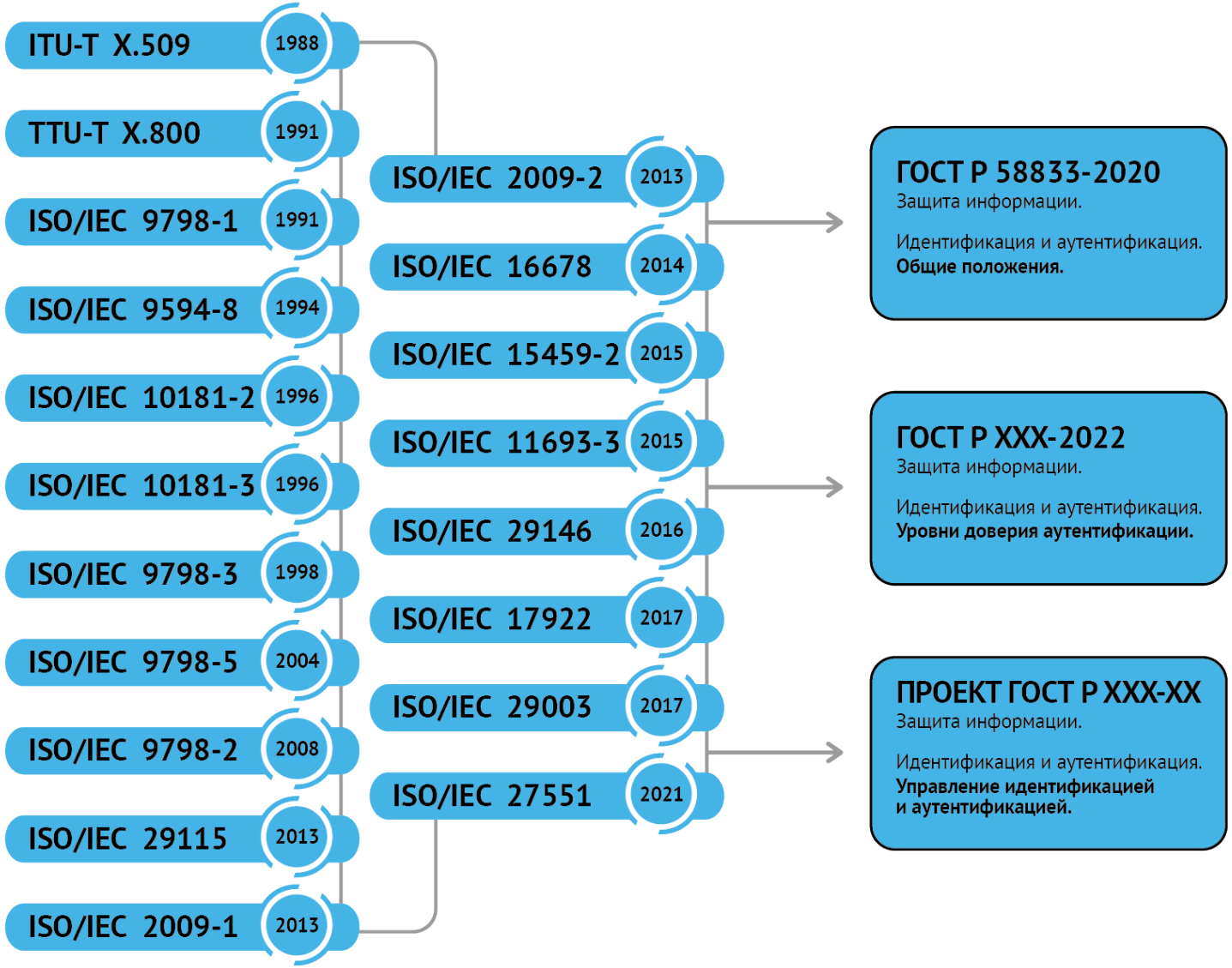
Аладдин

Соотношение международных и **базовых** стандартов системы ГОСТ Р по **идентификации** в задачах управления доступом



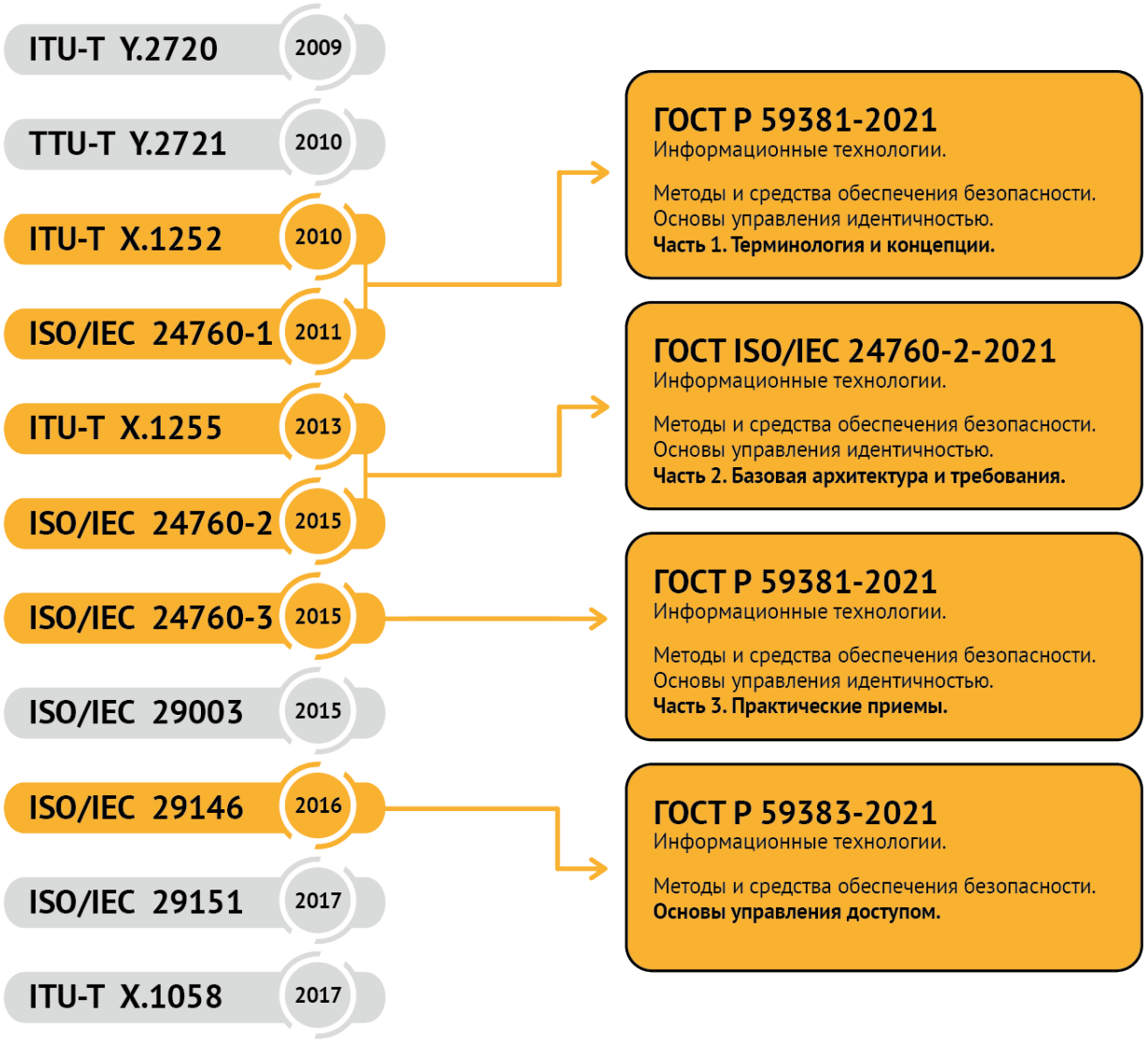
Аладдин

Соотношение международных и **базовых** стандартов системы ГОСТ Р по **аутентификации** в задачах управления доступом



Аладдин

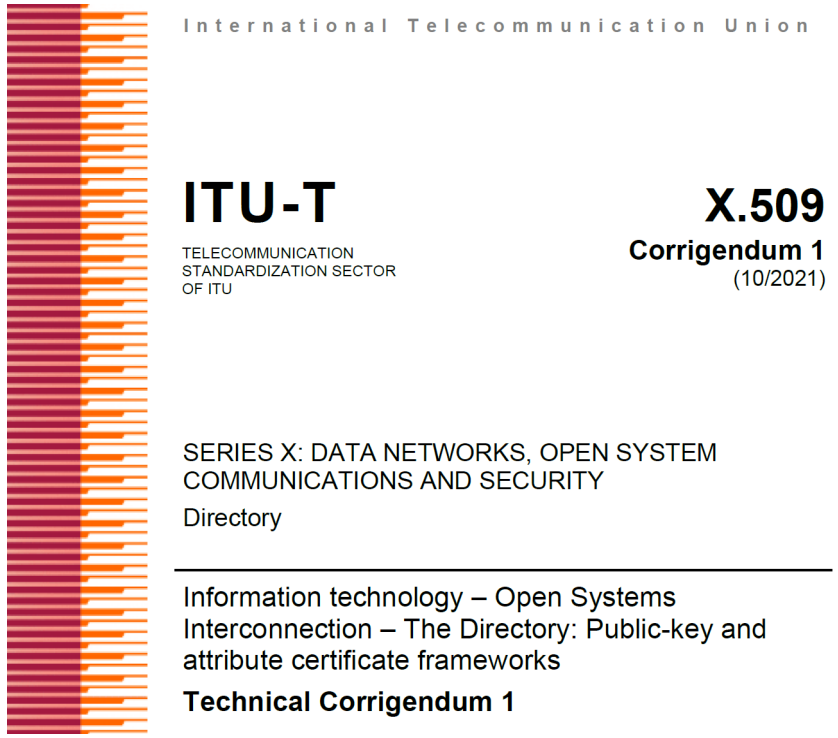
Соотношение международных и **информационных** стандартов системы ГОСТ Р по **идентификации** в задачах управления доступом



Аладдин

Проблемы развития стандартов по тематике PKI

- Нет официального, тем более относительно нового X.509 (сейчас действительна версия 9 от 14.10.19), нет официального перевода стандарта X.842.
- Стандартов по сервисам безопасности на базе PKI ждать еще несколько лет. Сравнение – РБ. Хотя в целом ситуация немного лучше, чем была 5 лет назад.
- Связь принципов Secure by Design и Privacy by Design с развитием стандартов по PKI в РФ



International Telecommunication Union

ITU-T

TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

X.509

Corrigendum 1

(10/2021)

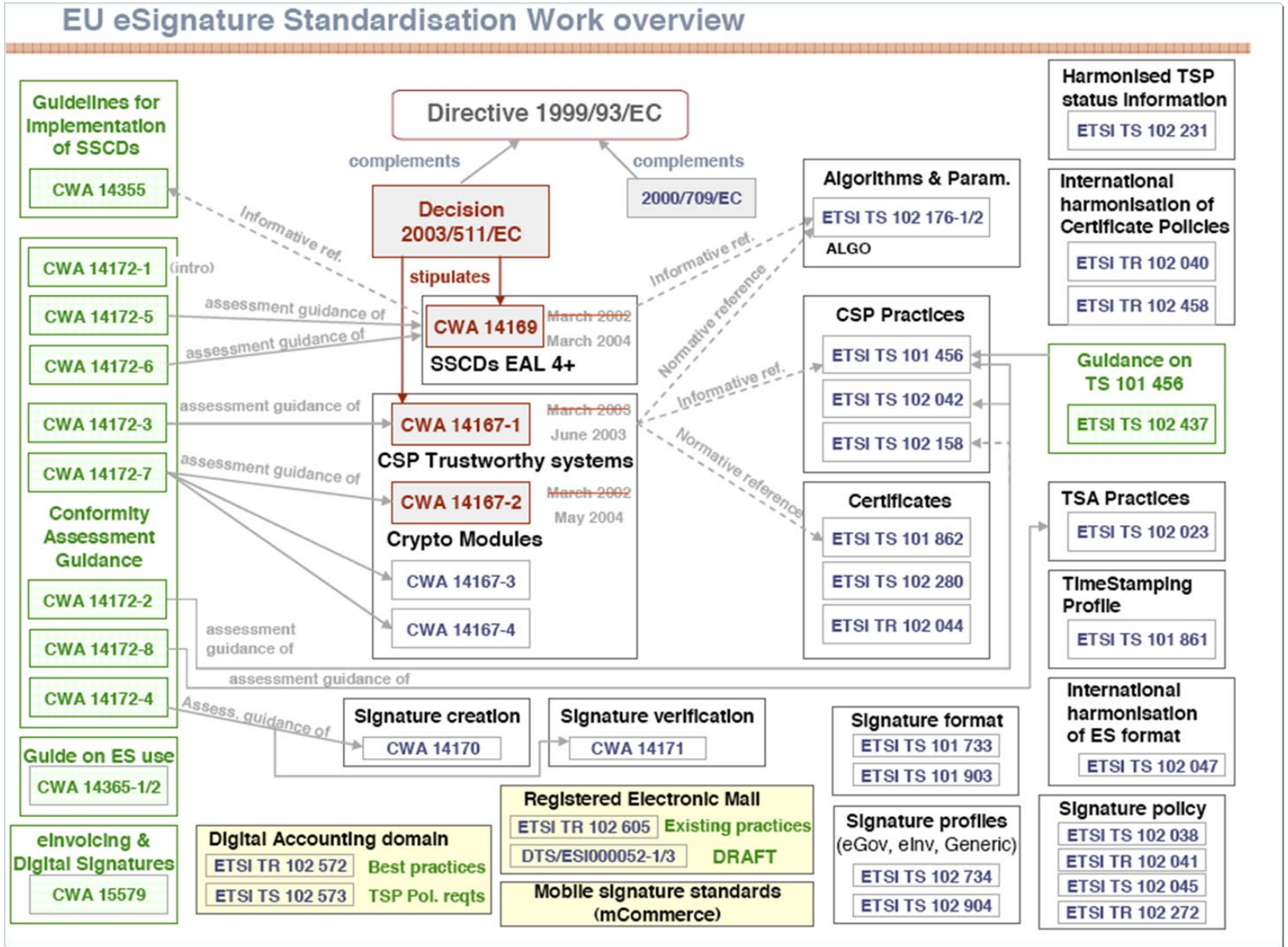
SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Technical Corrigendum 1

Европейские рекомендации – 2003-2005гг.



Спасибо за внимание!

a.sabanov@aladdin-rd.ru
8-985-924-52-09