Проблемы стандартизации в области инфраструктуры открытых ключей и доверенных сервисов

Сабанов Алексей Геннадьевич, д.т.н.,
процессор МГТУ им. Н.Э. Баумана,
главный эксперт АО «НИИАС»,
Р-эксперт ИСО, член ТК 362, ТК 26, ТК 122
академик Международной академии связи

Истоки проблем стандартизации

Согласно стандартам ГОСТ Р 1.1 – 1.7 система национальных стандартов в основном строится на базе систем международных стандартов, де-факто, большей частью на стандартах ISO/IEC.

Международная организация по стандартизации (ISO) была создана в 1947 г. первый стандарт ISO был выпущен в 1951 г. Штаб-квартира находится в Женеве (Швейцария). МЭК основана в 1906 году, с 1948г. находится в Женеве.

ИСО тесно связана с организациями в сфере международной торговли (ВТО, МБРР,…), так как ее деятельность способствует снижению технических барьеров в международной торговле, а также все большему вовлечению развивающихся стран в международную торговлю.

Вопрос: нужна ли нам сегодня и будет ли нужна завтра ориентация на ВТО? Не пора ли подумать о своей стратегии развития систем национальных стандартов, а также межгосударственных стандартов внутри ЕЭС, БРИКС, ШОС?

ISO

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

Каким PKI - стандартам ISO/C1/SC27/WG4 уделяет сейчас внимание?

1	ITU-T X.842 | ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party services	1st ed. 2002 Confirmed in 2018
2	ITU-T X.841 | ISO/IEC 15816	Security information objects for access control	1st ed. 2002 Confirmed in 2018
3	ITU-T X.843 | ISO/IEC 15945	Specification of TTP services to support the application of digital signatures	1st ed. 2021
4	ISO/IEC 27070	Requirements for establishing virtualized roots	
5	ISO/IEC 24760-:2025	A framework for identity management. Part 4: authenticators, credentials and authentication	WD stage
6	ISO/IEC 27099	Public key infrastructure – Practices and policy framework	1st ed. 2022

SC 27
Information Security, Cybersecurity and Privacy Protection

WG 4 SECURITY CONTROLS AND SERVICES

- Convener: Johann AMSENGA, ILNAS (LU)
- Convener-support: François LOREK, AFNOR (FR)

SCOPE

Aspects related to security controls and services, emphasizing standards for IT security and its application to the security of products and systems in information systems, as well as the security in the lifecycle of such products and systems.

The topics covered include:

- ICT security operations (for example readiness, continuity, incident and event management, investigation);
- Information lifecycle (for example creation, processing, storage, transmission and disposal);
- Organizational processes (for example design, acquisition, development and supply);
- Security aspects of Trusted services (for example in the provision, operation and management of these services);
- Cloud, internet and cybersecurity related technologies and architectures (for example network, virtualization, storage).

Каким стандартам ISO/C1/SC27/WG5 уделяет сейчас максимальное внимание?

1	ISO/IEC 27018	Code of practice for PII protection in public clouds acting as PII processors
2	ISO/IEC 27091	Cybersecurity and privacy – Artificial intelligence – Privacy protection
3	ISO/IEC 27550	Privacy engineering for system life cycle processes
4	ISO/IEC 27551	Requirements for attribute-based unlinkable entity authentication
5	ISO/IEC 27553	Security and privacy requirements for authentication using biometrics on mobile devices – Part 1, 2
6	ISO/IEC 27554	Application of ISO 31000 for assessment of identity-related risk
7	ISO/IEC 27555	Guidelines on personally identifiable information deletion
8	ISO/IEC 27556	User-centric privacy preferences management framework
9	ISO/IEC 27557	Application of ISO 31000:2018 for organizational privacy risk management
10	ISO/IEC 27559	Privacy enhancing data de-identification framework
11	ISO/IEC 27560	Consent record information structure (PII Principals' or data)
12	ISO/IEC 27561	Privacy operationalisation model and method for engineering (POMME)
13	ISO/IEC 27562	Privacy guidelines for fintech services
14	ISO/IEC 27563	Security and privacy in artificial intelligence use cases
15	ISO/IEC 27565	Guidance on privacy preservation based on zero knowledge proofs
16	ISO/IEC 27566	Age assurance systems – Framework
17	ISO/IEC 27570	Privacy guidelines for smart cities
18	ISO/IEC 27552	Extension to 27001 and 27002 for privacy in formation management – Requirements, guidelines
19	ISO/IEC 29003	Identity proofing
20	ISO/IEC 29101	Privacy architecture framework
21	ISO/IEC 29115	Entity authentication assurance framework
22	ISO/IEC 29134	Guidelines for privacy impact assessment
23	ISO/IEC 29146	A framework for access management
24	ISO/IEC 29151	Code of practice for personally identifiable information protection
25	ISO/IEC 29184	Online privacy notices and consent
26	ISO/IEC 29190	Privacy capability assessment model
27	ISO/IEC 29191	Requirements for partially anonymous, partially unlinkable authentication

Более 85% стандартов посвящено защите неприкосновенности частной жизни в цифровом мире

SC 27
Information Security, Cybersecurity and Privacy Protection

The scope of SC 27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personaldata. This includes:

- Identification of requirements for and development of future standards and guidelines in these areas. For example
  - In the area of Identity Management, topics such as:
    - A framework for Identity management;
    - Anonymity and pseudonymity;
    - Credentials and attributes;
    - Entity assurance and Identity proofing;
    - Access management;
  - In the area of Privacy, topics such as:
    - A privacyframework;
    - A privacy reference architecture;
    - Privacy infrastructures;
    - Privacy impact assessment;
    - Specific Privacy Enhancing Technologies (PETs);
    - Privacy engineering;
  - In the area of Biometrics, topics such as:
    - Protection of biometric data;
    - Authentication techniques.

Общие проблемы планирования и разработки стандартов в области ИБ

- Отсутствие стратегического планирования системы национальных стандартов.
- Система планирования построена снизу, от технических комитетов. Росстандарт утверждает представленные ими планы. Исключение составляют поручения министерств.
- Сегодня отсутствуют требования к квалификации разработчиков стандартов. Каждый ТК решает этот вопрос самостоятельно. Создать НТС при каждом ТК?
- Дискуссионный вопрос: так ли нам сейчас нужна навязываемая гармонизация с международными стандартами? Значительная часть международных стандартов нужна как информация о том, как «они это делают».
- Де-факто более 80% стандартов в области ИТ и ИБ имеют статус IDT. При наличии своей стратегии развития мы смогли бы на основе неэквивалентных стандартов (включающих в себя суть нескольких международных) догнать развитие мировых за 3-5 лет и двигаться по своей траектории параллельно с МСЭ и ИСО/МЭК.

Основные стандарты PKI

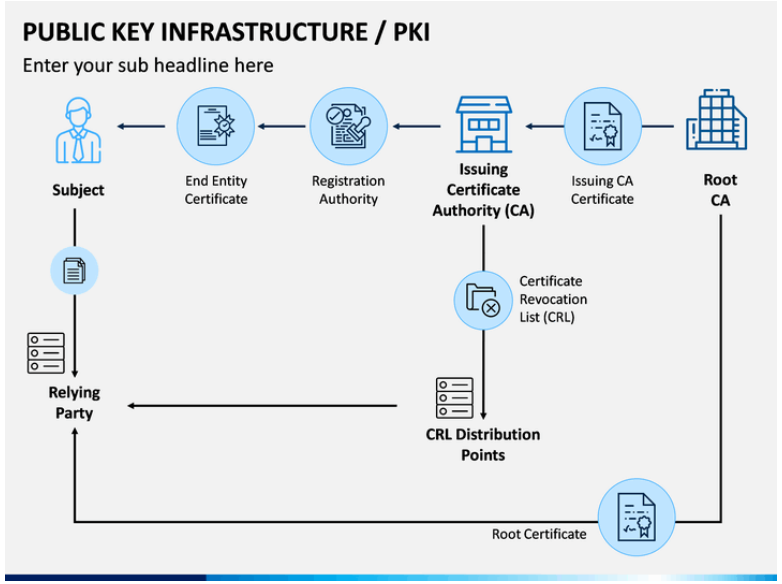
- Отсутствие официального перевода или стандарта ITU-T X.509 The Directory: Public-key and attribute certificate frameworks. (На сайте перевод: «Справочник: Системы сертификатов открытых ключей и атрибутов») в системе национальных стандартов.
- Отсутствие официального перевода стандарта ITU-T X.842:2000 Guidelines for the use and management of trusted third party services (на сайте ITU по-русски написано: «Руководящие принципы использования надежных сторонних служб и управления ими») в системе национальных стандартов.
- Стандарты по сервисам безопасности развиваются в разных ТК без централизованного планирования. Нет привязки новых стандартов к системе управления ИБ и созданию системы доверия в развивающемся цифровом пространстве.

Версии ITU-T Rec. X.509

INTERNATIONAL STANDARD ISO/IEC 9594-8 RECOMMENDATION ITU-T X.509
Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
History
Edition Recommendation Approval Study Group Unique ID*
1.0 ITU-T X.509 1988-11-25 11.1002/1000/2999
2.0 ITU-T X.509 1993-11-16 7 11.1002/1000/3000
3.0 ITU-T X.509 1997-08-09 7 11.1002/1000/4123
3.1 ITU-T X.509 (1997) Technical Cor. 1 2000-03-31 7 11.1002/1000/5033
3.2 ITU-T X.509 (1997) Technical Cor. 2 2001-02-02 7 11.1002/1000/5311
3.3 ITU-T X.509 (1997) Technical Cor. 3 2001-10-29 7 11.1002/1000/5559
3.4 ITU-T X.509 (1997) Technical Cor. 4 2002-04-13 17 11.1002/1000/6025
3.5 ITU-T X.509 (1997) Technical Cor. 5 2003-02-13 17 11.1002/1000/6236
3.6 ITU-T X.509 (1997) Technical Cor. 6 2004-04-29 17 11.1002/1000/7285
4.0 ITU-T X.509 2000-03-31 7 11.1002/1000/5034
4.1 ITU-T X.509 (2000) Technical Cor. 1 2001-10-29 7 11.1002/1000/5560
4.2 ITU-T X.509 (2000) Technical Cor. 2 2002-04-13 17 11.1002/1000/6026
4.3 ITU-T X.509 (2000) Technical Cor. 3 2004-04-29 17 11.1002/1000/7284
4.4 ITU-T X.509 (2000) Technical Cor. 4 2007-01-13 17 11.1002/1000/8637
5.0 ITU-T X.509 2005-08-29 17 11.1002/1000/8501
5.1 ITU-T X.509 (2005) Cor. 1 2007-01-13 17 11.1002/1000/9051
5.2 ITU-T X.509 (2005) Cor. 2 2008-11-13 17 11.1002/1000/9591
5.3 ITU-T X.509 (2005) Cor. 3 2011-02-13 17 11.1002/1000/11042
5.4 ITU-T X.509 (2005) Cor. 4 2012-04-13 17 11.1002/1000/11577
6.0 ITU-T X.509 2008-11-13 17 11.1002/1000/9590
6.1 ITU-T X.509 (2008) Cor. 1 2011-02-13 17 11.1002/1000/11043
6.2 ITU-T X.509 (2008) Cor. 2 2012-04-13 17 11.1002/1000/11578
6.3 ITU-T X.509 (2008) Cor. 3 2012-10-14 17 11.1002/1000/11736
7.0 ITU-T X.509 2012-10-14 17 11.1002/1000/11735
7.1 ITU-T X.509 (2012) Cor. 1 2015-05-29 17 11.1002/1000/12474
7.2 ITU-T X.509 (2012) Cor. 2 2016-04-29 17 11.1002/1000/12844
7.3 ITU-T X.509 (2012) Cor. 3 2016-10-14 17 11.1002/1000/13032
8.0 ITU-T X.509 2016-10-14 17 11.1002/1000/13031
9.0 ITU-T X.509 2019-10-14 17 11.1002/1000/14033
Cor 1 (10/2021)

Проблемы стандартизации вокруг PKI

- PKI по определению является инфраструктурой доверия к открытым ключам, содержащимся в сертификатах X.509
- Основные международные стандарты PKI «не прописаны» в РФ
- В развитии нормативно-правовой базы имеется явный перекос проблем нормативного регулирования PKI в сторону ЭП
- ЭП – всего лишь один из доверенных сервисов на базе PKI. Еще имеются сервисы:
  - идентификация,
  - аутентификация,
  - проверка полномочий,
  - штампы времени,
  - валидация,
  - гарантированная доставка документов и сообщений.



Со стандартами вокруг PKI все не так плохо. Пример ТК 26

- Международные стандарты с участием российских экспертов:
  - ISO/IEC 18014-2:2021 Information technology - Security techniques - Time-stamping services - Part 2: Mechanisms producing independent tokens;
  - ISO/IEC 13888-2 Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques;
  - ISO/IEC 13888-1:2020 Information technology - Security techniques - Non-repudiation - Part 1: General;
- Национальные стандарты:
  - ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012
- Рекомендации:
  - Р 1323565.1044-2022 Использование российских криптографических алгоритмов в протоколе штампов времени (TSP);
  - Р 1323565.1043-2022 Контрольные примеры использования российских криптографических алгоритмов в протоколе безопасности транспортного уровня;
  - Р 1323565.10023-2022 Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509;
  - Р 1323565.1033-2020 Использование российских криптографических алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML.

Со стандартами вокруг PKI все не так плохо. Пример ТК 362

- Утвержденные стандарты:
  - ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения;
  - ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации.
- Стандарты на разных стадиях утверждения:
  - ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации;
  - ГОСТ Р Защита информации. Идентификация и аутентификация. Управление идентификацией и аутентификацией;
  - ГОСТ Р Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости процессов идентификации и аутентификации;
  - ГОСТ Р Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией.

Выводы

1. Разработка международных стандартов в области PKI и сервисов на основе PKI традиционна, но на сегодняшнем этапе развития имеет тенденцию к концентрации на защите неприкосновенности частной жизни в цифровом мире.

2. По инициативе «снизу» (от Технических комитетов) в области PKI и доверенных сервисов на основе PKI разработано и находится в разработке существенное количество национальных стандартов, однако для полноты охвата и сокращения сроков появления необходимых потребителям стандартов требуется централизованное управление процессами планирования и разработки стандартов системы ГОСТ Р.

3. Планирование разработки стандартов в области PKI и сервисов на основе PKI предлагается организовать «сверху» на основе прозрачной и понятной всем стратегии. Также с целью сокращения сроков появления необходимых стандартов предлагается провести небольшую коррекцию системы планирования стандартизации в рассматриваемой области. Идентичные стандарты нужны, однако значительная часть их содержания может быть использована как информационная, а не нормативная. Для сокращения отставания от международной системы стандартов предлагается отдавать предпочтение неэквивалентным стандартам, объединяющим в себе не один, а несколько стандартов по заданной тематике.

4. Национальные стандарты должны способствовать созданию системы управления доверием в цифровом мире и улучшению качества продуктов (СЗИ, СКЗИ) для поддержки сервисов безопасности на базе PKI.

Спасибо за внимание!

Сабанов Алексей Геннадьевич

asabanov@mail.ru