Развитие базовых стандартов криптографической защиты информации в России и за рубежом

Лунин Анатолий Васильевич
ОАО «ИнфоТеКС»
Секретариат Технического комитета
по стандартизации (ТК26)
«Криптографическая защита информации»
GOST R Expert

Национальная система стандартизации

(организация)

GOST R

28 - 31 марта 2012 г.

ТК 26 ГОСТР

GOST R

Росстандарт

Федеральное агентство по техническому регулированию и метрологии

Действует на основании Положения о Росстандарте, утвержденного Постановлением Правительства Российской Федерации от 17 июня 2004 г. № 294

ТК 26 ГОСТР

GOST R

Росстандарт

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)

Создан приказом Росстандарта №3825дсп от 28 декабря 2007 г.

ТК 26

Председатель – Кузьмин А.С.

Зам. председателя – Качалин И.Ф.

Зам. председателя - Секретарь – Чапчаев А.А.

Секретариат – ОАО «ИнфоТеКС»

Росстандарт

В ТК 26 представлены органы и организации, к компетенции которых отнесена защита информации с использованием криптографических методов, имеющих опыт в организации разработок образцов шифровальных (криптографических) средств

(На 01.01.2012 – более 50 органов и организаций-членов ТК26, в т.ч. и ОГВ)

Региональная система стандартизации

(организация)

Межгосударственный Совет
по стандартизации, метрологии и сертификации

Об организации

Межгосударственный совет по стандартизации, метрологии и сертификации (МГС) Содружества Независимых Государств (СНГ) является межправительственным органом СНГ по формированию и проведению согласованной политики по стандартизации, метрологии и сертификации.

Международная система стандартизации

(организация)

ISO International Organization for Standardization

ISO (International Organization for Standardization)
ИСО (Международная организация по стандартизации)

Объединяет национальные системы стандартизации 163 стран.
Каждая стран представлена одним голосом.
Центральный Секретариат, координирующий деятельность в ИСО, расположен в Женеве, Швейцария.

Место в иерархии ИСО

JTC 1 - Information technology

JTC 1/SC 27 - IT Security techniques

JTC 1/SC 27/WG 2 - Cryptography and security mechanisms

Национальная система стандартизации

(практика)

GOST R

GOST R

Российские (национальные) криптографические стандарты

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

International Organization for Standardization

ГОСТ Р ИСО/МЭК

GOST R

Пример неудачной попытки гармонизации

ГОСТ Р ИСО/МЭК 10116-**93**. Информационная технология. Режимы работы для алгоритма n-разрядного блочного шифрования (1 ред.)

ISO/IEC 10116: **2006**, Modes of operation for an n-bit block cipher (3rd edition)

infotecs®

ТК 26 ГОСТР

GOST R

ГОСТ Р 34.11-20__
(проект, окончательная редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

infotecs®

ТК 26 ГОСТР

GOST R

ГОСТ Р 34.10-20__
(проект, окончательная редакция)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

infotecs®

ТК 26 ГОСТР

Региональная система стандартизации

(практика)

Межгосударственный Совет
по стандартизации, метрологии и сертификации

Международные (региональные) криптографические стандарты

- ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования;
- ГОСТ 34.310-2002. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
- ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования.

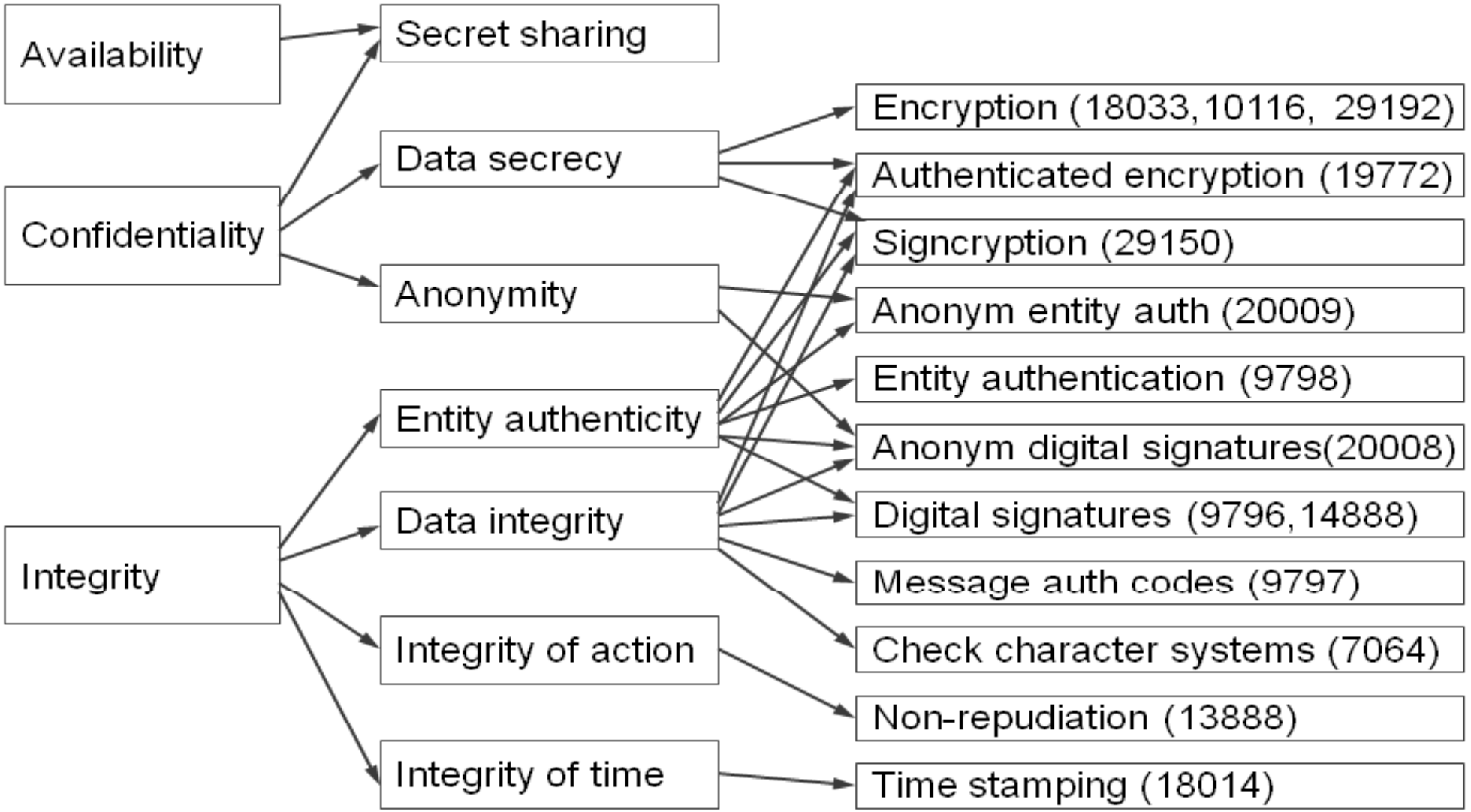
infotecs®

ТК 26 ГОСТР

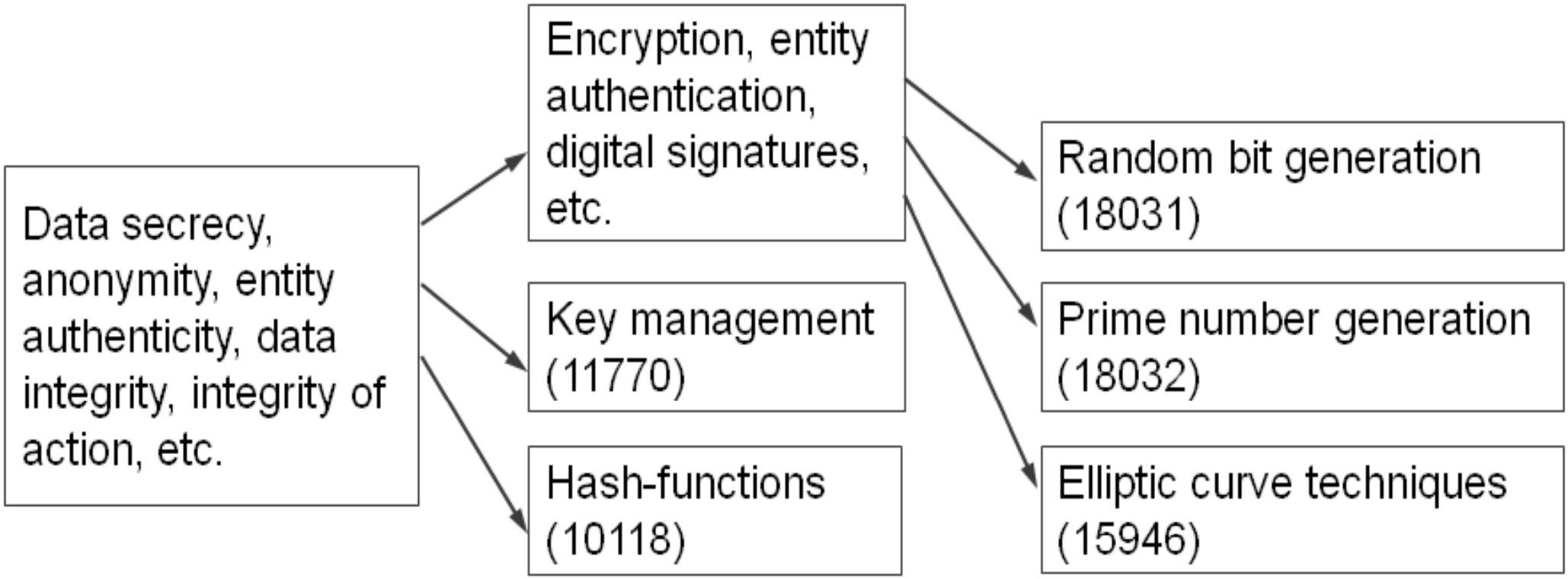
Международная система стандартизации

(практика)

ISO International Organization for Standardization



Relationships between the objectives and the 14 mechanism standards



Supporting and component mechanism standards

infotecs®

ТК 26 ГОСТР

International Organization for Standardization

ISO/IEC 14888-3. Information technology – Security techniques - Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms. Amendment 1. Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm

(Принят в июне 2010 г.)

ISO International Organization for Standardization

GOST R

Несостоявшийся проект

Подготовка дополнения к стандарту *18033-3:2005 «Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers»*

на основе *ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»*

Проект внесен в ИСО в мае 2009 года и открыт в октябре 2009 года.

Закрыт после голосования в октябре 2011 года.

ISO International Organization for Standardization

GOST R

Несостоявшийся проект

Подготовка дополнения к стандарту *10118-3:2004 «Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions»*

на основе российского стандарта ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»

Проект был внесен в ИСО в мае 2009 года

infotecs®

ТК 26 ГОСТР

Неправительственные системы стандартизации

RSA
The Security Division of EMC

OASIS
Advancing open standards for the information society

RSA
The Security Division of EMC

Расширение стандарта PKCS#11

Расширение стандарта *RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki)* российскими криптографическими алгоритмами.

В 2009 году был опубликован проект PKCS #11 v2.30, включающий ГОСТ 28147-89 и другие российские алгоритмы.

infotecs®

ТК 26 ГОСТР

RSA
The Security Division of EMC

Расширение стандарта PKCS#12

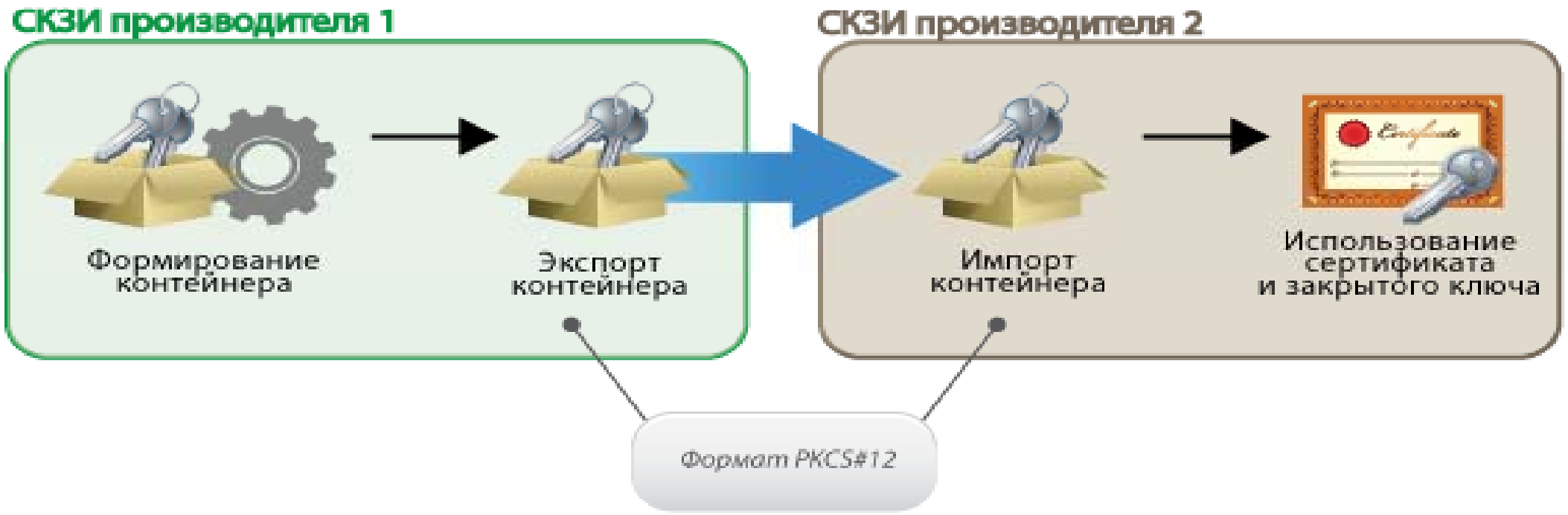
Использование стандарта RSA Security Inc. PKCS #12 Personal Information Exchange Syntax Standard совместно с российскими криптографическими алгоритмами.

Позволяет создать т.н. транспортный контейнер ключей, например, для организации получения госуслуг.

Использование стандарта PKCS#12

Регион 1 (Ведомство 1)

Регион 2 1 (Ведомство 2)



infotecs®

ТК 26 ГОСТР

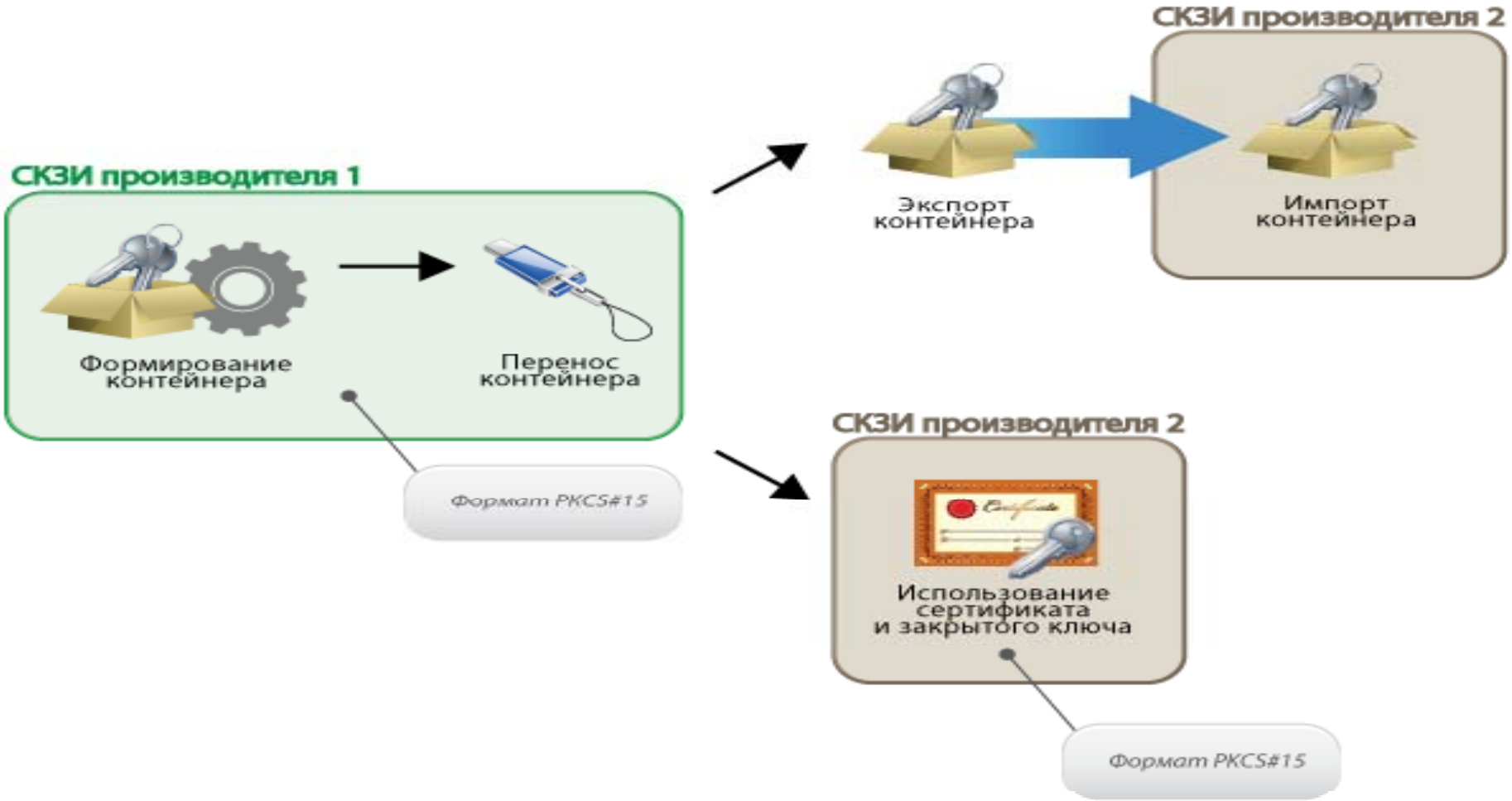
RSA
The Security Division of EMC

Расширение стандарта PKCS#15

Использование стандарта RSA Security Inc. PKCS #15 Cryptographic Token Information Format Standard совместно с российскими криптографическими алгоритмами.

Позволяет создать т.н. контейнер хранения ключей пользователя, например, для получения госуслуг.

Расширение стандарта PKCS#15



Стандарты RSA перейдут в стандарты OASIS?

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium.
The consortium has more than 5,000 participants representing over 600 organizations and individual members in 100 countries.
The Consortium hosts two of the most widely respected information portals on XML and Web services standards, Cover Pages and XML.org.
OASIS Member Sections include AMQP, Blue, CGM Open, eGov, Emergency, IDtrust, LegalXML, Open CSA, and WS-I.

Выводы:

- определение базового набора криптографических механизмов российской разработки, согласованных по функционалу и параметрам со стандартами ИСО;
- определение и принятие части криптографических стандартов ИСО в качестве национальных стандартов (не оказывающих существенного влияния на уровень ИБ);
- отсев части стандартов, как не имеющих спроса в настоящее время
- исследование оставшихся стандартов на соответствие российским треованиям.

Выводы:

- координация работ технических комитетов по стандартизации в области ИБ Росстандарта друг с другом и с другими организациями по стандартизации (в первую очередь, с МСЭ-Т) с целью подготовки и согласования криптографических механизмов для конкретных приложений, таких как оказание государственных услуг, использование интеллектуальных карт, управления правами, финансовыми услугами и др.

Благодарю за внимание!

Лунин Анатолий Васильевич
ОАО «ИнфоТеКС»
Секретариат технического комитета по стандартизации
«Криптографическая защита информации»
Тел. +7 (495) 737 61 92
tc26@infotecs.ru
www.tc26.ru