

Стандартизация криптографических методов защиты информации в России и за рубежом

Лунин Анатолий Васильевич

*Секретариат технического комитета по стандартизации
«Криптографическая защита информации»
ОАО «ИнфоТеКС»*

Национальная система стандартизации



29-30 января 2009 г.

ИНФОФОРУМ-11

Ростехрегулирование



*Федеральное агентство по техническому
регулированию и метрологии*

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

Ростехрегулирование



Среди его основных функций:

- реализация функций национального органа по стандартизации;
- осуществление госконтроля (надзора) за соблюдением обязательных требований стандартов;
- оказание государственных услуг в сфере стандартизации.

Ростехрегулирование



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

Создан приказом Ростехрегулирования
28 декабря 2007 г.

Ростехрегулирование



Основная цель ТК26 – организация и проведение работ в области национальной, региональной и международной стандартизации шифровальных (криптографических) средств защиты информации, а также технических решений по их применению в информационно-телекоммуникационных системах и системах шифрованной, засекреченной и иных видов специальной связи.



Ростехрегулирование

ТК26 уполномочен рассматривать вопросы стандартизации продукции и услуг, относящиеся к:

- методам шифрования (криптографического преобразования) информации;
- способам их реализации;
- методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись.

Ростехрегулирование



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

ГОСТ Р



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.

ГОСТ Р



ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования:

- блочный шифр;
- режимы блочного шифрования;
- шифр гаммирования;
- имитозащита.

ГОСТ Р



Российские (национальные) криптографические стандарты

ГОСТ Р 34.10-2001. Информационная технология.

Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи:

- формирования и проверки электронной цифровой подписи;
- выработка пар открытого и закрытого ключей.

ГОСТ Р



Российские (национальные) криптографические стандарты

Пример неудачной попытки гармонизации

ГОСТ Р ИСО/МЭК 10116-93. Информационная технология.
Режимы работы для алгоритма n-разрядного блочного
шифрования

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

Региональная система стандартизации



29-30 января 2009 г.

ИНФОФОРУМ-11



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.



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.

Международная система стандартизации



29-30 января 2009 г.

ИНФОФОРУМ-11



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

Объединяет национальные системы стандартизации 157 стран.

Каждая страна 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



Основные результаты JTC 1/SC 27/WG 2

Стандартизация алгоритмов шифрования

“Encryption algorithms” (ISO/IEC 18033)

Part 1 (ISO/IEC 18033-1:2005) - определяет основные термины и свойства для симметричных и асимметричных шифров.



Основные результаты JTC 1/SC 27/WG 2

Стандартизация алгоритмов шифрования

“Encryption algorithms” (ISO/IEC 18033)

Part 2 (ISO/IEC 18033-2:2006) – определяет шесть асимметричных алгоритмов: ECIES-KEM, PSEC-KEM, ACE-KEM, RSA-KEM, RSAES и HIME(R).



Основные результаты JTC 1/SC 27/WG 2

Стандартизация алгоритмов шифрования

“Encryption algorithms” (ISO/IEC 18033)

Part 3 (ISO/IEC 18033-3:2005) – определяет алгоритмы блочных шифров с размерами блоков 64 и 128 бит, а именно:

TDEA, MISTY1 и CAST-128 (с размерами блоков 64 бит),
AES, Camellia and SEED (с размерами блоков 128 бит).



Основные результаты JTC 1/SC 27/WG 2

Стандартизация алгоритмов шифрования

“Encryption algorithms” (ISO/IEC 18033)

Part 4 (ISO/IEC 18033-4:2005) определяет шифры гаммирования (поточковые шифры), а именно:

MUGI и SNOW 2.0, а также MULTI-S01



Основные результаты JTC 1/SC 27/WG 2

Стандарты для выработки случайных последовательностей и простых чисел

“Random bit generation” (ISO/IEC 18031:2005)

“Prime number generation” (ISO/IEC 18032:2005)



Основные результаты JTC 1/SC 27/WG 2

“Digital signature giving message recovery” (ISO/IEC 9796)

“Digital signature with appendix” (ISO/IEC 14888)

“Message authentication codes (MACs)” (ISO/IEC 9797)

“Authenticated encryption” (ISO/IEC 19772)

“Hash-functions” (ISO/IEC 10118)

“Key management” (ISO/IEC 11770)

...



ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

Компанией «ИнфоТеКС» было предложено подготовить дополнение к стандарту **ISO/IEC 14888-3:2006(E)** «*Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*» на основе **ГОСТ 34.10-2001** «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»



ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

- К 15 июля 2007 г. первая редакция дополнения была направлена в ПК 27**
- В конце 2008 г. доработанная редакция передана в национальные органы по стандартизации в качестве проекты ПК27.**
- В январе 2009 объявлено голосование.**



ПК 27 СТК 1 ИСО/МЭК (ISO/IEC JTC 1 SC 27)

ISO/IEC 14888-3/Amd.1 Information technology – Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms. Amendment 1

History/Target Dates

(WD 2007-11)

(PDAM 2008-11)

(FDAM 2009-11)

(AMD 2010-05)

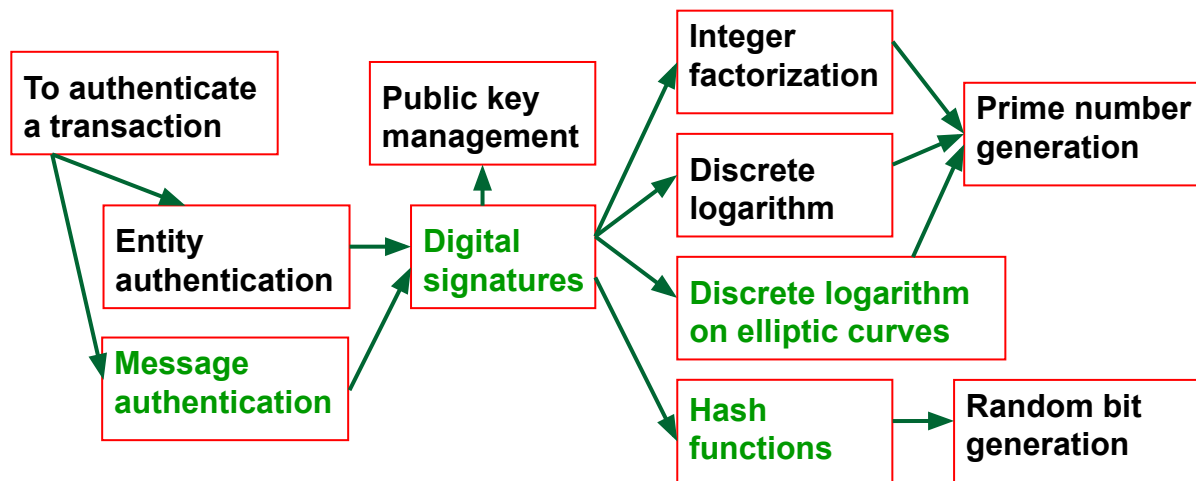


Fig 1 Model combination of standards for authentication of commercial transaction

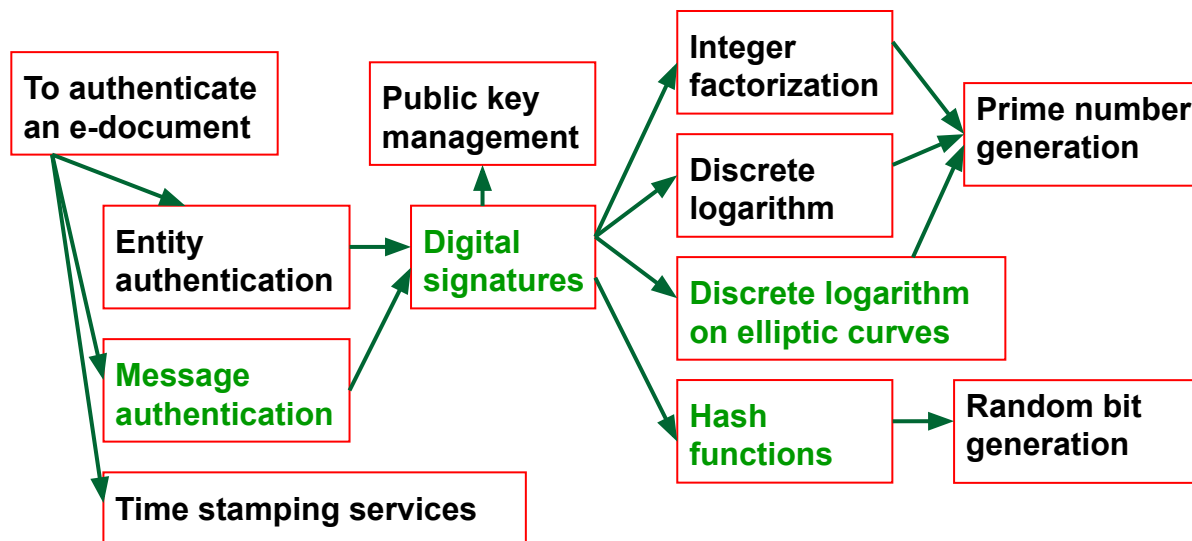


Fig. 2 Model combination of standards for authentication of e-documents

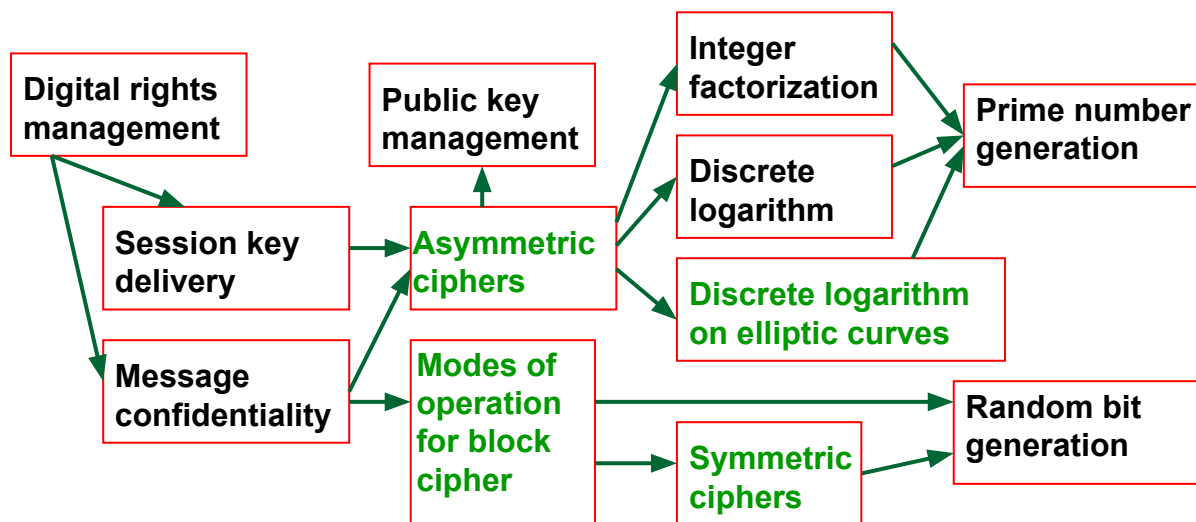


Fig. 3 Model combination of standards for digital rights management



Перспективы JTC 1/SC 27/WG 2

- Улучшение применимости криптографических стандартов, т.е.:
 - Критерии выбора алгоритма
 - Формальное доказательство и проверка
 - Алгоритмы для низкопотребляющей элементной базы
- Реорганизация и расширение стандартов, связанных с ЭЦП, т.е.:
 - Реорганизация стандартов 15946, 9796, 14888 и 11770
 - Signcryption (одновременное шифрование и аутентификация сообщений)
- Активный пересмотр существующих криптографических стандартов,
 - Исключение слабых схем;
 - Включение новых и более эффективных схем.

Перспективы ТК26



- Актуализация фонда криптографических стандартов (исключение, пересмотр, новые стандарты), в т.ч. работы по внесению изменений и дополнений в действующий национальный стандарт ГОСТ 28147-89
- Разработка национального стандарта для TPM с российскими алгоритмами и протоколами криптографической защиты информации
- Стандартизация процедур криптографической защиты информации в составе микропрограммных устройств с российскими алгоритмами и протоколами криптографической защиты информации
- Стандартизация PKCS № 11 с российскими алгоритмами и протоколами криптографической защиты информации
- Стандартизация реализации функций криптографической защиты информации в рамках российской ИОК
- Стандартизация криптографической защиты персональных данных

Вопросы?

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