infotecs®

ТК 26 ГОСТР

GOST R

# Процессы стандартизации криптографических методов защиты информации на национальном и международном уровне

Сериков Игорь Анатольевич

18 сентября 2012 г.

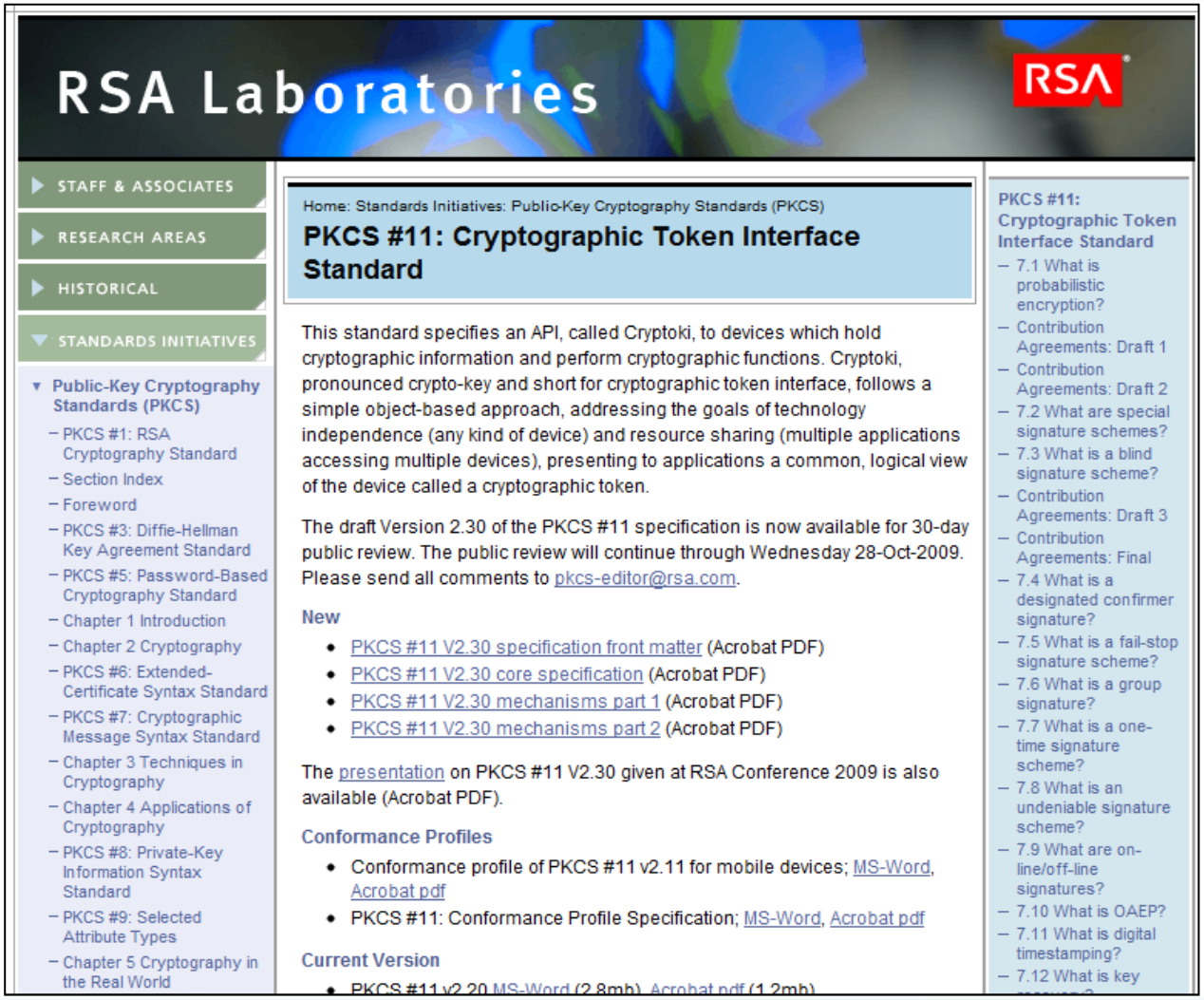
Конференция
«PKI-Forum Россия 2012»

**Семейство RFC определяющих использование российских криптографических алгоритмов в PKI** (Public Key Infrastructure)**:**

**RFC 4490** «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)»

**RFC 4491** «Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile»

**RFC 4357** «Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms»



RSA Laboratories

RSA

STAFF & ASSOCIATES

RESEARCH AREAS

HISTORICAL

STANDARDS INITIATIVES

Public-Key Cryptography Standards (PKCS)

- PKCS #1: RSA Cryptography Standard
- Section Index
- Foreword
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- Chapter 1 Introduction
- Chapter 2 Cryptography
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- Chapter 3 Techniques in Cryptography
- Chapter 4 Applications of Cryptography
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- Chapter 5 Cryptography in the Real World

Home: Standards Initiatives: Public-Key Cryptography Standards (PKCS)

## PKCS #11: Cryptographic Token Interface Standard

This standard specifies an API, called Cryptoki, to devices which hold cryptographic information and perform cryptographic functions. Cryptoki, pronounced crypto-key and short for cryptographic token interface, follows a simple object-based approach, addressing the goals of technology independence (any kind of device) and resource sharing (multiple applications accessing multiple devices), presenting to applications a common, logical view of the device called a cryptographic token.

The draft Version 2.30 of the PKCS #11 specification is now available for 30-day public review. The public review will continue through Wednesday 28-Oct-2009. Please send all comments to pkcs-editor@rsa.com.

**New**

- PKCS #11 V2.30 specification front matter (Acrobat PDF)
- PKCS #11 V2.30 core specification (Acrobat PDF)
- PKCS #11 V2.30 mechanisms part 1 (Acrobat PDF)
- PKCS #11 V2.30 mechanisms part 2 (Acrobat PDF)

The presentation on PKCS #11 V2.30 given at RSA Conference 2009 is also available (Acrobat PDF).

**Conformance Profiles**

- Conformance profile of PKCS #11 v2.11 for mobile devices; MS-Word, Acrobat pdf
- PKCS #11: Conformance Profile Specification; MS-Word, Acrobat pdf

**Current Version**

- PKCS #11 v2.20 MS-Word (2.8mb), Acrobat pdf (1.2mb)

PKCS #11: Cryptographic Token Interface Standard

- 7.1 What is probabilistic encryption?
- Contribution Agreements: Draft 1
- Contribution Agreements: Draft 2
- 7.2 What are special signature schemes?
- 7.3 What is a blind signature scheme?
- Contribution Agreements: Draft 3
- Contribution Agreements: Final
- 7.4 What is a designated confirmer signature?
- 7.5 What is a fail-stop signature scheme?
- 7.6 What is a group signature?
- 7.7 What is a one-time signature scheme?
- 7.8 What is an undeniable signature scheme?
- 7.9 What are on-line/off-line signatures?
- 7.10 What is OAEP?
- 7.11 What is digital timestamping?
- 7.12 What is key

GOST R

infotecs®

ТК 26 ГОСТ Р

RSA LABORATORIES

GOST R

**PKCS #11 Mechanisms v2.30: Cryptoki – Draft 7**

*RSA Laboratories*

*29 July 2009*

infotecs®

ТК 26
ГОСТР

GOST R

# *Технический комитет по стандартизации «Криптографическая защита информации»*

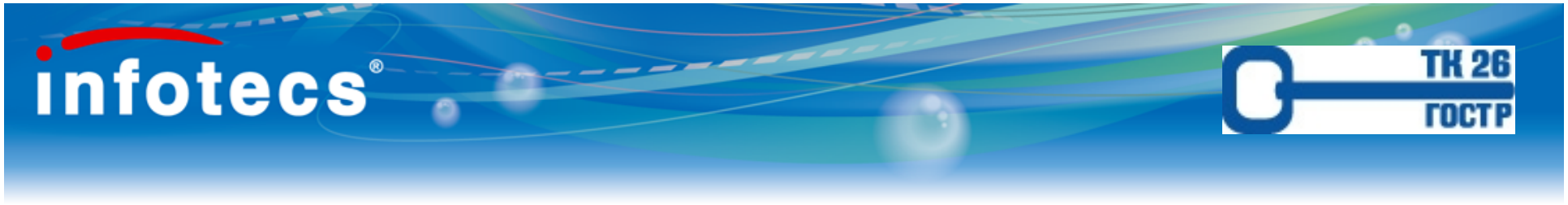
# *(ТК 26)*

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

***Основная цель ТК 26*** – 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

***Технический комитет 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.




GOST R

## Технический комитет по стандартизации (ТК26) "Криптографическая защита информации"

Рус | Eng

- Главная страница
- Новости
- Архив новостей
- Положение о ТК
- Структура ТК 26
- О деятельности по международной стандартизации
- Конференция Workshop on Current Trends in Cryptology. CTCrypt 2012
- Форум
- Контактная информация

Конец 2007 г. ознаменовался значительным для российской криптографии событием. Приказом Ростехрегулирования от 28 декабря 2007 г . был создан технический комитет по стандартизации "Криптографическая защита информации", получивший сокращенное наименование ТК 26. Этим приказом было утверждено положение о нем, его структура и перечень организаций (предприятий), ставших его членами. В марте 2008 г. было проведено первое заседание ТК 26 "Криптографическая защита информации".

Приказом Федерального агентства по техническому регулированию и метрологии от 12.08.2011 г. № 4402 председателем ТК 26 утвержден действительный член Академии криптографии Российской Федерации, доктор физико-математических наук, профессор Кузьмин А.С. Заместители председателя ТК 26: кандидат технических наук Игорь Качалин и генеральный директор "ИнфоТеКС" Андрей Чапчаев (ответственный секретарь ТК 26).

ФСБ России, как федеральный орган исполнительной власти, обеспечивающий информационную безопасность Российской

**Новости и события**

**22.03.2012**
Размещены проекты методических документов по криптоконтейнерам Читать дальше...

**07.03.2012**
Мини-симпозиум ТК 26 «Современные тенденции в криптографии» Читать дальше...

**05.03.2012**
Размещен отчет о деятельнос ТК 26 в 2011 году. Читать дальше...

***В техническом комитете «Криптографическая защита информации»*** представлены ФОИВ и предприятия (организации), к компетенции которых отнесена защита информации с использованием криптографических методов, имеющих опыт в организации разработок образцов шифровальных (криптографических) средств

(На 01.09.2012 – более 50 организаций)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 34.10-2012**

**Информационная технология**

# КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

**Процессы формирования и проверки электронной цифровой подписи**

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 34.11-2012**

**Информационная технология**

# КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

**Функция хэширования**

Стандарт ИСО/МЭК 14888-3:2006/Изм. 1:2010

Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 3. Механизмы на основе дискретного логарифма. Изменение 1. Алгоритм русской цифровой подписи эллиптической кривой, алгоритм цифровой подписи Шнора, алгоритм цифровой подписи Шнора для эллиптической кривой, и полный алгоритм цифровой подписи Шнора для эллиптической кривой

ISO/IEC 14888-3:2006/Amd 1:2010

«Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms. Ammendment 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

infotecs®

ТК 26 ГОСТ Р

CSR 2012

## The 7th International Computer Science Symposium in Russia

GOST R

### CTCrypt 2012 Call for Papers

- Conference
- Call For Papers
- News
- Important Dates
- Topics
- Program
- Workshops
- Invited Speakers
- Committees
- Venue
- Travel information
- Registration
- Submissions

**********

Call for Papers

Workshop on Current Trends in Cryptology (CTCrypt 2012б http://agora.guru.ru/display.php?conf=csr2012&page=item011) affiliated with 7th International Computer Science Symposium in Russia (CSR-2012), will be held on July 2, 2012 in Nizhny Novgorod, Russia. CTCrypt 2012 is organized by Russian Technical Committee for Standardization (TC 26) "Cryptography and security mechanisms".

(Please refer http://www.tc26.ru/invite.html for further details.)

**********

**Important dates**

- Abstract submission: April 16, 2012
- Notification: April 23, 2012
- Extended abstract submission: July 2, 2012

Official language: English
Extended abstract language: English or Russian

**Scope and Topics**

Research papers on all technical aspects of cryptology are welcome. In particular,

infotecs®

ТК 26
ГОСТ Р

GOST R

*Технический комитет по стандартизации*

*«Криптографическая защита информации» (ТК 26)*

*Сайт и форум*

***www.tc26.ru***

*Секретариат*

***tc26@infotecs.ru***