infotecs

О работе технического комитета по стандартизации «Криптографическая защита информации», ТК26 в 2013г.

Поташников Александр

Новые стандарты введены в действие 01.01.2013

- 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».

Порядок ввода в действие определен документом

«О порядке ввода в действие новых национальных стандартов электронной цифровой подписи и функции хэширования»

http://tc26.ru/info/34.10-2012_34.11-2012

Международная стандартизация

Официальный перевод ГОСТ Р 3411-2012 на английский язык доступен для специалистов

http://www.tc26.ru/en/GOSTR3411-2012/index.php

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

GOST R 34.11-2012

NATIONAL STANDARD OF THE RUSSIAN FEDERATION

Information technology

CRYPTOGRAPHIC DATA SECURITY

Hash-functions

Внедрение алгоритмов

- Разработка методик и выбор параметров для ГОСТ Р 34.10-2012 с размерностью открытого ключа 1024
- Разработка принципов идентификации новых алгоритмов, присвоение объектных идентификаторов новым алгоритмам и их параметрам
- Разработка методических рекомендаций по применению новых алгоритмов в различных протоколах и форматах

Параметры алгоритма

- ГОСТ Р 34.10.2012 512 бит – RFC4357
- ГОСТ Р 34.10.2012 1024 бита - «Методические рекомендации по выбору параметров эллиптических кривых в соответствии с ГОСТ Р 34.10-2012»

Идентификаторы алгоритмов

1.2.643.2.2

iso(1) member-body(2) ru(643) rans(2) cryptopro(2)

1.2.643.7.1

iso(1) member-body(2) ru(643) reg(7) tk26(1)

http://www.oid-inform.ru

OID РФ

Авторская страница Марины Алексеевны Игнатьевой

Поиск по странице

Найти

Например: Сервис или 1.2.643.3.5

OID организаций по стандартизации

NN	ИДЕНТИФИКАТОР	ИМЯ	ОРГАНИЗАЦИЯ-ЭМИТЕНТ	ОБЛАСТЬ ИСПОЛЬЗОВАНИЯ
1		————		
2	1.2.643.7.1	C=ru,o=REG7,o= Technical committee on standardization (TC26) "Cryptography and security mechanisms"	Технический комитет по стандартизации (ТК26) «Криптографическая защита информации»	вопросы стандартизации продукции и услуг, классифицируемые в соответствии с кодом Общероссийского классификатора стандартов 35.040 «Наборы знаков и кодирование информации, включая методы обеспечения безопасности ИТ, шифрование и т.д.» и 35.160 «Микропроцессорные системы, включая персональные ЭВМ и т.д.», относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись

Идентификаторы объектов технического комитета по стандартизации

"Криптографическая защита информации" (ТК 26)

Зарегистрированный за ТК 26 корень - 1.2.643.7.1

Область применения:

35.040 Наборы знаков и кодирование информации *Включая кодирование аудио-, изобразительной, мультимедиа и гипермедиа информации, методы обеспечения безопасности ИТ, шифрование, штриховое кодирование и т. д.

35.160 Микропроцессорные системы *Включая персональные ЭВМ, калькуляторы и т.д. *Интегральные схемы см. 31.200

Value	*Name*	*Comment*
1.2.643.7.1	id-tc26	корень ТК 26 в российском сегменте мирового пространства идентификаторов объектов
1.2.643.7.1.1	id-tc26-algorithms	алгоритмы
1.2.643.7.1.1.1	id-tc26-sign	алгоритмы подписи
1.2.643.7.1.1.1.1	id-tc26-gost3410-12-256	алгоритм подписи ГОСТ Р 34.10-12 с ключом 256
1.2.643.7.1.1.1.2	id-tc26-gost3410-12-512	алгоритм подписи ГОСТ Р 34.10-12 с ключом 512
1.2.643.7.1.1.2	id-tc26-digest	алгоритмы хэширования
~~1.2.643.7.1.1.2.1~~	~~id-tc26-gost3411-94~~	~~алгоритм хэширования ГОСТ Р 34.11-94~~ OID исключен (*)
1.2.643.7.1.1.2.2	id-tc26-gost3411-12-256	алгоритм хэширования ГОСТ Р 34.11-12 с длиной 256
1.2.643.7.1.1.2.3	id-tc26-gost3411-12-512	алгоритм хэширования ГОСТ Р 34.11-12 с длиной 512
1.2.643.7.1.1.3	id-tc26-signwithdigest	алгоритмы подписи вместе хэшированием
~~1.2.643.7.1.1.3.1~~	~~id-tc26-signwithdigest-gost3410-12-94~~	~~алгоритм подписи ГОСТ Р 34.10-12 с ключом 256 с хэшированием ГОСТ Р 34.11-94~~ OID исключен (*)
1.2.643.7.1.1.3.2	id-tc26-signwithdigest-gost3410-12-256	алгоритм подписи ГОСТ Р 34.10-12 с ключом 256 с хэшированием ГОСТ Р 34.11-12
1.2.643.7.1.1.3.3	id-tc26-signwithdigest-gost3410-12-512	алгоритм подписи ГОСТ Р 34.10-12 с ключом 512 с хэшированием ГОСТ Р 34.11-12
1.2.643.7.1.1.4	id-tc26-mac	алгоритмы выработки кодов аутентификации сообщений

Методические рекомендации

Форматы хранения и транспорта ключей

- Парольная защита с использованием алгоритмов ГОСТ, Дополнения к PKCS#5, версия 2.0
- Транспортный ключевой контейнер, Дополнения к PKCS#8 и PKCS#12, версия 2.0
- Ключевой контейнер, Дополнение к PKCS#15, версия 2.0.

Методические рекомендации

Рекомендации по применению новых алгоритмов в форматах и протоколах CMS, X.509, TLS

- Методические рекомендации по использованию стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в криптографических протоколах.
- Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509;
- Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS;
- Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS).

Доступные версии с поддержкой алгоритмов 2012г.

ViPNet CSP

Криптопровайдер ViPNet CSP — это средство криптографической защиты информации, предназначенное для выполнения криптографических операций, доступ к которым обеспечивается встраиванием криптопровайдера в приложения через стандартизованные интерфейсы. ViPNet CSP реализует криптографические алгоритмы, соответствующие российским стандартам.

http://www.infotecs.ru/downloads/product_beta.php

http://www.cryptopro.ru/products/csp/downloads

КриптоПро CSP 4.0.9007 Archimedes

Опубликовано raandom в 09 Сентябрь 2013 - 19:12

Представляем предварительную версию КриптоПро CSP 4.0 (сборка 4.0.9007 Archimedes).

Основные изменения:

Планы на будущее

- Согласование методических рекомендаций
- Обеспечение совместимости реализаций разных производителей
- Внесение изменений в спецификацию криптографического интерфейса PKCS#11

infotecs

Спасибо за внимание!
Вопросы?

Поташников Александр