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 34.10-2012 с ключом 256
1.2.643.7.1.1.1.2	id-tc26-gost3410-12-512	алгоритм подписи ГОСТ Р 34.10-2012 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 34.11-2012 с длиной 256
1.2.643.7.1.1.2.3	id-tc26-gost3411-12-512	алгоритм хэширования ГОСТ Р 34.11-2012 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 34.10-2012 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 34.10-2012 с ключом 256 с хэшированием ГОСТ Р 34.11-2012

1.2.643.7.1.1.3.3	id-tc26-signwithdigest-gost3410-12-512	алгоритм подписи ГОСТ Р 34.10-2012 с ключом 512 с хэшированием ГОСТ Р 34.11-2012
1.2.643.7.1.1.4	id-tc26-mac	алгоритмы выработки кодов аутентификации сообщений
1.2.643.7.1.1.4.1	id-tc26-hmac-gost-3411-12-256	алгоритм HMAC- ГОСТ Р 34.11-2012 с ключом 256 со значениями B = 64, L = 32
1.2.643.7.1.1.4.2	id-tc26-hmac-gost-3411-12-512	алгоритм HMAC ГОСТ Р 34.11-2012 с ключом 512 со значениями B = 64, L = 64
1.2.643.7.1.1.5	id-tc26-cipher	алгоритмы шифрования
1.2.643.7.1.1.6	id-tc26-agreement	алгоритмы согласования ключа
1.2.643.7.1.1.6.1	id-tc26-agreement-gost-3410-12-256	алгоритмы согласования ключа на основе ГОСТ Р 34.10-2012 для ключа 256
1.2.643.7.1.1.6.2	id-tc26-agreement-gost-3410-12-512	алгоритмы согласования ключа на основе ГОСТ Р 34.10-2012 для ключа 512
1.2.643.7.1.2	id-tc26-constants	константы (параметры)
1.2.643.7.1.2.1	id-tc26-sign-constants	параметры алгоритмов подписи
1.2.643.7.1.2.1.2	id-tc26-gost-3410-12-512-constants	параметры алгоритма подписи ГОСТ Р 34.10-2012 с ключом 512
1.2.643.7.1.2.1.2.0	id-tc26-gost-3410-12-512-paramSetTest	тестовые параметры алгоритма подписи ГОСТ Р 34.10-2012 с ключом 512
1.2.643.7.1.2.1.2.1	id-tc26-gost-3410-12-512-paramSetA	рабочие параметры алгоритма подписи ГОСТ Р 34.10-2012 с ключом 512
1.2.643.7.1.2.1.2.2	id-tc26-gost-3410-12-512-paramSetB	рабочие параметры алгоритма подписи ГОСТ Р 34.10-2012 с ключом 512
1.2.643.7.1.2.2	id-tc26-digset-constants	параметры алгоритмов хэширования
~~1.2.643.7.1.2.2.1~~	~~id-tc26-gost-3411-94-constants~~	~~параметры алгоритма хэширования ГОСТ Р 34.11-94~~ OID исключен (*)
~~1.2.643.7.1.2.2.1.1~~	~~id-tc26-gost-3411-94-paramSetA~~	~~параметры алгоритма хэширования ГОСТ Р 34.11-94~~ OID исключен (*)
1.2.643.7.1.2.5	id-tc26-cipher-constants	параметры алгоритмов шифрования
1.2.643.7.1.2.5.1	id-tc26-gost-28147-constants	параметры алгоритма шифрования ГОСТ 28147-89
1.2.643.7.1.2.5.1.1	id-tc26-gost-28147-param-A	набор A параметры алгоритма шифрования ГОСТ 28147-89

(*) - OID исключен по результатам обсуждения на форуме ТК 26 и заседании ТК 26 от 11.04.2013

Определяемые идентификаторы предлагается использовать наряду с идентификаторами из RFC 4357.

Идентификаторы для параметров ГОСТ Р 34.10-2012 для модуля длины 256 бит не вводится, в соответствующих случаях рекомендуется пользоваться идентификаторами параметров ГОСТ Р 34.10-2001