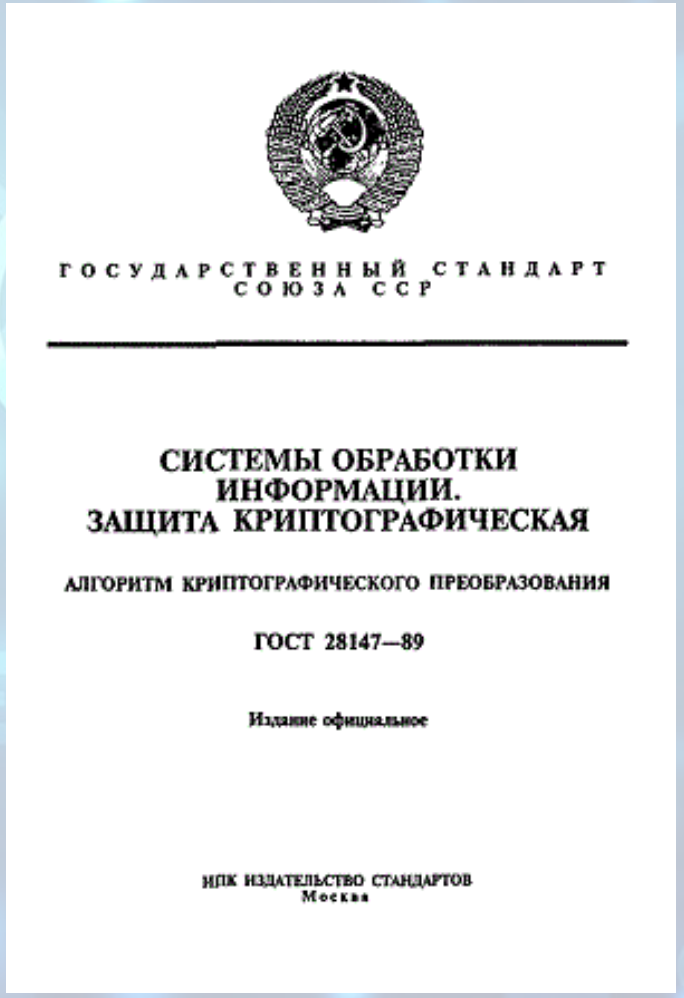
XXVII научно-практическая конференция
«Комплексная защита информации»

О российских стандартизированных решениях в области криптографической защиты информации и перспективах их использования в рамках Союзного государства

Бондаренко Александр Иванович

Академия криптографии Российской Федерации

ГОСТ 28147-89



ГОСУДАРСТВЕННЫЙ СТАНДАРТ
СОЮЗА ССР

СИСТЕМЫ ОБРАБОТКИ
ИНФОРМАЦИИ.
ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28147—89

Издание официальное

ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ
Москва

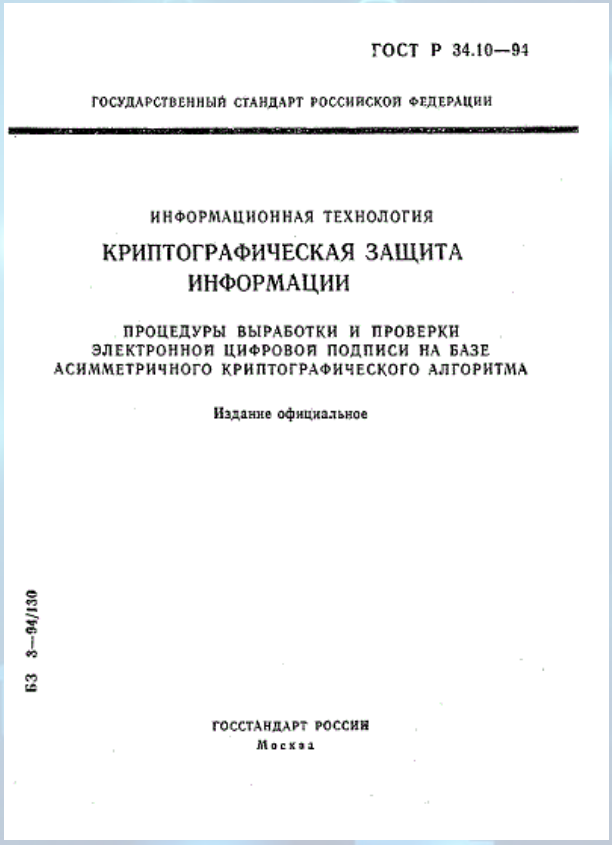
1989

1989

2022

ГОСТ 28147-89

ГОСТ Р 34.10-94/ ГОСТ Р 34.11-94



ГОСТ Р 34.10—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

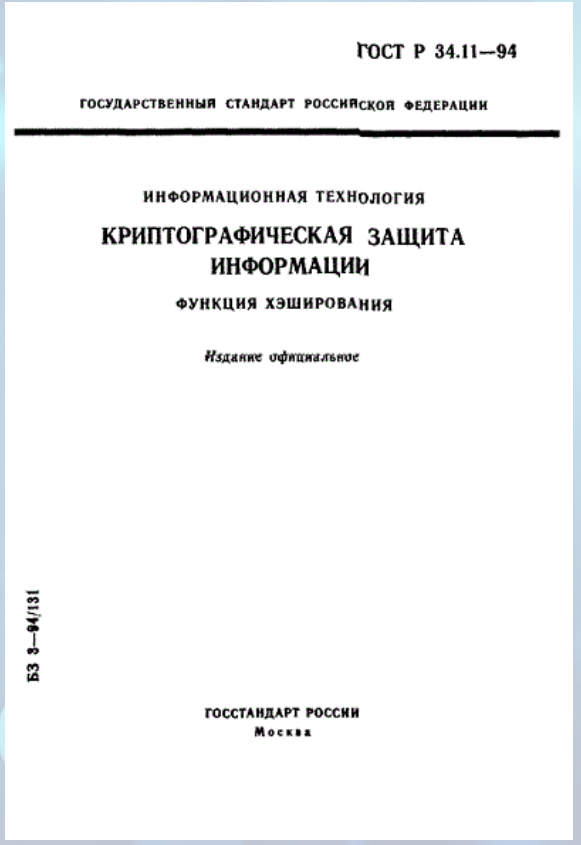
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕДУРЫ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Издание официальное

БЗ 3—94/130

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ Р 34.11—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

Издание официальное

БЗ 3—94/131

ГОССТАНДАРТ РОССИИ
Москва

1989

2022

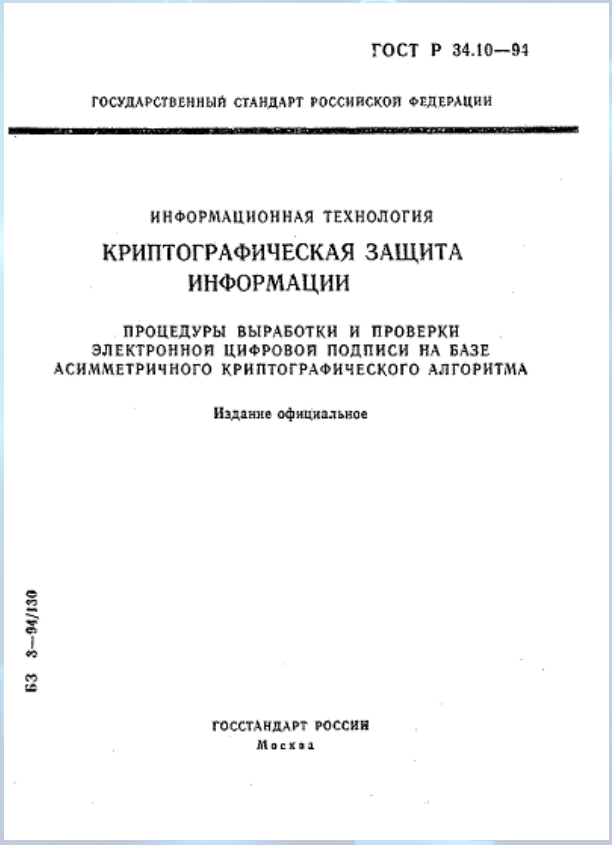
ГОСТ 28147-89

1994

ГОСТ Р 34.10-94

ГОСТ Р 34.11-94

ГОСТ 34.310-95/ ГОСТ 34.311-95



ГОСТ Р 34.10—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

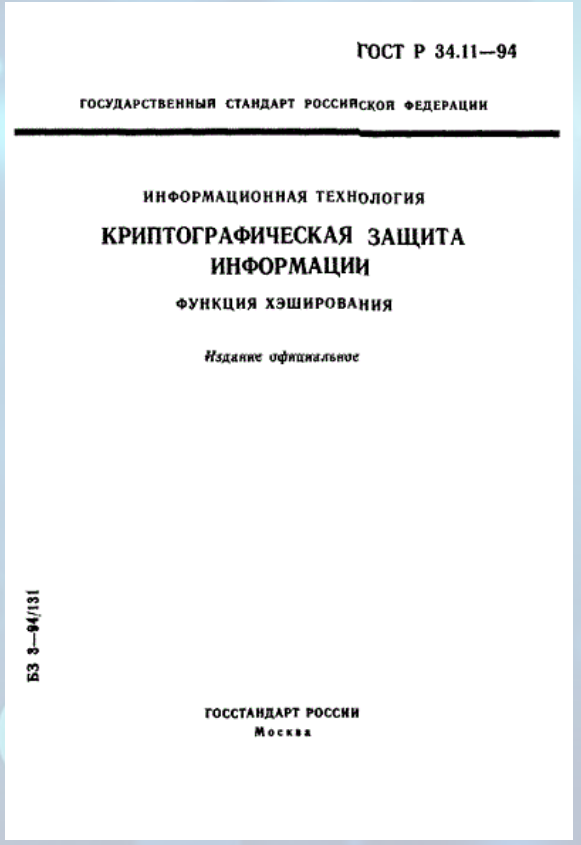
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕДУРЫ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Издание официальное

БЗ 3—94/130

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ Р 34.11—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

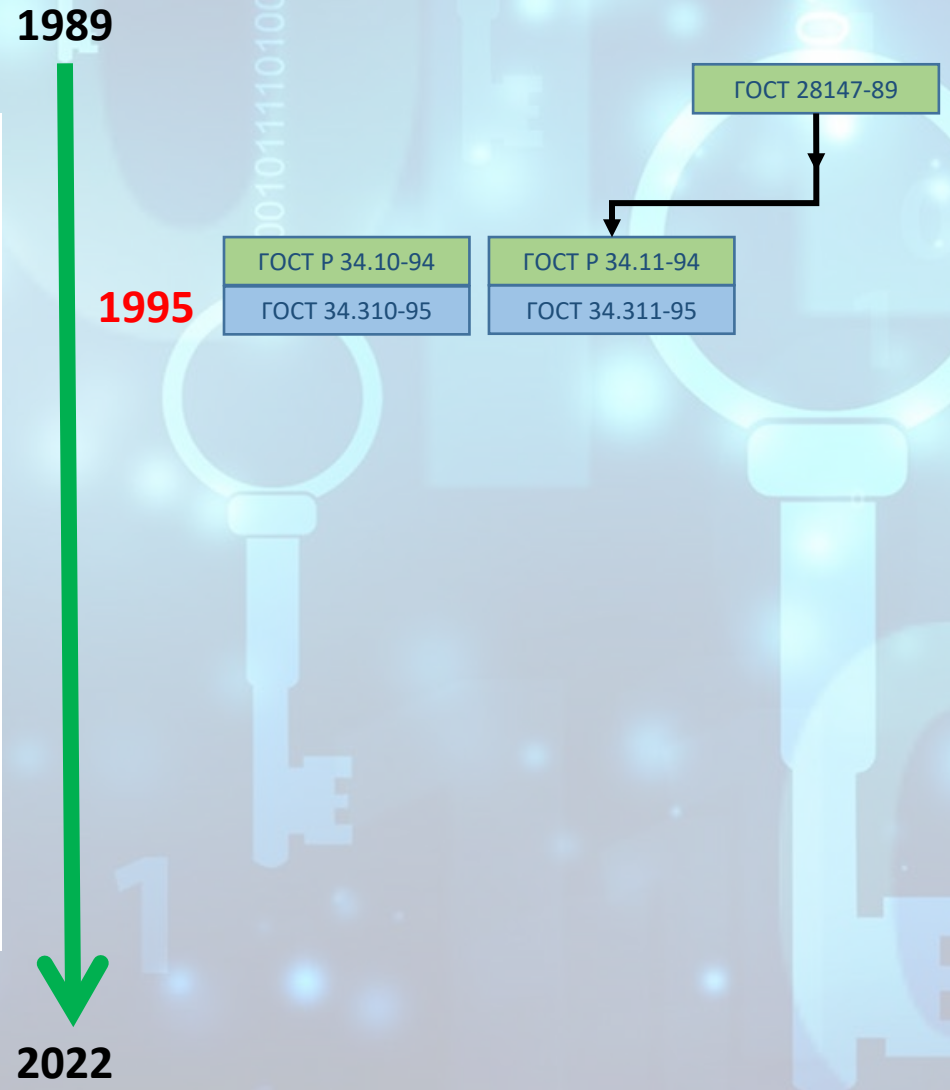
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

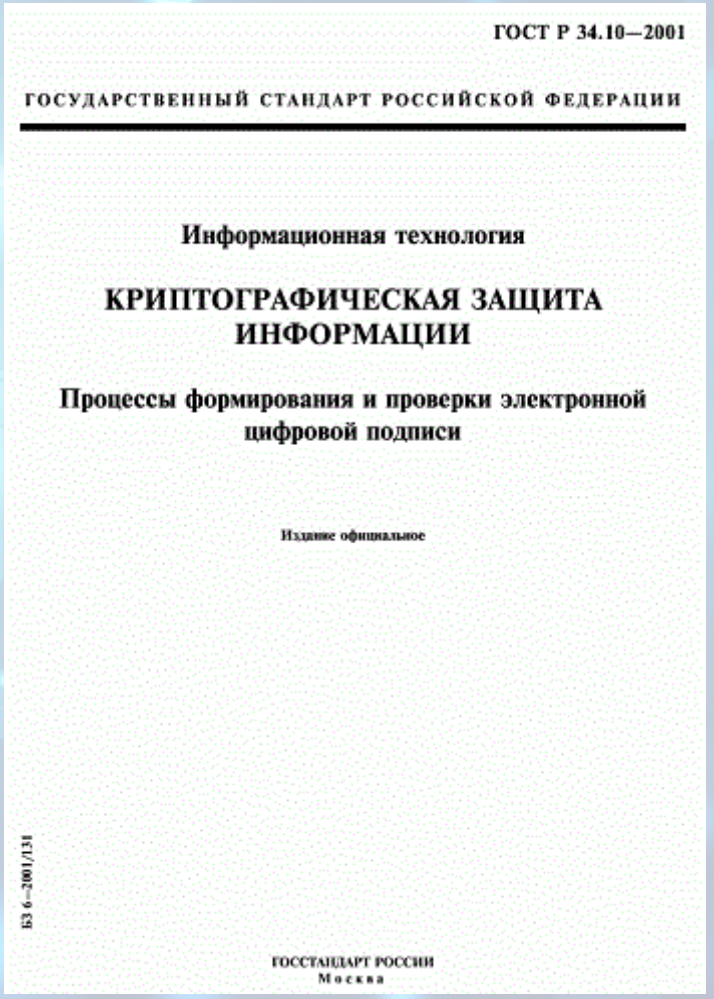
Издание официальное

БЗ 3—94/131

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ Р 34.10-2001



ГОСТ Р 34.10—2001

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

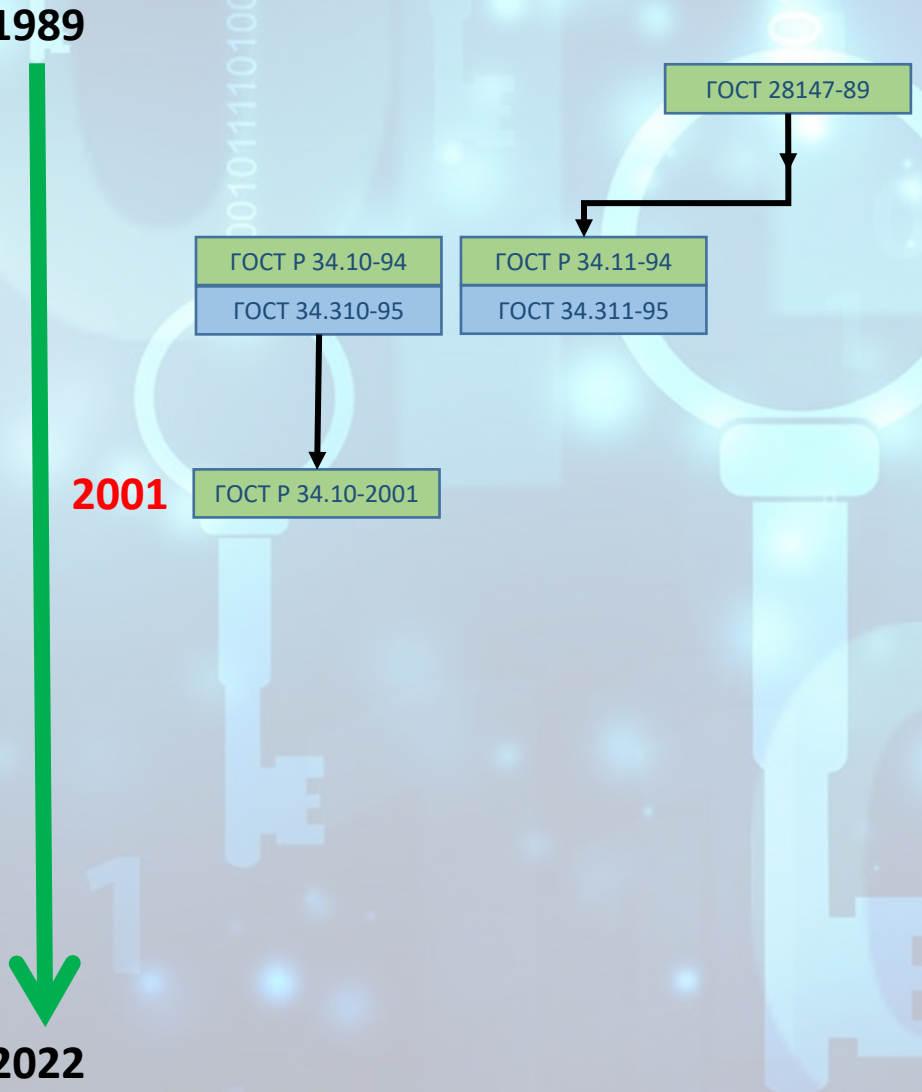
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

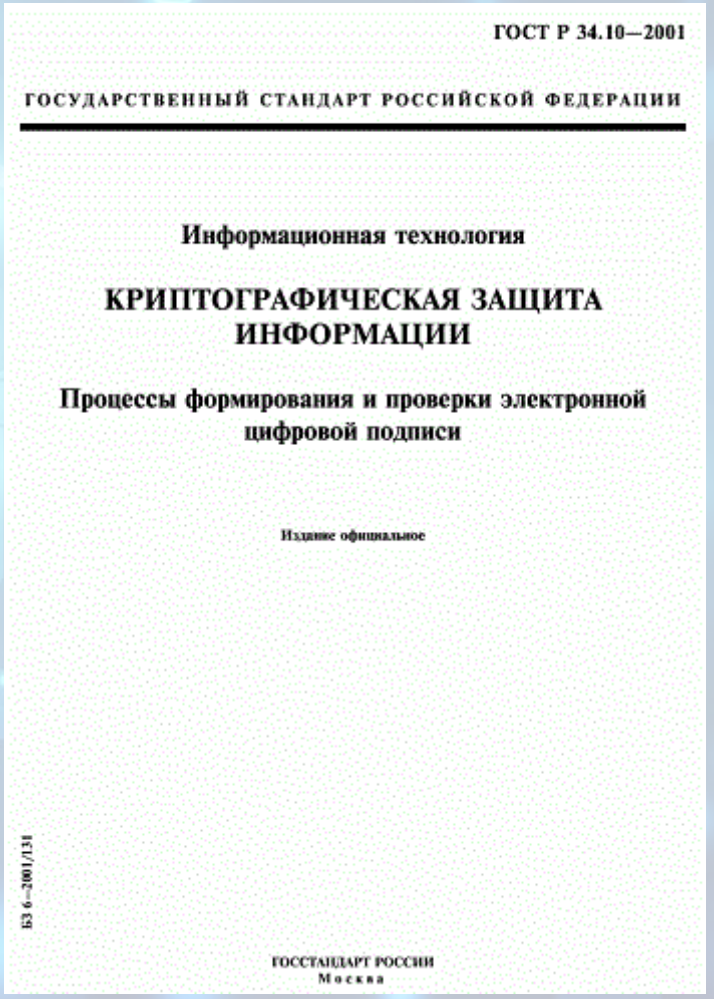
Издание официальное

БЗ 6—2001/131

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ 34.310-2004


ГОСТ Р 34.10—2001

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

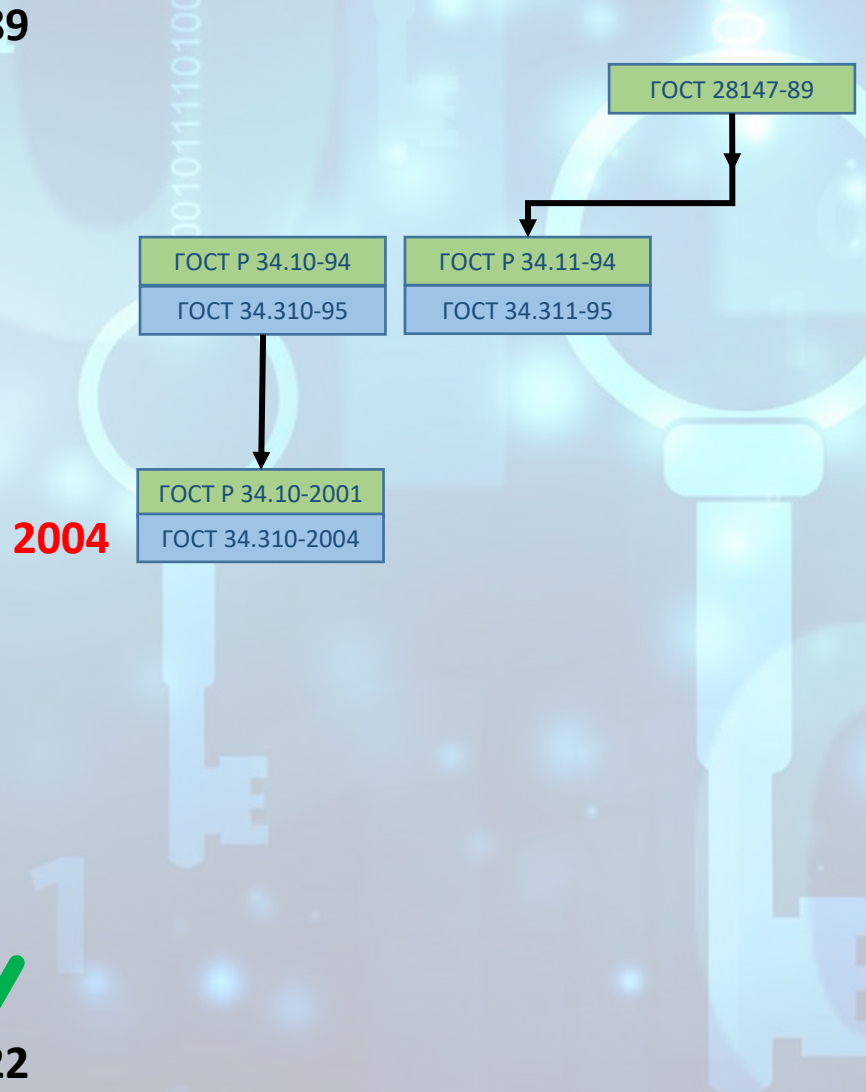
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

БЗ 6—2001/131

ГОССТАНДАРТ РОССИИ
Москва



RCF 4357/4490/4491

1989

Network Working Group
Request for Comments: 4357
Category: Informational

V. Popov
I. Kurepkin
S. Leontiev
CRYPTO-PRO
January 2006

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

Status of This Memo

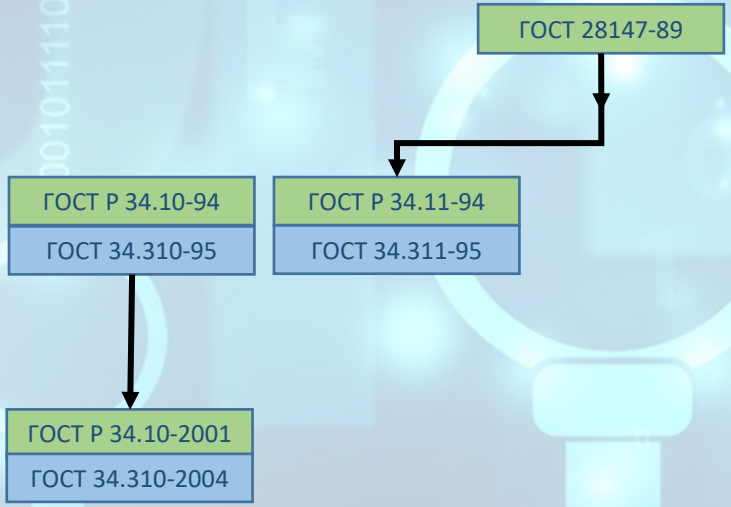
This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the cryptographic algorithms and parameters supplementary to the original GOST specifications, GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94, for use in Internet applications.



2006

Network Working Group
Request for Comments: 4491
Updates: 3279
Category: Standards Track

S. Leontiev, Ed.
CRYPTO-PRO
D. Shefanovski, Ed.
Mobile TeleSystems OJSC
May 2006

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

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document supplements RFC 3279. It describes encoding formats, identifiers, and parameter formats for the algorithms GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 for use in Internet X.509 Public Key Infrastructure (PKI).

Network Working Group
Request for Comments: 4490
Category: Standards Track

S. Leontiev, Ed.
G. Chudov, Ed.
CRYPTO-PRO
May 2006

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)

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the conventions for using the cryptographic algorithms GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 with the Cryptographic Message Syntax (CMS). The CMS is used for digital signature, digest, authentication, and encryption of arbitrary message contents.

2022

RCF 5830/5831/5832

Independent Submission
Request for Comments: 5830
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

GOST 28147-89: Encryption, Decryption,
and Message Authentication Code (MAC) Algorithms

Abstract

This document is intended to be a source of information about the Russian Federal standard for electronic encryption, decryption, and message authentication algorithms (GOST 28147-89), which is one of the Russian cryptographic standard algorithms called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST 28147-89 for encryption, decryption, and message authentication.

Independent Submission
Request for Comments: 5832
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

GOST R 34.10-2001:
Digital Signature Algorithm

Abstract

This document is intended to be a source of information about the Russian Federal standard for digital signatures (GOST R 34.10-2001), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST R 34.10-2001 for digital signature generation and verification.

Independent Submission
Request for Comments: 5831
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

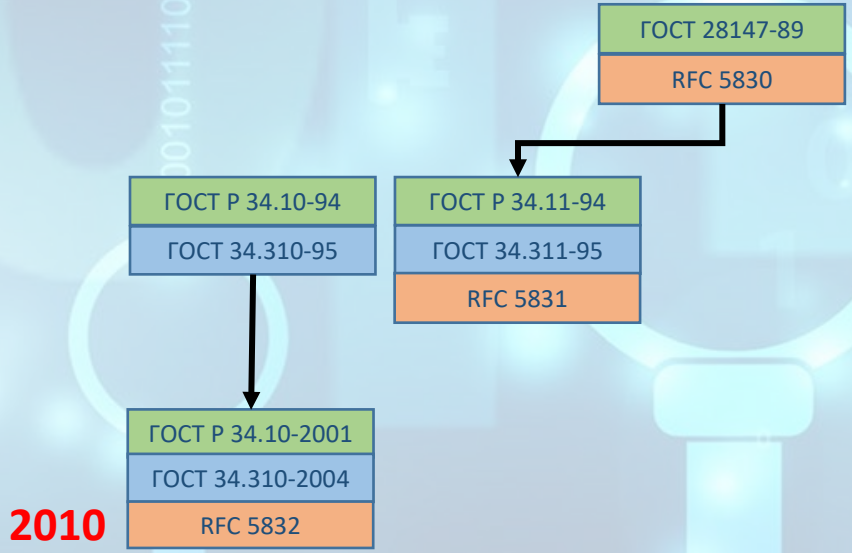
GOST R 34.11-94: Hash Function Algorithm

Abstract

This document is intended to be a source of information about the Russian Federal standard hash function (GOST R 34.11-94), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST R 34.11-94 for hash computation.

1989

2022



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

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

П Р И К А З

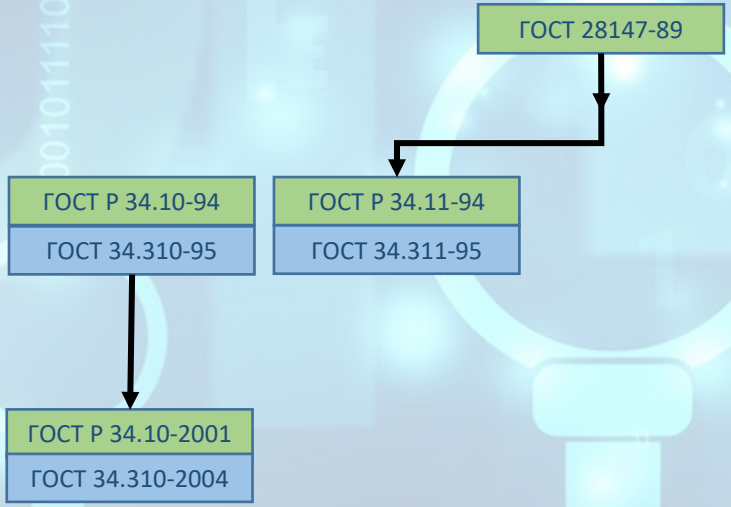
(выписка)

«28» декабря 2007 г. № 3825дсп

О создании технического комитета по стандартизации «Криптографическая защита информации»

В целях реализации Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности», Указа Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации», обеспечения в Российской Федерации организации работ по разработке, принятию и применению документов по стандартизации шифровальных (криптографических) средств защиты информации, а также вопросов их использования в защищенных системах **приказываю:**

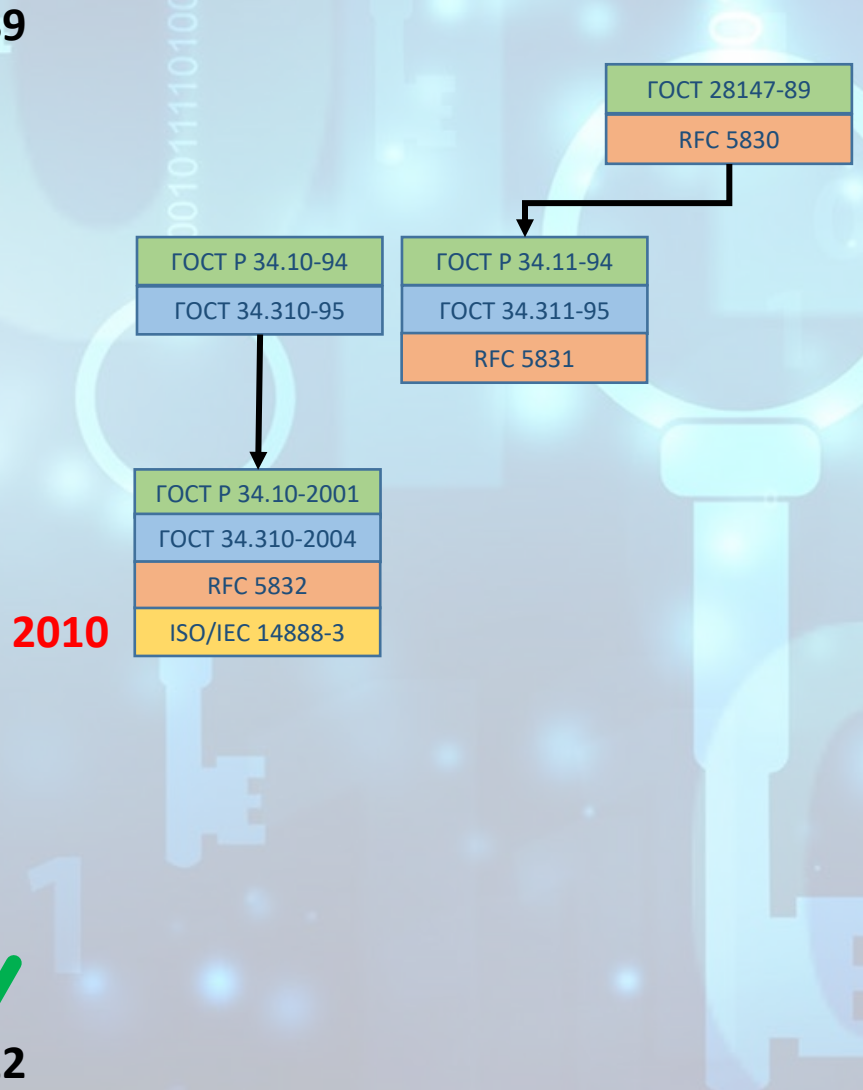
1. Создать технический комитет по стандартизации (далее - ТК) «Криптографическая защита информации» и закрепить за ним вопросы стандартизации продукции и услуг, классифицируемые в соответствии с кодами Общероссийского классификатора стандартов 35.040 «Наборы знаков и кодирование информации, включая методы 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.



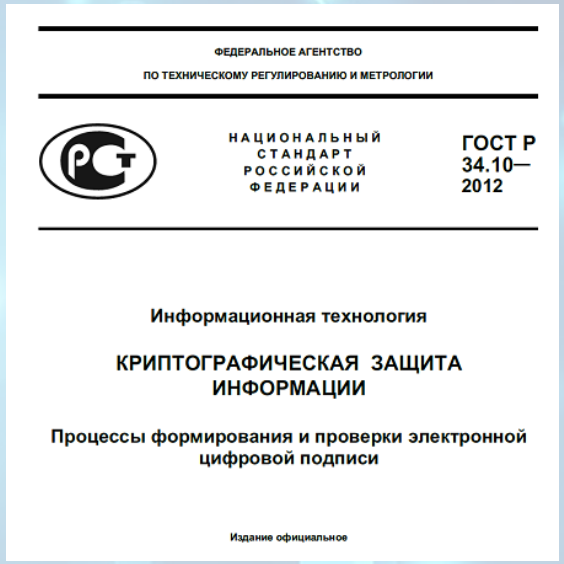
ISO/IEC 14888-3

ISO/IEC 14888-3:2018

IT Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms



ГОСТ Р 34.10-2012/ ГОСТ Р 34.11-2012



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

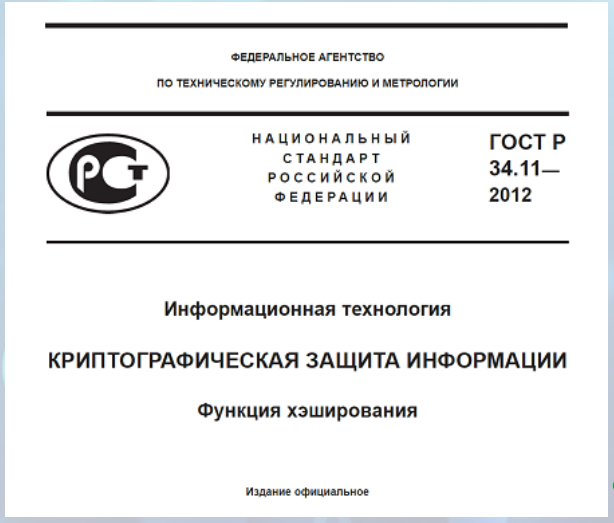
ГОСТ Р 34.10— 2012

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

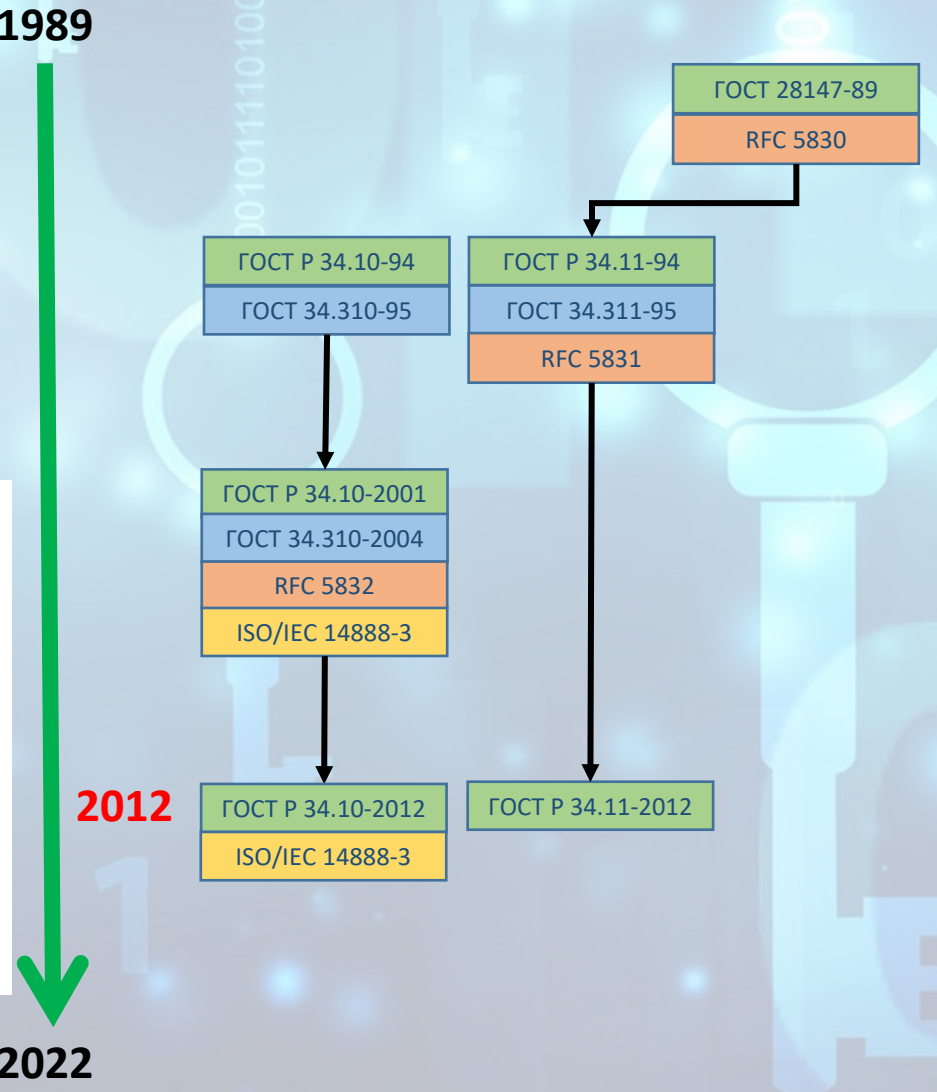
ГОСТ Р 34.11— 2012

Информационная технология

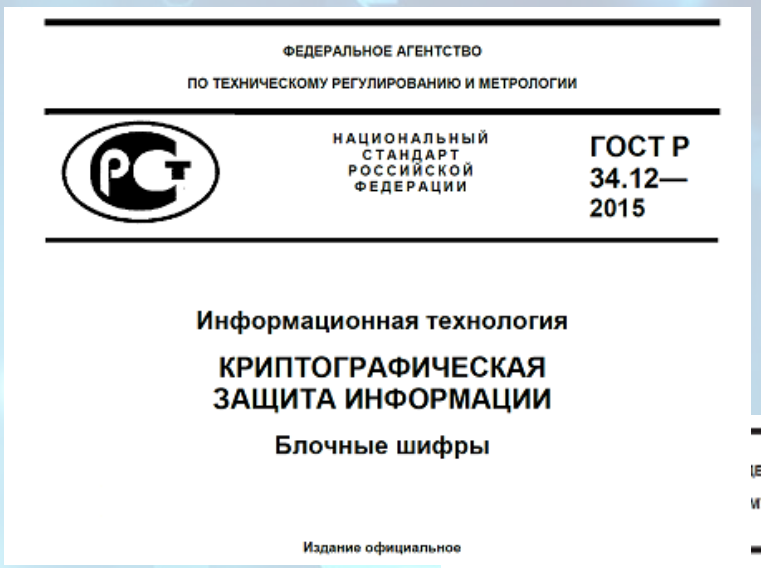
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

Издание официальное



ГОСТ Р 34.12-2015/ ГОСТ Р 34.13-2015


ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

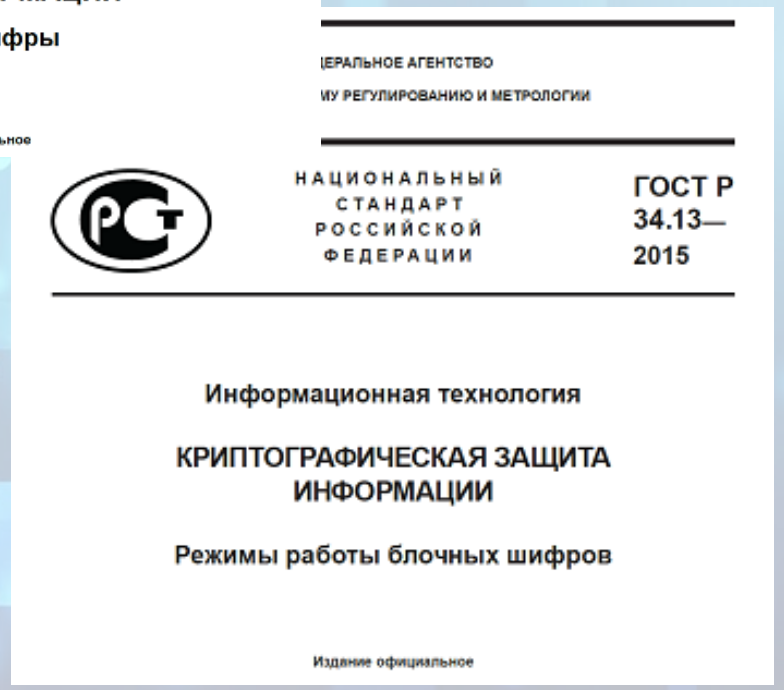
ГОСТ Р 34.12— 2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное


НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

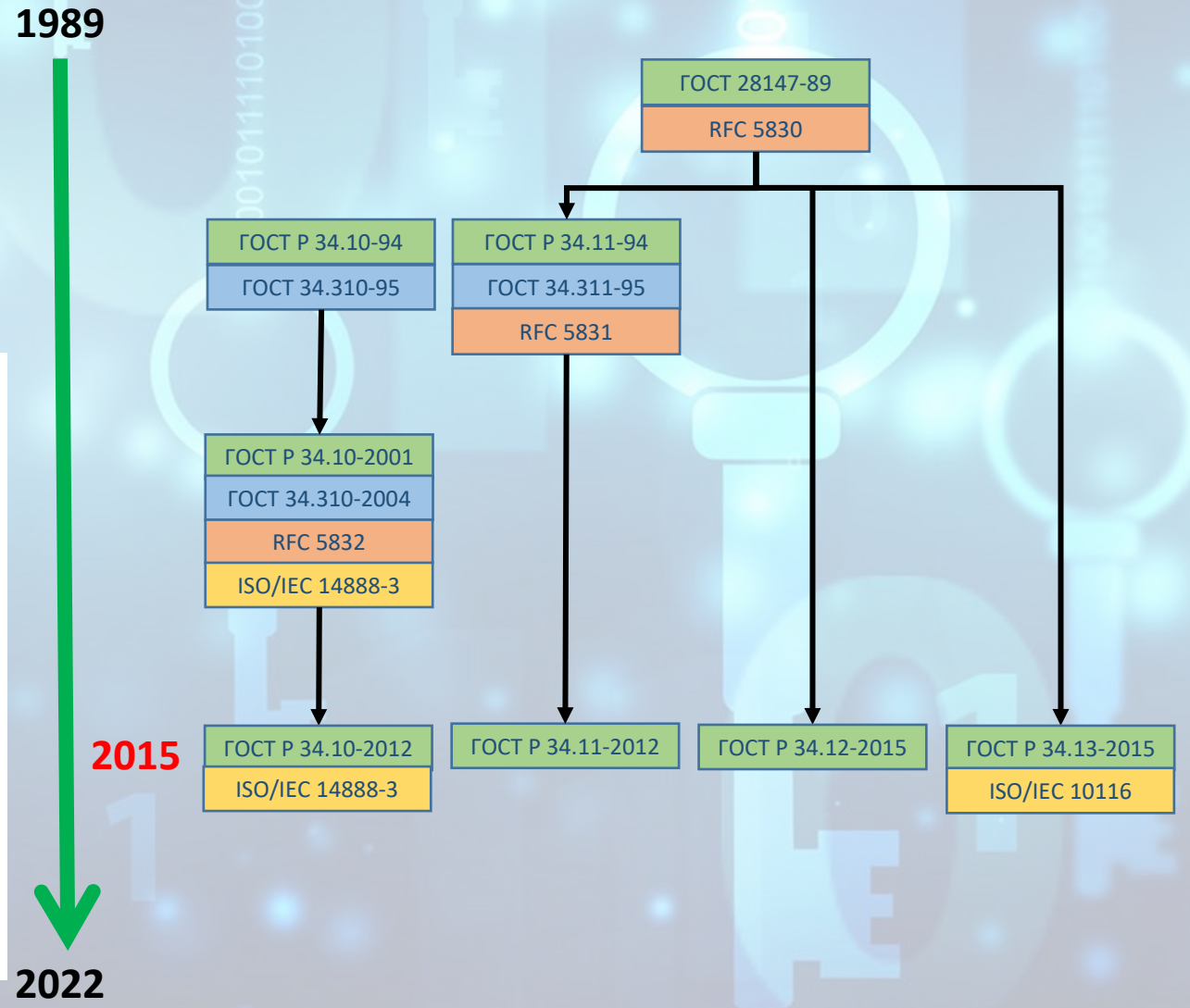
ГОСТ Р 34.13— 2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное



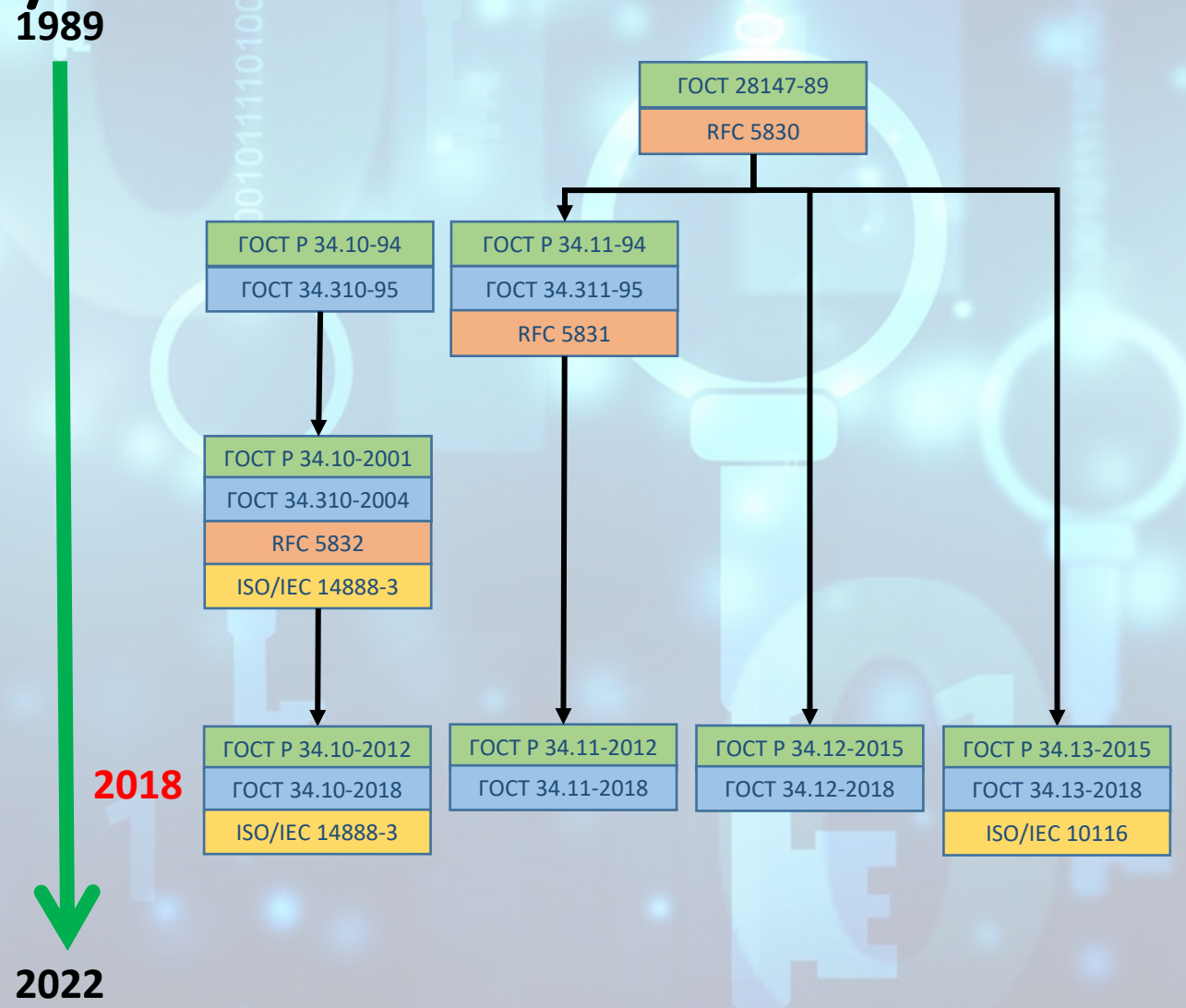
ГОСТ 34.10-2018/ ГОСТ 34.11-2018
ГОСТ 34.12-2018/ ГОСТ 34.13-2018


ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (EASC)
МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ
ГОСТ 34.10– 2018
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Процессы формирования и проверки электронной цифровой подписи
Издание официальное

ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (EASC)
МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ
ГОСТ 34.11– 2018
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Функция хэширования
Издание официальное


ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (EASC)
МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ
ГОСТ 34.12– 2018
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Блочные шифры
Издание официальное


ЕВРАЗИЙСКИЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ (EACC)
EURO-ASIAN COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION (EASC)
МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ
ГОСТ 34.13– 2018
Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Режимы работы блочных шифров
Издание официальное



RFC 6986/7091/7801/8891

Independent Submission
Request for Comments: 6986
Updates: 5831
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.
August 2013

GOST R 34.11-2012: Hash Function

Abstract

This document is intended to be a source of information about the Russian Federal standard hash function (GOST R 34.11-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). This document updates RFC 5831.

Independent Submission
Request for Comments: 7091
Updates: 5832
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.
December 2013

GOST R 34.10-2012: Digital Signature Algorithm

Abstract

This document provides information about the Russian Federal standard for digital signatures (GOST R 34.10-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document provides information for developers and users of GOST R 34.10-2012 regarding digital signature generation and verification. This document updates RFC 5832.

Independent Submission
Request for Comments: 8891
Updates: 5830
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
JSC "NPK Kryptonite"
D. Baryshkov
Auriga, Inc.
September 2020

GOST R 34.12-2015: Block Cipher "Magma"

Abstract

In addition to a new cipher with a block length of n=128 bits (referred to as "Kuznyechik" and described in RFC 7801), Russian Federal standard GOST R 34.12-2015 includes an updated version of the block cipher with a block length of n=64 bits and key length of k=256 bits, which is also referred to as "Magma". The algorithm is an updated version of an older block cipher with a block length of n=64 bits described in GOST 28147-89 (RFC 5830). This document is intended to be a source of information about the updated version of the 64-bit cipher. It may facilitate the use of the block cipher in Internet applications by providing information for developers and users of the GOST 64-bit cipher with the revised version of the cipher for encryption and decryption.

Independent Submission
Request for Comments: 7801
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Research Computer Center MSU
March 2016

GOST R 34.12-2015: Block Cipher "Kuznyechik"

Abstract

This document is intended to be a source of information about the Russian Federal standard GOST R 34.12-2015 describing the block cipher with a block length of n=128 bits and a key length of k=256 bits, which is also referred to as "Kuznyechik". This algorithm is one of the set of Russian cryptographic standard algorithms (called GOST algorithms).

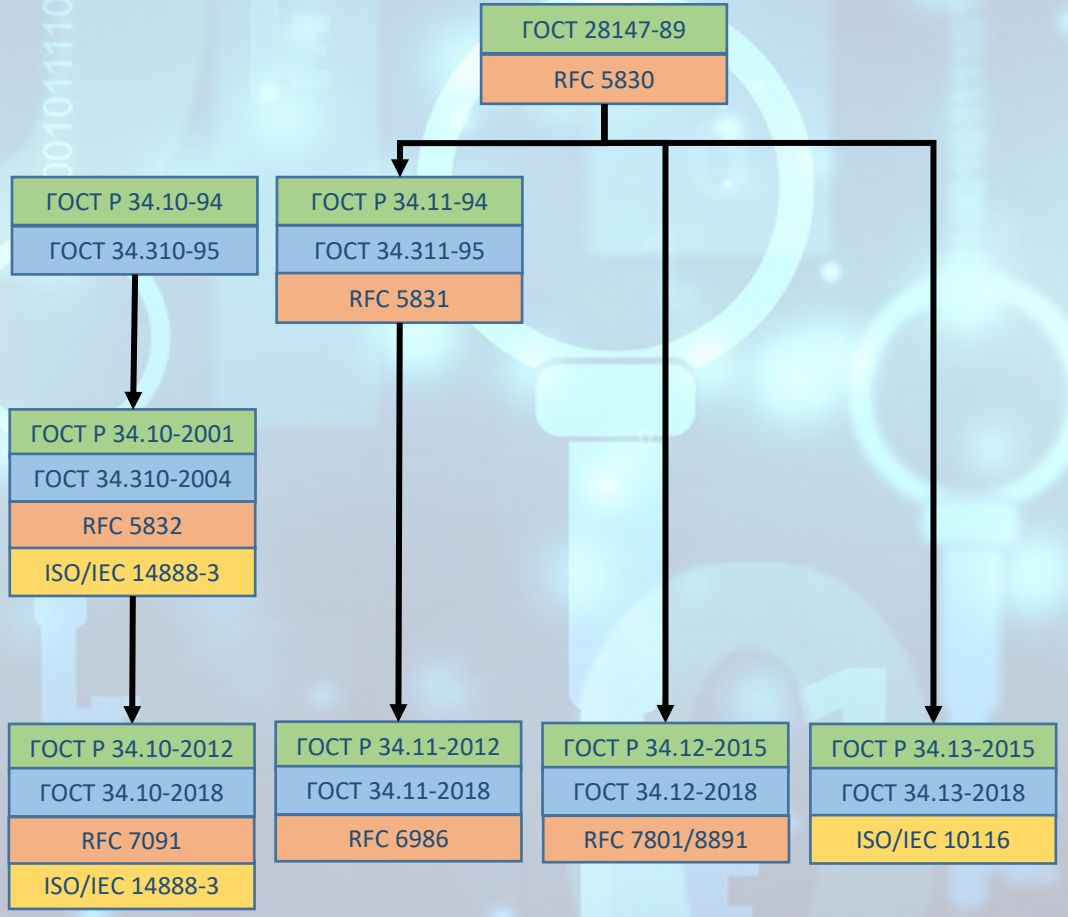
1989

2013

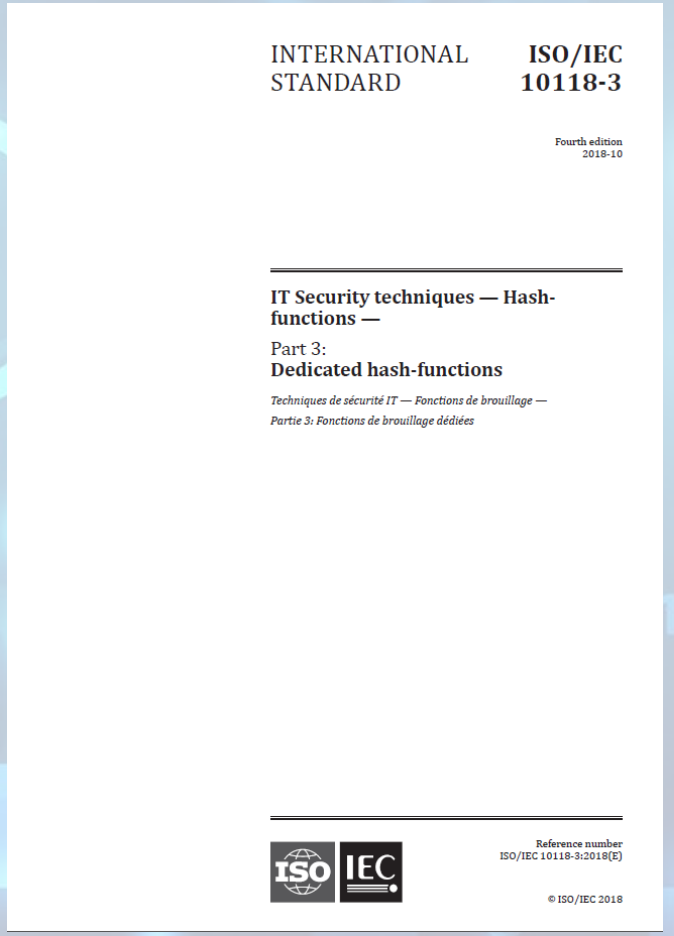
...

2016

2022



ISO/IEC 10118-3


INTERNATIONAL STANDARD

ISO/IEC 10118-3

Fourth edition
2018-10

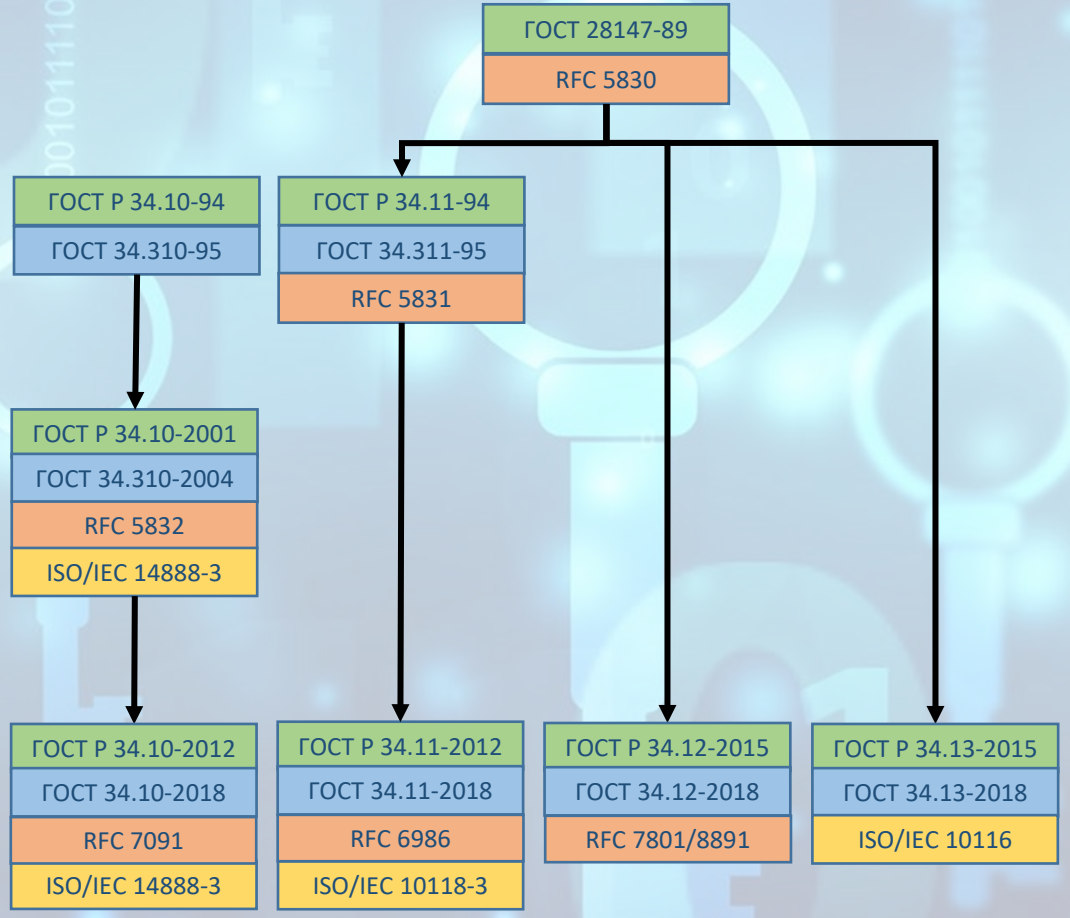
IT Security techniques — Hash-functions —

Part 3:
Dedicated hash-functions

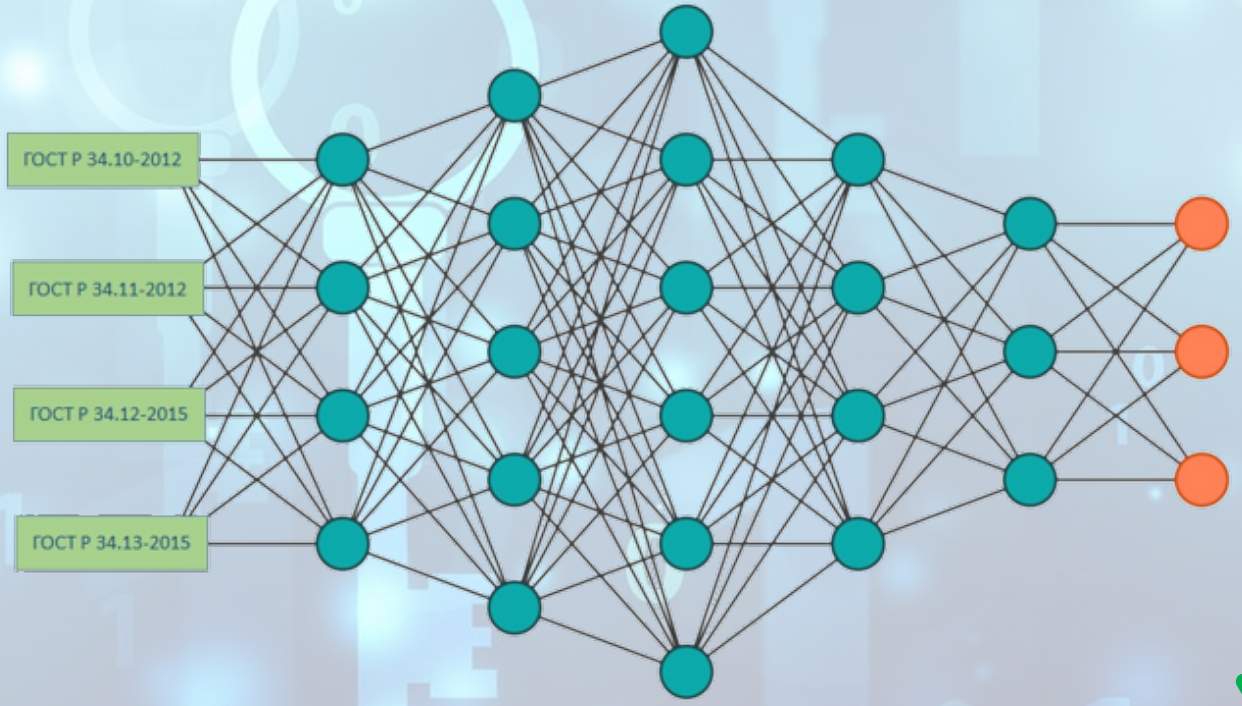
Techniques de sécurité IT — Fonctions de brouillage —
Partie 3: Fonctions de brouillage dédiées

Reference number
ISO/IEC 10118-3:2018(E)

© ISO/IEC 2018



Документы по стандартизации



2016

2022

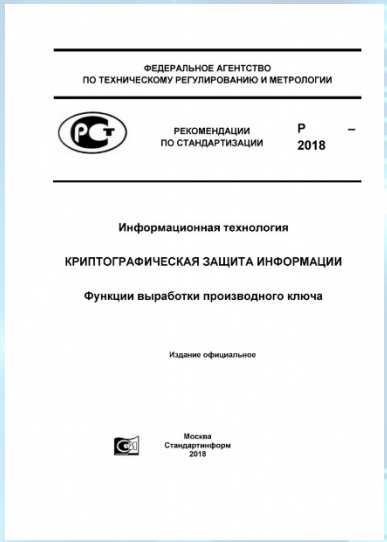
2025

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

Документы по стандартизации - общие


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р – 2018

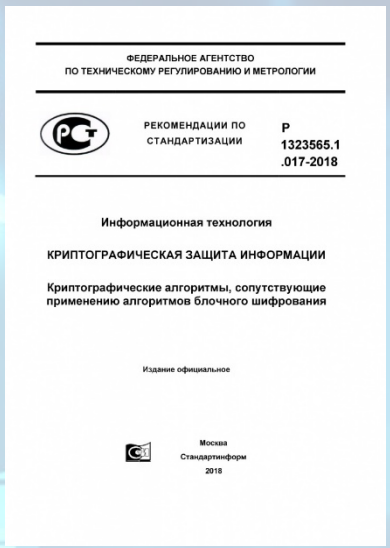
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функции выработки производного ключа

Издание официальное

Москва Стандартинформ 2018


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1 .017-2018

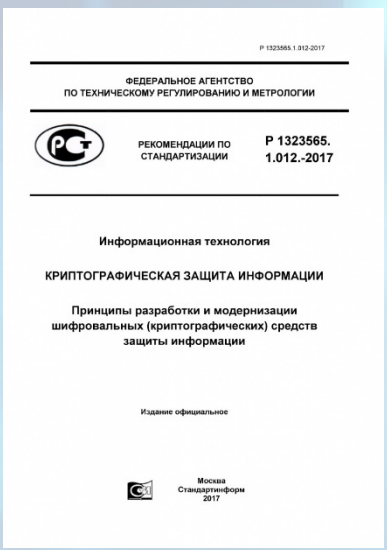
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Издание официальное

Москва Стандартинформ 2018


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565. 1.012.-2017

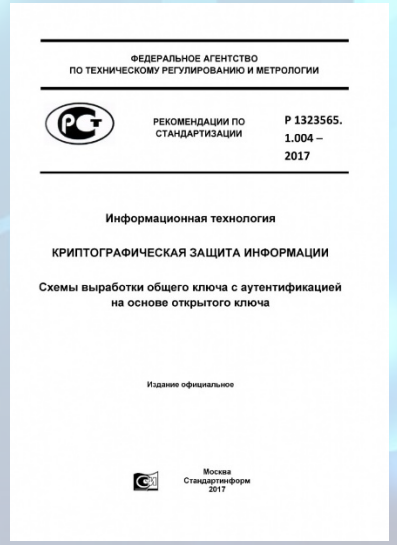
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565. 1.004 – 2017

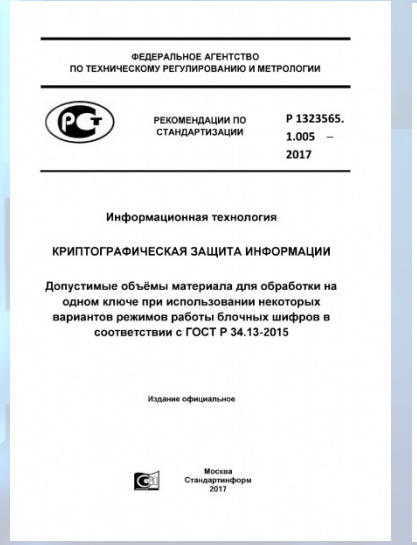
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Схемы выработки общего ключа с аутентификацией на основе открытого ключа

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565. 1.005 – 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565. 1.006 – 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Механизмы выработки псевдослучайных последовательностей

Издание официальное

Москва Стандартинформ 2017

2016

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	**Р 50.1.115–2016**	Р 1323565.1.003-2017	**Р 1323565.1.004-2017**
Р 1323565.1.005-2017	**Р 1323565.1.006-2017**	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	**Р 1323565.1.012-2017**
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	**Р 1323565.1.017-2018**
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	**Р 1323565.1.022-2018**
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	**Р 1323565.1.026-2019**
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

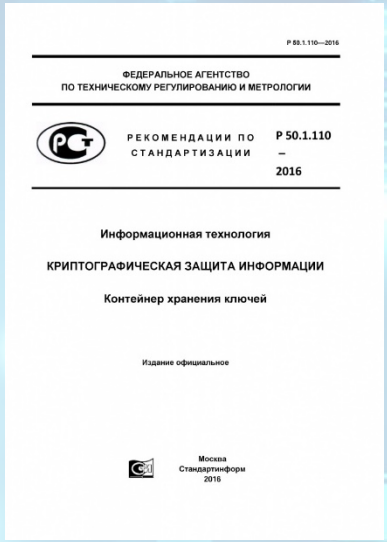
2022

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

2025

Документы по стандартизации - ЭДО


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 50.1.110 – 2016

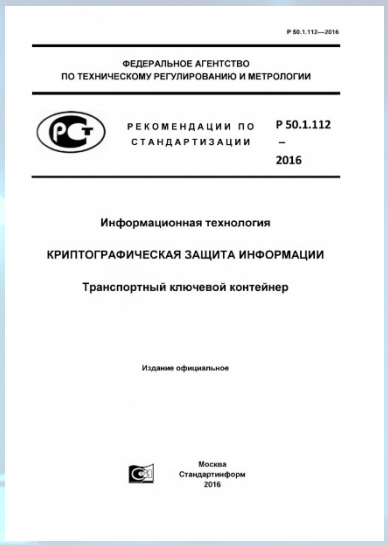
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Контейнер хранения ключей

Издание официальное

Москва
Стандартинформ
2016


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 50.1.112 – 2016

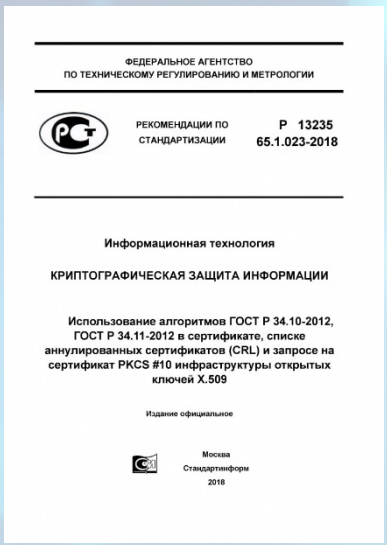
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Транспортный ключевой контейнер

Издание официальное

Москва
Стандартинформ
2016


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 13235 65.1.023-2018

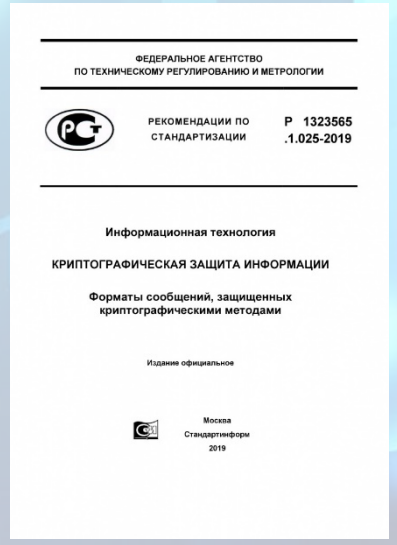
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509

Издание официальное

Москва
Стандартинформ
2018


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.025-2019

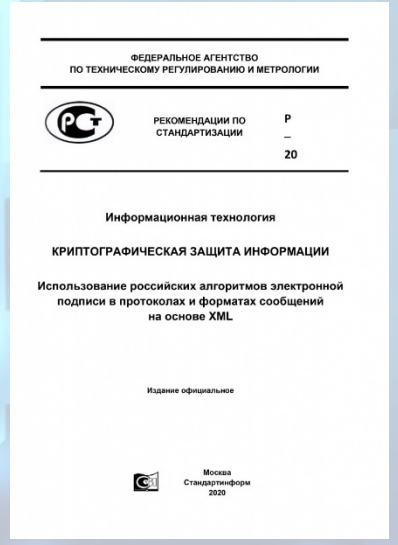
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Форматы сообщений, защищенных криптографическими методами

Издание официальное

Москва
Стандартинформ
2019


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р – 20

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML

Издание официальное

Москва
Стандартинформ
2020


ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ТК 26 МР 26.2.001-2021

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе штампов времени (TSP)

© Технический комитет по стандартизации «Криптографическая защита информации»

Москва
2021

2016

2022

2025

Р 50.1.110–2016	Р 50.1.111–2016	**Р 50.1.112–2016**	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	**Р 1323565.1.025-2019**	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

Документы по стандартизации - НСПК


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.007-2017

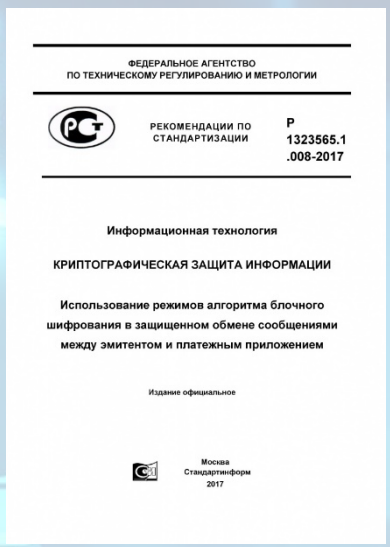
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.008-2017

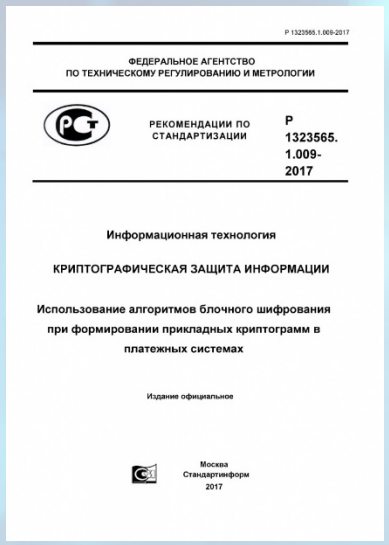
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование режимов алгоритма блочного шифрования в защищенном обмене сообщениями между эмитентом и платежным приложением

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.009-2017

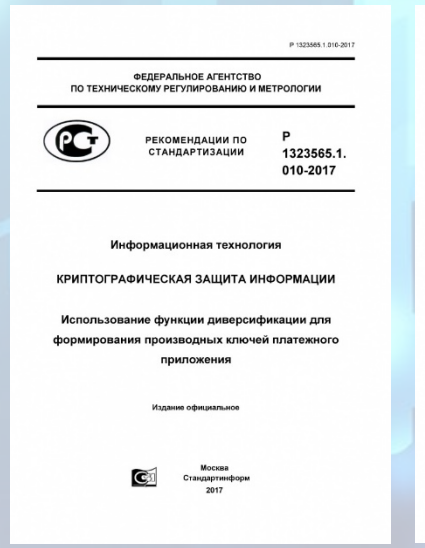
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.010-2017

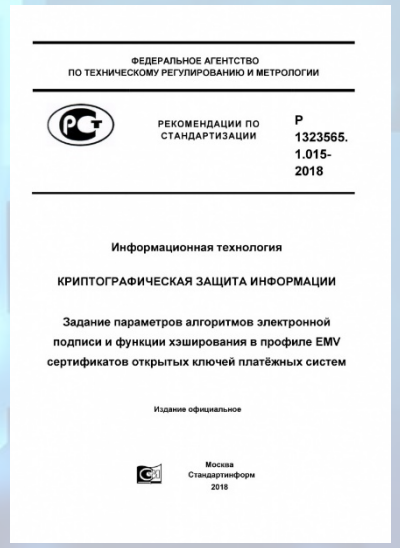
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование функции диверсификации для формирования производных ключей платежного приложения

Издание официальное

Москва Стандартинформ 2017


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.015-2018

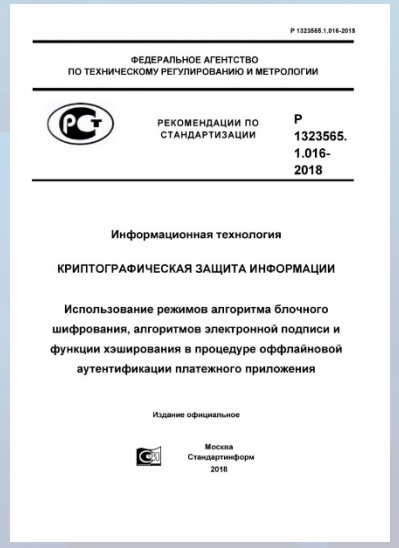
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Задание параметров алгоритмов электронной подписи и функции хэширования в профиле EMV сертификатов открытых ключей платёжных систем

Издание официальное

Москва Стандартинформ 2018


ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.016-2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре оффлайновой аутентификации платежного приложения

Издание официальное

Москва Стандартинформ 2018

2016

2022

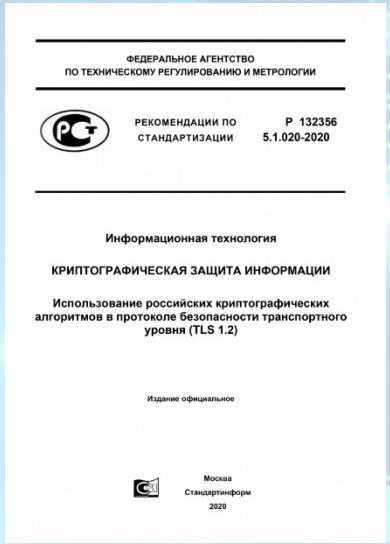
2025

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	**Р 1323565.1.007-2017**	**Р 1323565.1.008-2017**
Р 1323565.1.009-2017	**Р 1323565.1.010-2017**	**Р 1323565.1.011-2017**	Р 1323565.1.012-2017
Р 1323565.1.013-2017	**Р 1323565.1.015-2018**	**Р 1323565.1.016-2018**	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

Документы по стандартизации – протоколы



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 132356 5.1.020-2020

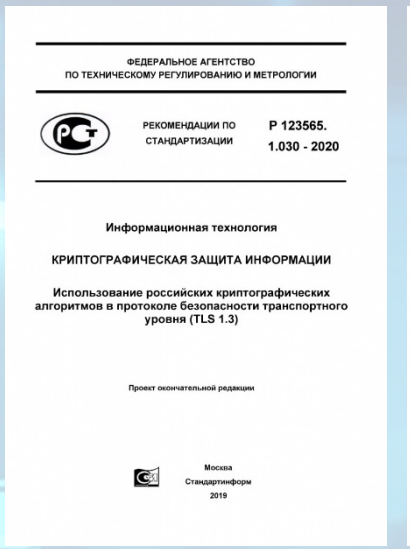
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)

Издание официальное

Москва
Стандартинформ
2020



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 123565. 1.030 - 2020

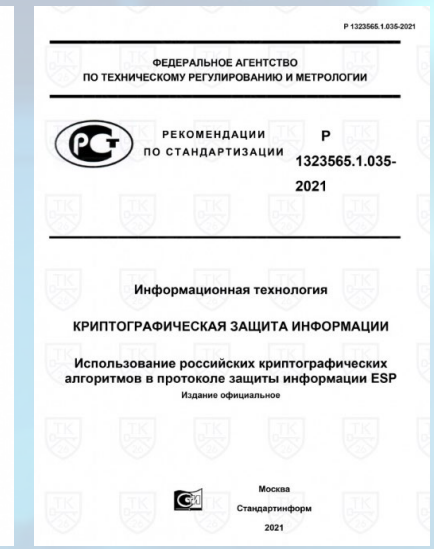
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)

Проект окончательной редакции

Москва
Стандартинформ
2019



Р 1323565.1.035-2021

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.035-2021

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе защиты информации ESP

Издание официальное

Москва
Стандартинформ
2021

0xC1,0x00	TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC	N	N	[RFC9189]
0xC1,0x01	TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC	N	N	[RFC9189]
0xC1,0x02	TLS_GOSTR341112_256_WITH_28147_CNT_IMIT	N	N	[RFC9189]
0xC1,0x03	TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L	N	N	[draft-smyshlyaev-tls13-gost-suites]
0xC1,0x04	TLS_GOSTR341112_256_WITH_MAGMA_MGM_L	N	N	[draft-smyshlyaev-tls13-gost-suites]
0xC1,0x05	TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S	N	N	[draft-smyshlyaev-tls13-gost-suites]
0xC1,0x06	TLS_GOSTR341112_256_WITH_MAGMA_MGM_S	N	N	[draft-smyshlyaev-tls13-gost-suites]

32	ENCR_KUZNYECHIK_MGM_KTREE	[RFC9227]	[RFC9227]
33	ENCR_MAGMA_MGM_KTREE	[RFC9227]	[RFC9227]
34	ENCR_KUZNYECHIK_MGM_MAC_KTREE	[RFC9227]	Not allowed
35	ENCR_MAGMA_MGM_MAC_KTREE	[RFC9227]	Not allowed

2016

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	**Р 1323565.1.020-2020**	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	**Р 1323565.1.030-2020**	Р 1323565.1.032-2020
Р 1323565.1.033-2020	**Р 1323565.1.034-2020**	**Р 1323565.1.035-2021**	

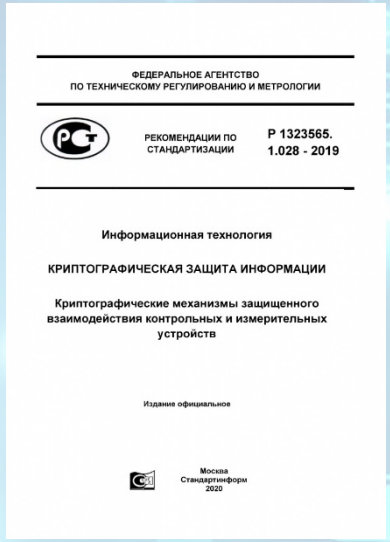
2022

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

2025

Документы по стандартизации - Интернета вещей


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.028 - 2019

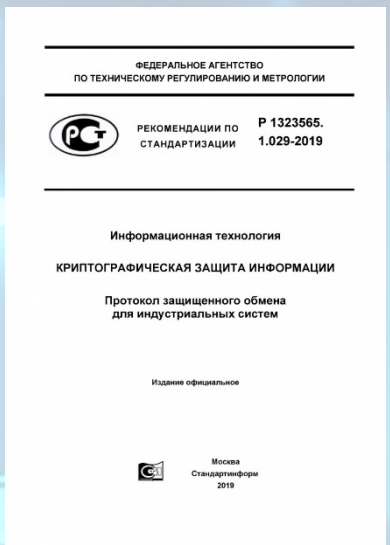
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств

Издание официальное

Москва
Стандартинформ
2020


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.029-2019

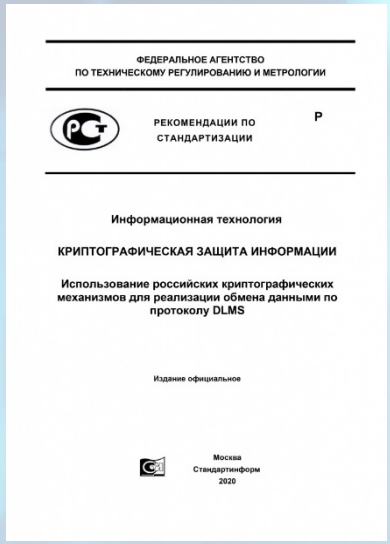
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол защищенного обмена для индустриальных систем

Издание официальное

Москва
Стандартинформ
2019


ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS

Издание официальное

Москва
Стандартинформ
2020

2016

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	**Р 1323565.1.029-2019**	Р 1323565.1.030-2020	**Р 1323565.1.032-2020**
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

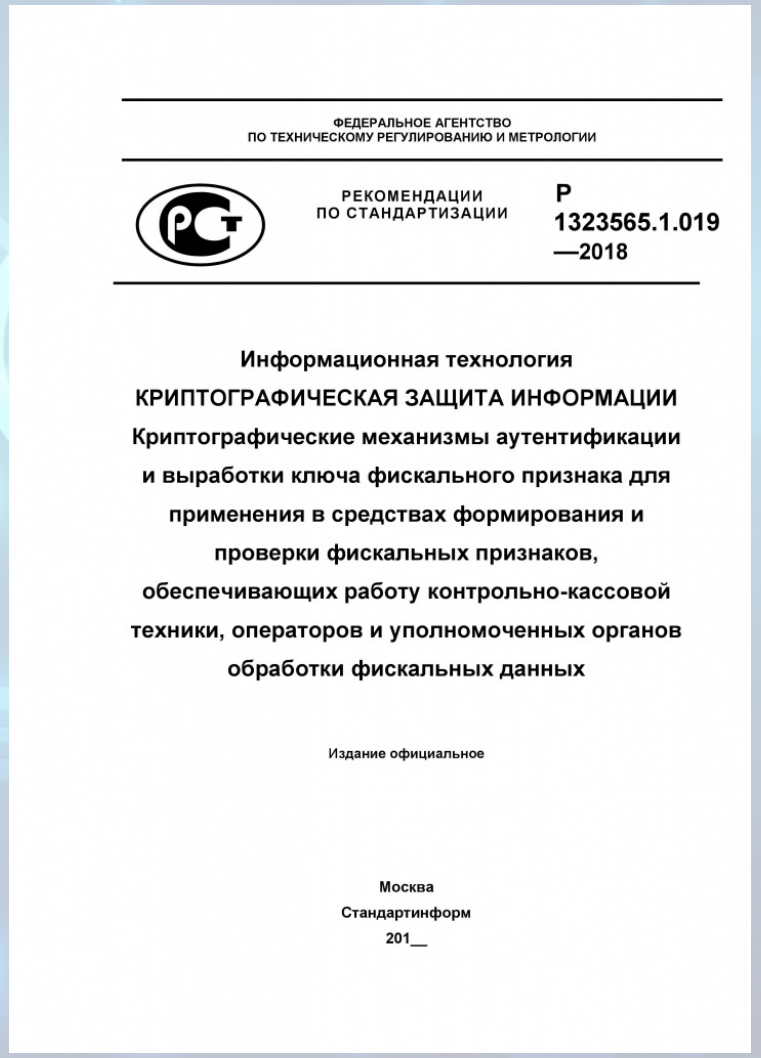
2022

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

2025

Документы по стандартизации - ККТ



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ
ПО СТАНДАРТИЗАЦИИ

Р
1323565.1.019
—2018

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
Криптографические механизмы аутентификации
и выработки ключа фискального признака для
применения в средствах формирования и
проверки фискальных признаков,
обеспечивающих работу контрольно-кассовой
техники, операторов и уполномоченных органов
обработки фискальных данных

Издание официальное

Москва
Стандартинформ
201__

2016

2022

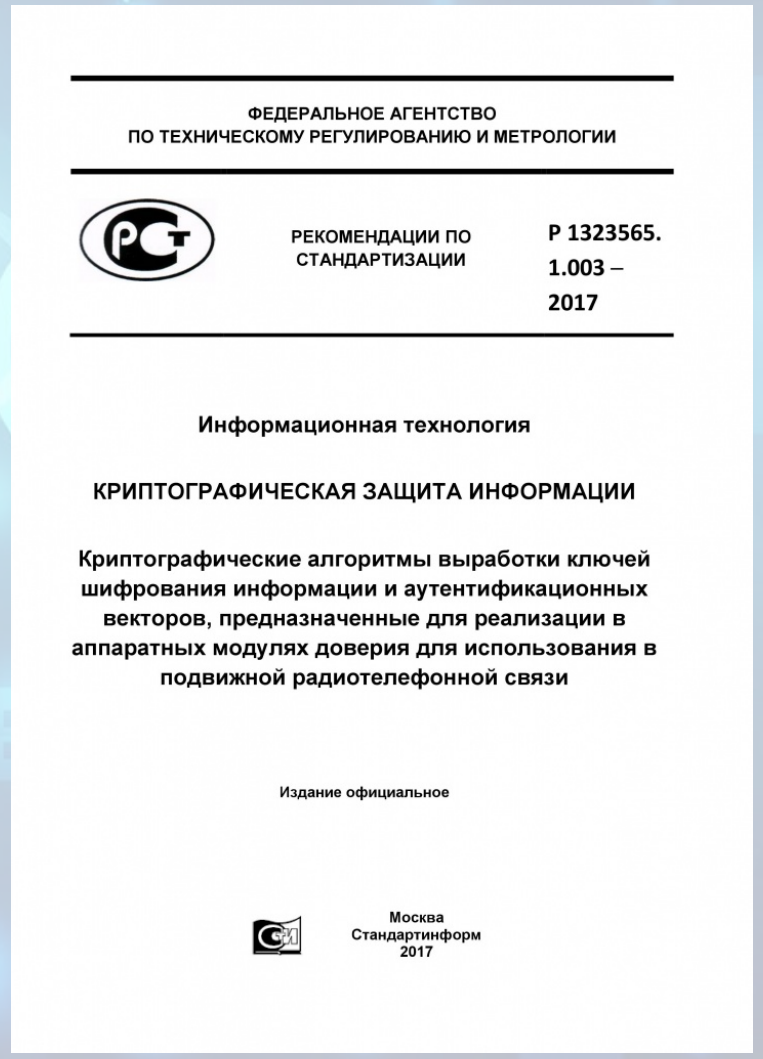
2025

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	**Р 1323565.1.019-2018**	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

Документы по стандартизации – 3G/4G



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.003 – 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

Издание официальное

Москва
Стандартинформ
2017

2016

2022

2025

Р 50.1.110–2016	Р 50.1.111–2016	Р 50.1.112–2016	Р 50.1.113–2016
Р 50.1.114–2016	Р 50.1.115–2016	Р 1323565.1.003-2017	Р 1323565.1.004-2017
Р 1323565.1.005-2017	Р 1323565.1.006-2017	Р 1323565.1.007-2017	Р 1323565.1.008-2017
Р 1323565.1.009-2017	Р 1323565.1.010-2017	Р 1323565.1.011-2017	Р 1323565.1.012-2017
Р 1323565.1.013-2017	Р 1323565.1.015-2018	Р 1323565.1.016-2018	Р 1323565.1.017-2018
Р 1323565.1.018-2018	Р 1323565.1.019-2018	Р 1323565.1.020-2020	Р 1323565.1.022-2018
Р 1323565.1.023-2022	Р 1323565.1.024-2019	Р 1323565.1.025-2019	Р 1323565.1.026-2019
Р 1323565.1.028-2019	Р 1323565.1.029-2019	Р 1323565.1.030-2020	Р 1323565.1.032-2020
Р 1323565.1.033-2020	Р 1323565.1.034-2020	Р 1323565.1.035-2021	

Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	Проект Р
Проект Р	Проект Р	Проект Р	

Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	Проект МР
Проект МР	Проект МР	Проект МР	Проект МР	Проект МР	

Новые направления стандартизации

3.1. Квантовые системы связи:

- защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации, описанный в методических рекомендациях МР 26.4.004 – 2021;

- ключевые системы сетей шифрованной связи с использованием квантовой криптографической сети, которые будут описаны в разрабатываемых в настоящее время методических рекомендациях;

3.2. Постквантовые криптографические алгоритмы:

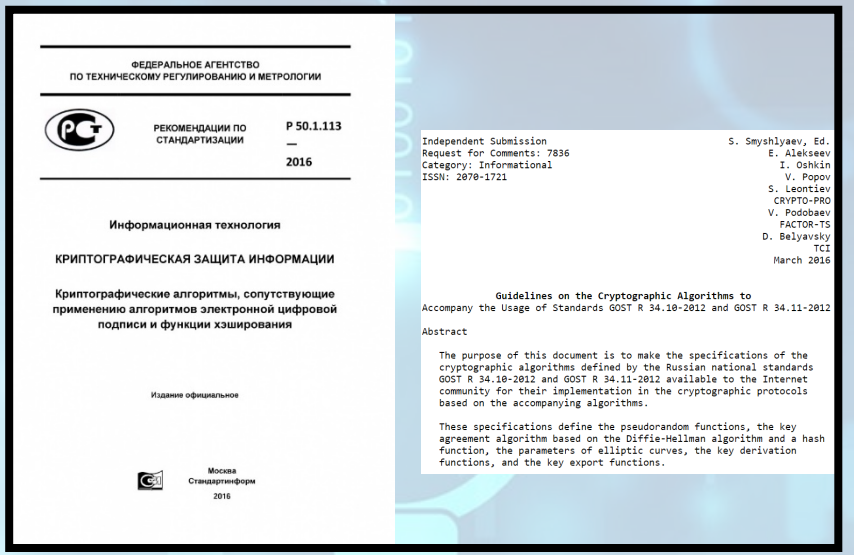
- схема электронной подписи, построенной на основе кодов, исправляющих ошибки, которая будет описана в разрабатываемых методических рекомендациях;

- схема инкапсуляции ключа, построенная на основе изогений эллиптических кривых, которая будет описана в разрабатываемых методических рекомендациях;

- криптографические механизмы, построенные на основе хэш-функций, которые будут описаны в разрабатываемых методических рекомендациях;

- схема электронной подписи, построенной на решеток, которая будет описана в разрабатываемых методических рекомендациях, и т.д.;

Стандартизация в IETF



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 50.1.113 — 2016

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

Издание официальное

Москва
Стандартинформ
2016

Independent Submission
Request for Comments: 7836
Category: Informational
ISSN: 2070-1721

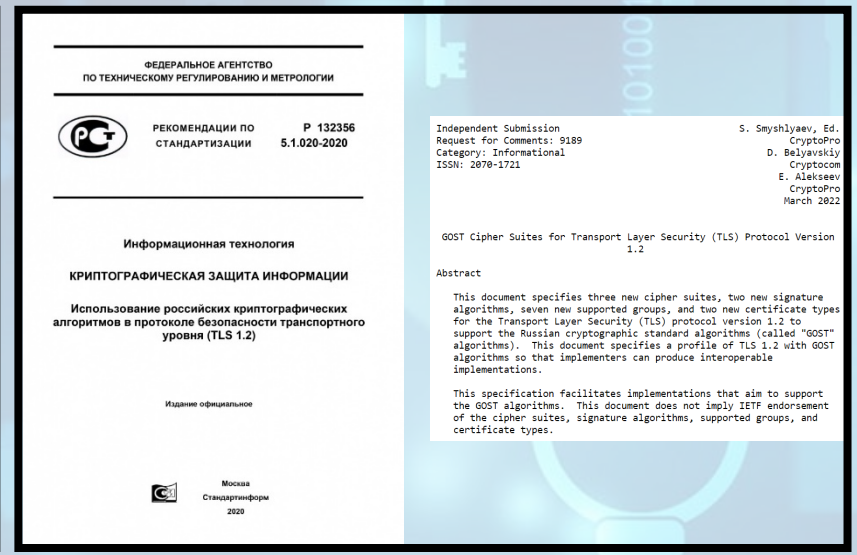
S. Smyshlyaev, Ed.
E. Alekseev
I. Oshkin
V. Popov
S. Leontiev
CRYPTO-PRO
V. Podobaev
FACTOR-TS
D. Belyavsky
TCI
March 2016

Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012

Abstract

The purpose of this document is to make the specifications of the cryptographic algorithms defined by the Russian national standards GOST R 34.10-2012 and GOST R 34.11-2012 available to the Internet community for their implementation in the cryptographic protocols based on the accompanying algorithms.

These specifications define the pseudorandom functions, the key agreement algorithm based on the Diffie-Hellman algorithm and a hash function, the parameters of elliptic curves, the key derivation functions, and the key export functions.



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 132356 5.1.020-2020

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)

Издание официальное

Москва
Стандартинформ
2020

Independent Submission
Request for Comments: 9189
Category: Informational
ISSN: 2070-1721

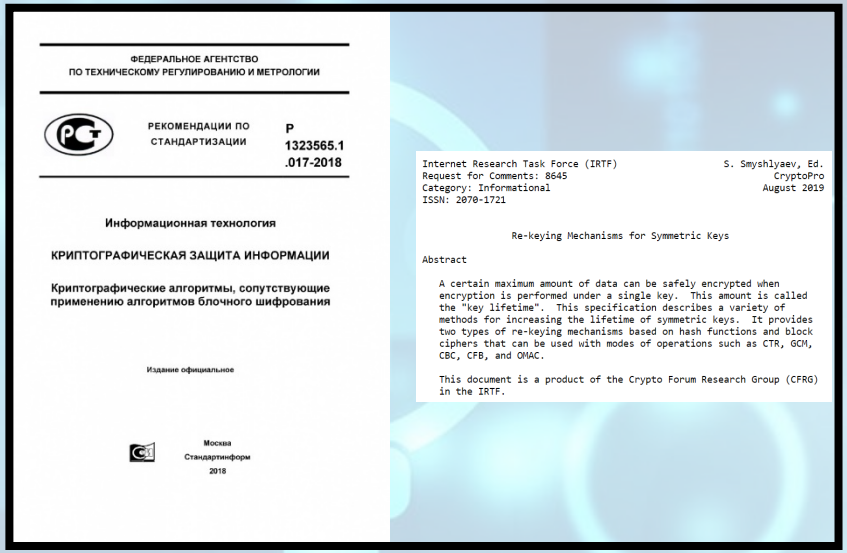
S. Smyshlyaev, Ed.
CryptoPro
D. Belyavskiy
Cryptocom
E. Alekseev
CryptoPro
March 2022

GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.2

Abstract

This document specifies three new cipher suites, two new signature algorithms, seven new supported groups, and two new certificate types for the Transport Layer Security (TLS) protocol version 1.2 to support the Russian cryptographic standard algorithms (called "GOST" algorithms). This document specifies a profile of TLS 1.2 with GOST algorithms so that implementers can produce interoperable implementations.

This specification facilitates implementations that aim to support the GOST algorithms. This document does not imply IETF endorsement of the cipher suites, signature algorithms, supported groups, and certificate types.



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.017-2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Издание официальное

Москва
Стандартинформ
2018

Internet Research Task Force (IRTF)
Request for Comments: 8645
Category: Informational
ISSN: 2070-1721

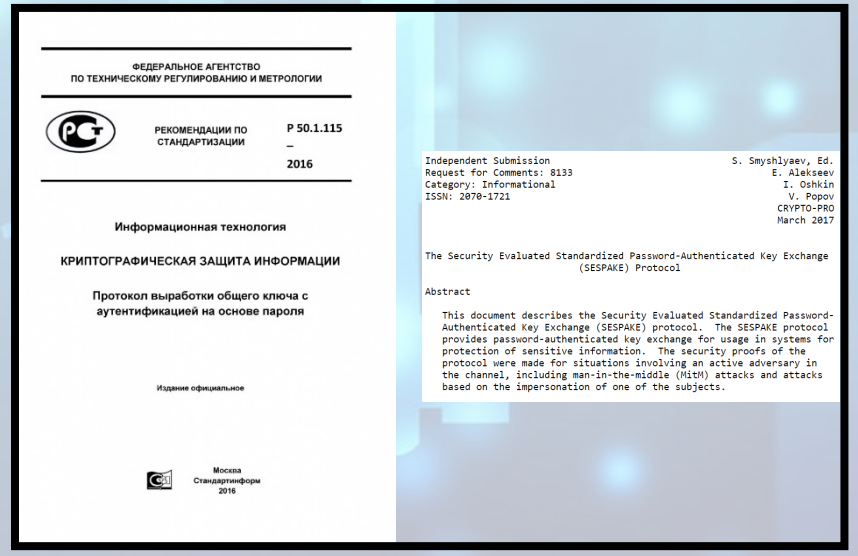
S. Smyshlyaev, Ed.
CryptoPro
August 2019

Re-keying Mechanisms for Symmetric Keys

Abstract

A certain maximum amount of data can be safely encrypted when encryption is performed under a single key. This amount is called the "key lifetime". This specification describes a variety of methods for increasing the lifetime of symmetric keys. It provides two types of re-keying mechanisms based on hash functions and block ciphers that can be used with modes of operations such as CTR, GCM, CBC, CFB, and OMAC.

This document is a product of the Crypto Forum Research Group (CFRG) in the IRTF.



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 50.1.115 — 2016

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол выработки общего ключа с аутентификацией на основе пароля

Издание официальное

Москва
Стандартинформ
2016

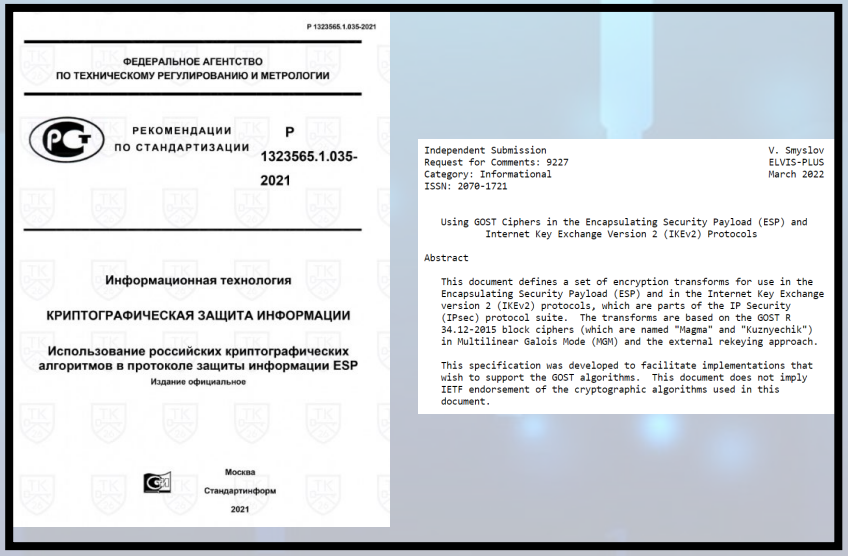
Independent Submission
Request for Comments: 8133
Category: Informational
ISSN: 2070-1721

S. Smyshlyaev, Ed.
E. Alekseev
I. Oshkin
V. Popov
CRYPTO-PRO
March 2017

The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol

Abstract

This document describes the Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) protocol. The SESPAKE protocol provides password-authenticated key exchange for usage in systems for protection of sensitive information. The security proofs of the protocol were made for situations involving an active adversary in the channel, including man-in-the-middle (MitM) attacks and attacks based on the impersonation of one of the subjects.



Р 1323565.1.035-2021

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р 1323565.1.035-2021

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование российских криптографических алгоритмов в протоколе защиты информации ESP

Издание официальное

Москва
Стандартинформ
2021

Independent Submission
Request for Comments: 9227
Category: Informational
ISSN: 2070-1721

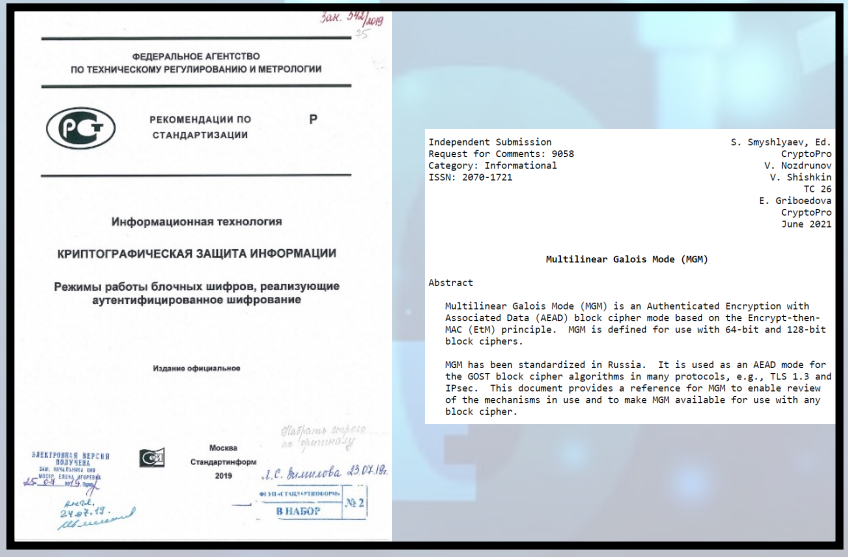
V. Smyslov
ELVIS-PLUS
March 2022

Using GOST Ciphers in the Encapsulating Security Payload (ESP) and Internet Key Exchange Version 2 (IKEv2) Protocols

Abstract

This document defines a set of encryption transforms for use in the Encapsulating Security Payload (ESP) and in the Internet Key Exchange version 2 (IKEv2) protocols, which are parts of the IP Security (IPsec) protocol suite. The transforms are based on the GOST R 34.12-2015 block ciphers (which are named "Magma" and "Kuznyechik") in Multilinear Galois Mode (MGM) and the external rekeying approach.

This specification was developed to facilitate implementations that wish to support the GOST algorithms. This document does not imply IETF endorsement of the cryptographic algorithms used in this document.



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ Р

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров, реализующие аутентифицированное шифрование

Издание официальное

Москва
Стандартинформ
2019

Independent Submission
Request for Comments: 9058
Category: Informational
ISSN: 2070-1721

S. Smyshlyaev, Ed.
CryptoPro
V. Nozdrunov
V. Shishkin
TC 26
E. Griboedova
CryptoPro
June 2021

Multilinear Galois Mode (MGM)

Abstract

Multilinear Galois Mode (MGM) is an Authenticated Encryption with Associated Data (AEAD) block cipher mode based on the Encrypt-then-MAC (EtM) principle. MGM is defined for use with 64-bit and 128-bit block ciphers.

MGM has been standardized in Russia. It is used as an AEAD mode for the GOST block cipher algorithms in many protocols, e.g., TLS 1.3 and IPsec. This document provides a reference for MGM to enable review of the mechanisms in use and to make MGM available for use with any block cipher.

ВЫСШИЙ ГОСУДАРСТВЕННЫЙ СОВЕТ СОЮЗНОГО ГОСУДАРСТВА

ДЕКРЕТ

от 4 ноября 2021 г. № 6

Минск – Москва

Об Основных направлениях реализации положений Договора о создании Союзного государства на 2021 – 2023 годы

В целях реализации Договора о создании Союзного государства от 8 декабря 1999 года (далее – Договор), а также унификации, гармонизации и сближения законодательства государств – участников Союзного государства, Высший Государственный Совет Союзного государства **постановляет:**

Основные направления реализации положений Договора о создании Союзного государства на 2021 – 2023 годы

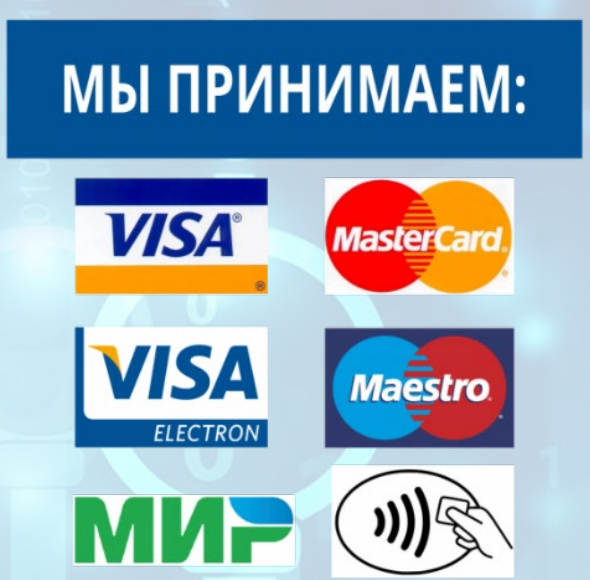
1. Программа интеграции информационных систем маркировки товаров.

2. Программа по гармонизации требований в области обеспечения информационной безопасности в финансовой сфере (в части компетенции Банка России и Национального банка Республики Беларусь).

3. Программа по интеграции платежных систем в области национальных систем платежных карт, систем передачи финансовых сообщений и расчетов, системы быстрых платежей…

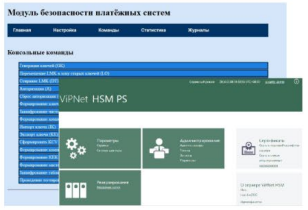
4. Программа по интеграции информационных систем государственных контролирующих органов по прослеживаемости товаров.

Инфраструктура платежных карт Союзного государства



Программно-аппаратный комплекс ViPNet HSM PS — надежное и современное российское решение для обеспечения безопасности финансовых операций в платежных системах «Мир», Visa и MasterCard.

Платформа ViPNet HSM PS успешно применяется для обработки платежных транзакций, поддержки эмиссии банковских карт, а также выполняет функции центра сертификации платежных систем.



Веб-интерфейс ViPNet HSM PS

Задняя панель ViPNet HSM PS

Внешний вид ViPNet HSM

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«4» июня 2020 г. № 719-П

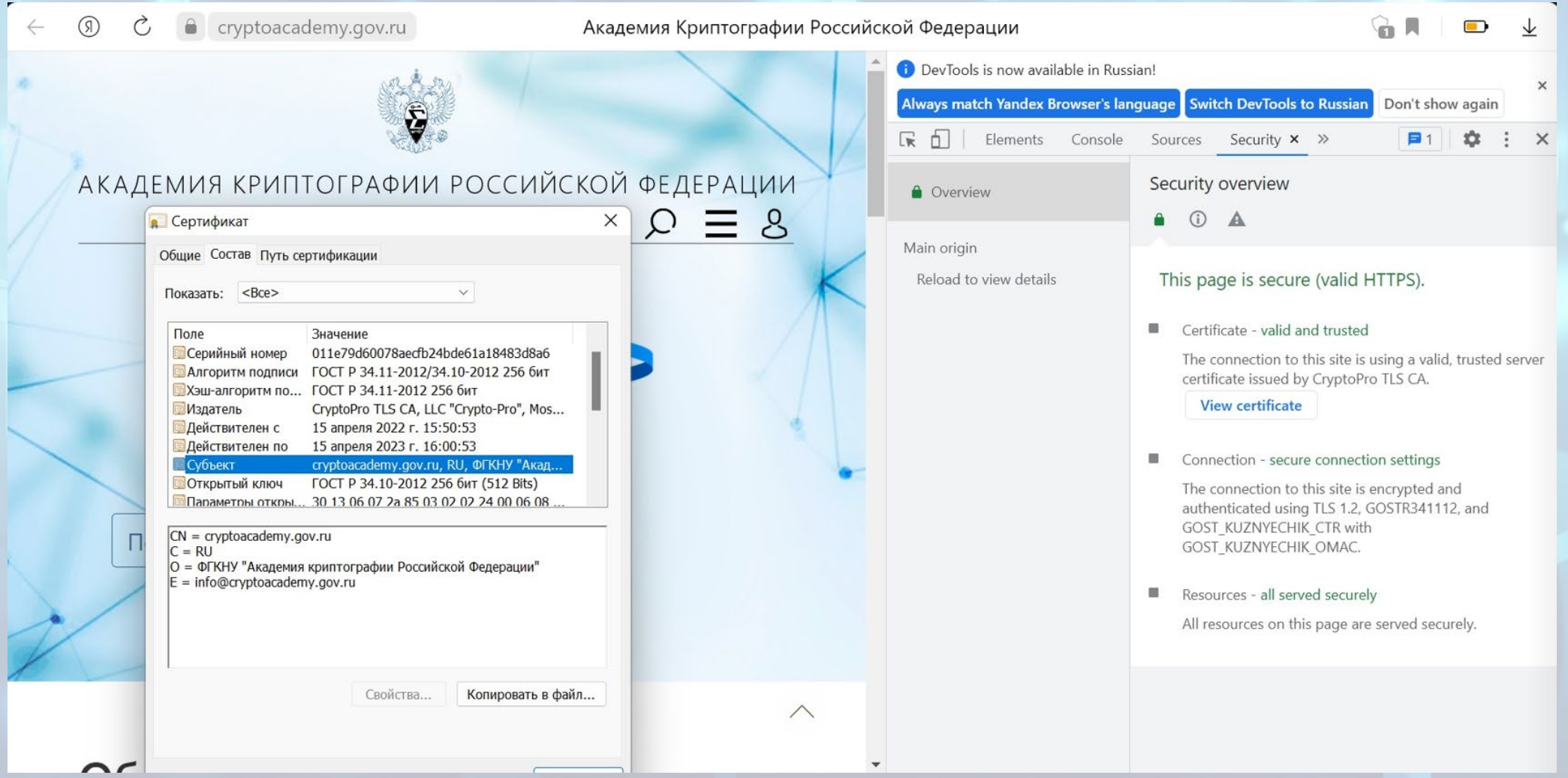
г. Москва

ЗАРЕГИСТРИРОВАНО
Регистрационный № 59991
от "23" сентября 2020 г.

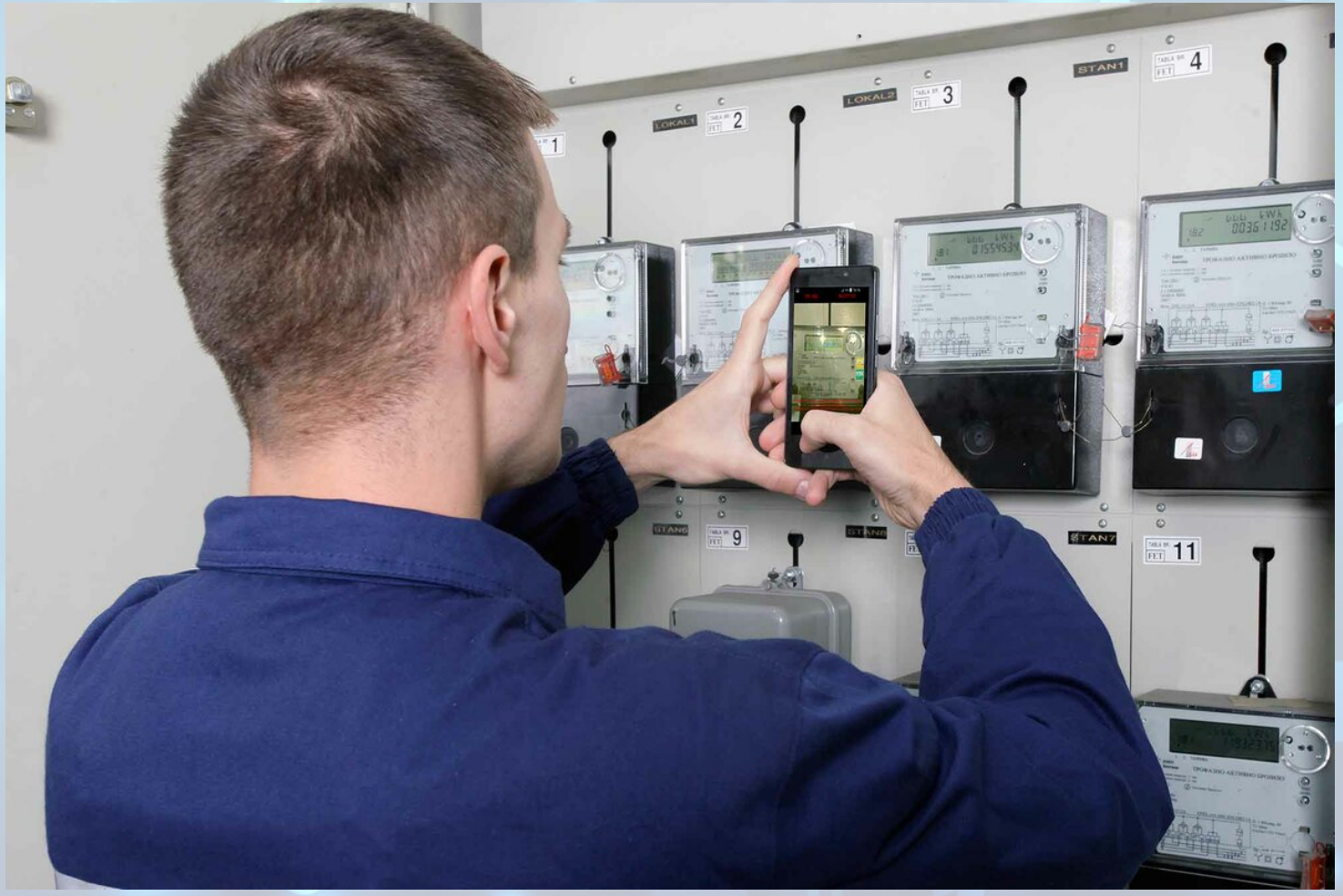
О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств

Настоящее Положение на основании части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) устанавливает требования к обеспечению операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами услуг информационного обмена, поставщиками платежных приложений, операторами платежных систем, операторами услуг платежной инфраструктуры защиты информации при осуществлении переводов денежных средств, а также порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств в рамках осуществляемого Банком России надзора в национальной платежной системе.

Защищенные технологии доступа к информационным ресурсам Союзного государства



Учет ресурсов на базе технологий Интернета вещей



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 19 июня 2020 г. № 890

МОСКВА

О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)

В соответствии с Федеральным законом "Об электроэнергетике" Правительство Российской Федерации **п о с т а н о в л я е т :**

1. Утвердить прилагаемые Правила предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности).

2. Министерству энергетики Российской Федерации:

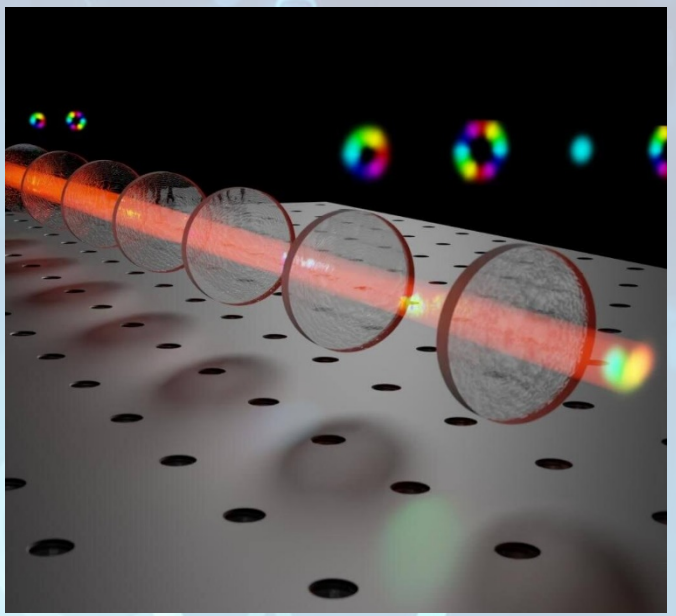
не позднее 12 месяцев со дня вступления в силу настоящего постановления утвердить методику и порядок кодификации мест установки приборов учета электрической энергии и точек поставки электрической энергии;

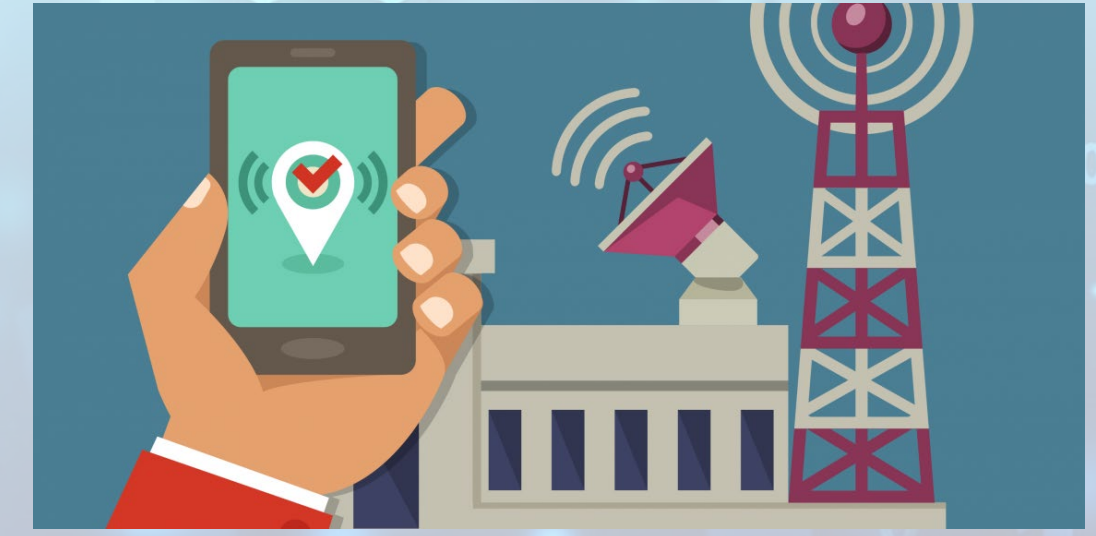
по согласованию с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации до 1 января 2021 г. утвердить перечень и спецификацию защищенных протоколов передачи данных, которые могут быть использованы для организации информационного обмена между владельцами и пользователями интеллектуальных систем учета электрической энергии (мощности), и разместить их на официальном сайте Министерства энергетики Российской Федерации в информационно-телекоммуникационной сети "Интернет";

совместно с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному

Сети сотовой связи

Квантовые системы связи






КВ 208
КВ 207

Спасибо за внимание

Документы по стандартизации

ГОСТ 28147-89