INTERNATIONAL STANDARD

ISO 20215

First edition
2015-08-15

Space data and information transfer systems — CCSDS cryptographic algorithms

Systèmes de transfert des informations et données spatiales — Algorithmes cryptographiques CCSDS

Reference number
ISO 20215:2015(E)

© ISO 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 20215 was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 352.0-B-1, November 2012) and was adopted (without modifications except those stated in clause 2 of this International Standard) by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 13, *Space data and information transfer systems*.

© ISO 2015 – All rights reserved

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

CCSDS CRYPTOGRAPHIC ALGORITHMS

RECOMMENDED STANDARD

CCSDS 352.0-B-1

BLUE BOOK

November 2012

AUTHORITY

Issue:	Recommended Standard, Issue 1
Date:	November 2012
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

© ISO 2015 – All rights reserved

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommended Standards** and are not considered binding on any Agency.

This **Recommended Standard** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommendation** is entirely voluntary. Endorsement, however, indicates the following understandings:

- Whenever a member establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommended Standard**. Establishing such a **standard** does not preclude other provisions which a member may develop.
- Whenever a member establishes a CCSDS-related **standard**, that member will provide other CCSDS members with the following information:
  - -- The **standard** itself.
  - -- The anticipated date of initial operational capability.
  - -- The anticipated duration of operational service.
- Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommended Standard** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than three years from its date of issuance, this **Recommended Standard** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Standard** is issued, existing CCSDS-related member standards and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such standards or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new standards and implementations towards the later version of the Recommended Standard.

© ISO 2015 – All rights reserved

FOREWORD

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS shall not be held responsible for identifying any or all such patent rights.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Standard is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

© ISO 2015 – All rights reserved

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

© ISO 2015 – All rights reserved

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 352.0-B-1	CCSDS Cryptographic Algorithms, Recommended Standard, Issue 1	November 2012	Original issue

© ISO 2015 – All rights reserved

CONTENTS

Section Page

1 INTRODUCTION 1-1

1.1 PURPOSE OF THIS RECOMMENDED STANDARD 1-1
1.2 SCOPE 1-1
1.3 APPLICABILITY 1-2
1.4 RATIONALE 1-2
1.5 DOCUMENT STRUCTURE 1-2
1.6 NOMENCLATURE 1-2
1.7 REFERENCES 1-3

2 OVERVIEW 2-1

2.1 GENERAL OVERVIEW 2-1
2.2 ENCRYPTION OVERVIEW 2-1
2.3 AUTHENTICATION/INTEGRITY OVERVIEW 2-2
2.4 AUTHENTICATED ENCRYPTION 2-3

3 ENCRYPTION ALGORITHMS 3-1

3.1 ALGORITHM AND MODE 3-1
3.2 CRYPTOGRAPHIC KEY SIZE 3-1
3.3 ALGORITHM MODE OF OPERATION 3-1
3.4 AUTHENTICATED ENCRYPTION 3-1

4 AUTHENTICATION ALGORITHMS 4-1

4.1 OVERVIEW 4-1
4.2 CCSDS HASH MESSAGE BASED AUTHENTICATION 4-1
4.3 CIPHER-BASED AUTHENTICATION 4-2
4.4 DIGITAL SIGNATURE BASED AUTHENTICATION 4-2

ANNEX A SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE) A-1
ANNEX B INFORMATIVE REFERENCES (INFORMATIVE) B-1
ANNEX C ABBREVIATIONS AND ACRONYMS (INFORMATIVE) C-1

© ISO 2015 – All rights reserved

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDED STANDARD

This Recommended Standard provides the recommendation for standard CCSDS security algorithms.

A single, symmetric encryption algorithm is recommended for use by all CCSDS missions. In addition, a specific mode of operation for the algorithm is also recommended.

This Recommended Standard provides several alternative authentication/integrity algorithms which may be chosen for use by individual missions depending on their specific mission environments.

This Recommended Standard does not specify how, when, or where these algorithms should be implemented or used. Those specifics are left to the individual mission planners based on the mission security requirements and the results of the mission risk analysis. Suggestions for the use of these algorithms may be found in *The Application of CCSDS Protocols to Secure Systems* (reference [B1]), *Security Architecture for Space Data Systems* (reference [B17]), and *Space Data Link Security Protocol* (reference [B23]).

By using standardized, well-known algorithms, the use of high-quality cryptography and authentication is ensured, the potential rewards of economies of scale through the ability to buy off-the-shelf products is enabled, and the potential for interoperability among missions choosing the same algorithm is assured.

The implementer shall take into account that the use of this Recommended Standard alone does not mitigate all security risks related to confidentiality, integrity, and authentication. An information security risk assessment is necessary to identify additional security risks.

1.2 SCOPE

The algorithms contained in this document are recommended for use on space missions with a requirement for information (e.g., data, voice, and video) confidentiality, authentication, or authenticated confidentiality. The algorithms may be employed on any or all mission communications links such as the forward space link (e.g., telecommand), the return space link (e.g., telemetry, science data), as well as across the ground data network. They could as well be used to ensure confidentiality and authenticity of stored data.

A symmetric algorithm assumes that all communicating entities possess a shared secret (i.e., a ‘key’) which enables them to encrypt, decrypt, and authenticate information shared among them. The manner in which the shared secret is distributed and managed (key management) is not within the scope of this document. Further information on key management can be found in *Space Missions Key Management Concept* (reference [B22]).

© ISO 2015 – All rights reserved

1.3 APPLICABILITY

This Recommended Standard is applicable to all civilian space missions with a requirement for information confidentiality, authentication, and authenticated confidentiality.

While the use of security services is encouraged for all missions, particularly on command links, the results of a risk analysis may reduce or eliminate its need on a mission-by-mission basis.

1.4 RATIONALE

Traditionally, security mechanisms have not been employed on civilian space missions. In recognition of the increased threat, there has been a steady trend towards the integration of security services and mechanisms. For example, ground network infrastructures typically make use of *controlled* or *protected* networks. However, telecommands, telemetry, and science payload data, are still, for the most part, transmitted over unencrypted and unauthenticated Radio Frequency (RF) channels. As the threat environment becomes more hostile, this concept of operation becomes much more susceptible to attacks.

This CCSDS Cryptographic Algorithm Recommended Standard is necessary because of the increasing interconnection of ground networks; the movement towards *joy-sticking* of instruments by principal investigators; the decreasing costs for hardware, potentially allowing cheap *rogue* ground stations to be established; and national trends towards enhancing mission security. These recommended algorithms establish a set of common denominators among all missions for implementing information security services.

1.5 DOCUMENT STRUCTURE

Four sections and three annexes make up this document. Section 1 provides introductory information, definitions, nomenclature, and normative references. Section 2 provides background and rationale for choice of the algorithms. Section 3 describes the encryption algorithm. Section 4 describes the authentication algorithms. Annex A discusses security considerations related to use of symmetric encryption on the space link. Annex B provides informative references. Annex C is a glossary of abbreviations and acronyms used in the document.

1.6 NOMENCLATURE

1.6.1 NORMATIVE TEXT

The following conventions apply for the normative specifications in this Recommended Standard:

a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;

© ISO 2015 – All rights reserved

b) the word ‘should’ implies an optional, but desirable, specification;

c) the word ‘may’ implies an optional specification;

d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.6.2 INFORMATIVE TEXT

In the normative sections of this document (sections 3 and 4), informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

– Overview;

– Background;

– Rationale;

– Discussion.

1.7 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Standard. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommended Standard are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS documents.

[1] *Advanced Encryption Standard (AES).* Federal Information Processing Standards Special Publication 197. Gaithersburg, Maryland: NIST, 2001.

[2] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.* National Institute of Standards and Technology Special Publication 800-38A. Gaithersburg, Maryland: NIST, 2001.

[3] R. Housley. *Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP).* RFC 3686. Reston, Virginia: ISOC, January 2004.

[4] Morris Dworkin. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* National Institute of Standards and Technology Special Publication 800-38D. Gaithersburg, Maryland: NIST, November 2007.

© ISO 2015 – All rights reserved