INTERNATIONAL STANDARD

ISO 20214

First edition
2015-08-15

Space data and information transfer systems — Security architecture for space data systems

Systèmes de transfert des informations et données spatiales — Architecture de sécurité pour les systèmes de données spatiales

Reference number
ISO 20214:2015(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 20214 was prepared by the Consultative Committee for Space Data Systems (CCSDS) (as CCSDS 351.0-M-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 Practices

SECURITY ARCHITECTURE FOR SPACE DATA SYSTEMS

RECOMMENDED PRACTICE

CCSDS 351.0-M-1

MAGENTA BOOK

November 2012

AUTHORITY

Issue:	Recommended Practice, 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* (CCSDS A02.1-Y-3), 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 **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** 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 Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

© ISO 2015 – All rights reserved

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *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

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 351.0-M-1	Security Architecture for Space Data Systems, Recommended Practice, Issue 1	November 2012	Original issue

© ISO 2015 – All rights reserved

CONTENTS

Section Page

1 INTRODUCTION 1-1

1.1 PURPOSE AND SCOPE 1-1
1.2 DOCUMENT STRUCTURE 1-2
1.3 GLOSSARY OF TERMS 1-3
1.4 NOMENCLATURE 1-3

2 THE CCSDS REFERENCE ARCHITECTURE 2-1

2.1 INTRODUCTION 2-1
2.2 BACKGROUND 2-1
2.3 CCSDS REFERENCE ARCHITECTURE 2-1

3 GENERAL SECURITY PRINCIPLES 3-1

3.1 GENERAL 3-1
3.2 PHYSICAL SECURITY 3-1
3.3 INFORMATION SECURITY 3-1
3.4 TRANSMISSION SECURITY 3-2
3.5 PROCEDURES 3-2
3.6 MISSION SECURITY DOCUMENTATION 3-2

4 SECURITY AND THE CCSDS REFERENCE ARCHITECTURE 4-1

4.1 OVERVIEW 4-1
4.2 SECURITY AND THE ENTERPRISE VIEW 4-1
4.3 SECURITY AND THE CONNECTIVITY VIEW 4-3
4.4 SECURITY AND THE FUNCTIONAL VIEW 4-5
4.5 SECURITY AND THE INFORMATION VIEW 4-7
4.6 SECURITY AND THE COMMUNICATIONS VIEW 4-9

5 SECURITY ARCHITECTURE PRINCIPLES 5-1

5.1 OVERVIEW 5-1
5.2 OPEN STANDARDS 5-1
5.3 PROTECTION THROUGH LAYERED SECURITY MECHANISMS 5-1
5.4 EXPANDABILITY 5-1
5.5 FLEXIBILITY 5-1
5.6 INTEROPERABILITY 5-1
5.7 KEY MANAGEMENT 5-2
5.8 ENCRYPTION ALGORITHM SELECTION 5-2

© ISO 2015 – All rights reserved

CONTENTS (continued)

Section Page

5.9 KERCKHOFF'S PRINCIPLE 5-2
5.10 FAULT TOLERANCE 5-2

6 MISSION PROFILES 6-1

6.1 OVERVIEW 6-1
6.2 GENERAL 6-1
6.3 HUMAN SPACEFLIGHT 6-1
6.4 EARTH OBSERVATION 6-2
6.5 COMMUNICATIONS 6-2
6.6 SCIENTIFIC 6-2
6.7 NAVIGATION 6-3
6.8 MULTI-ORGANIZATIONAL SPACECRAFT 6-4

7 PROPOSED ARCHITECTURE 7-1

7.1 REQUIREMENTS 7-1
7.2 SERVICES 7-1
7.3 PROPOSED SECURITY ARCHITECTURE 7-2
7.4 CCSDS SECURITY CORE SUITE 7-3
7.5 SECURITY CORE SUITE CONFIGURATION 7-6
7.6 EXPANDABILITY 7-8
7.7 EMERGENCY OPERATIONS 7-10

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

Figure

1-1 Relationship between This and Other CCSDS Documentation 1-2
4-1 Enterprise View 4-2
4-2 Connectivity View and Example Security Application Points 4-4
4-3 Example Analysis of the Functional View (Functions with Specific Security Requirements Shown in Red) 4-6
4-4 Information View and Security Implications 4-7
4-5 Communications View and Security Layer Choices 4-9
7-1 CCSDS Space Mission Protocols and Security Options 7-4
7-2 CCSDS Security Core Suite 7-6

© ISO 2015 – All rights reserved

CONTENTS (continued)

Figure Page

7-3 Example Security Architecture for ‘Mission 1’ 7-8
7-4 Security Architecture for a Simple Mission, Which Uses Only the Network Layer Security Subsystem from the Core Suite 7-9
7-5 A Simple Mission Using Its Own Transport Layer Security 7-10

© ISO 2015 – All rights reserved

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

1.1.1 PURPOSE

This document is intended as a high-level systems engineering reference to enable engineers to better understand the layered security concepts required to secure a space system. As such, this document is a Security Architecture for Space Data Systems (SASDS).

This architecture uses the views described in the Reference Architecture for Space Data Systems (reference [B1]) developed by the CCSDS Architecture Working Group.

The SASDS will be used:

- to establish an overall CCSDS conceptual framework for the incorporation of security into the data systems of space missions;
- to define common language and representation so that risks, requirements, and solutions in the area of security within space data systems can be readily communicated;
- to provide a source of information for the security architects on a space mission to use to develop the system security design;
- to facilitate development of standards in a consistent way so that any standard can be used with other appropriate standards in a system.

1.1.2 SCOPE

This document presents a security reference architecture for space data systems and is intended to provide a standardized approach for description of security within data system architectures and high-level designs, which individual working groups may use within CCSDS.

For further information regarding security's role in space systems, the reader is directed to the supporting CCSDS documentation listed in annex B.

© ISO 2015 – All rights reserved