The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

CCSDS AUTHENTICATION CREDENTIALS

RECOMMENDED STANDARD

CCSDS 357.0-B-1

BLUE BOOK

July 2019

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

CCSDS AUTHENTICATION CREDENTIALS

RECOMMENDED STANDARD

CCSDS 357.0-B-1

BLUE BOOK

July 2019

AUTHORITY

Issue:	Recommended Standard, Issue 1
Date:	July 2019
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-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the e-mail address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

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 five 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.

FOREWORD

The goal of this specification is to develop a profile to facilitate the use of X.509 certificates within space applications for those communities wishing to make use of X.509 technology. In order to relieve some of the obstacles to using X.509 certificates, this document defines a profile to promote certificate management systems for space interoperability. Some communities will need to supplement this profile in order to meet the requirements of specialized application domains or environments with additional authorization, assurance, or operational requirements.

The specification allows for protected simple authentication procedure in conformance with ISO/IEC 9594-8 standard for those communities that have performed an evaluation of its use.Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS has processes for identifying patent issues and for securing from the patent holder agreement that all licensing policies are reasonable and non-discriminatory. However, CCSDS does not have a patent law staff, and 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-4). 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 sent to the CCSDS Secretariat at the email address indicated on page i.

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 (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.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- 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.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- 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.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 357.0-B-1	CCSDS Authentication Credentials, Recommended Standard, Issue 1	July 2019	Original issue

CONTENTS

1 INTRODUCTION

1.1 SECURITY CREDENTIALS

A credential is a document or certificate that enables trust between entities. In the CCSDS space environment, credentials are needed to allow communicating entities to authenticate each other to determine potential authorization and access control actions. CCSDS recommends two types of credentials in this document: X.509 certificates and protected simple authentication. The X.509 certificates properties (references [1] and [2]) are specified by the Internet Engineering Task Force (IETF), and this document specifies its CCSDS profile. Protected simple authentication, as specified Information Technology Open Systems Interconnection ISO 9594-8 (reference [3]), is recommended in this document as an alternative to X.509.

1.2 PURPOSE

This CCSDS Recommended Standard provides the specification for credentials to be used for authentication by CCSDS missions and ground systems.

1.3 SCOPE

This Recommended Standard may be used by any CCSDS program that requires authentication.

1.4 APPLICABILITY

This Recommended Standard applies to any CCSDS mission requiring end-to-end confidentiality, authentication, or integrity from the sender to the receiver.

1.5 RATIONALE

Many CCSDS missions require security services to protect commanding (command authentication, command confidentiality, command integrity) and payload data (confidentiality, integrity). This document specifies CCSDS ‘credential profiles’ to enable the establishment of trust relationships between CCSDS entities.

1.6 DEFINITIONS

This document uses terms defined in references [4] and [5].

1.7 REFERENCES

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

[1] D. Cooper, et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280. Reston, Virginia: ISOC, May 2008.

[2] P. Yee. *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 6818. Reston, Virginia: ISOC, January 2013.

[3] *Information Technology—Open Systems Interconnection—The Directory: Public-Key and Attribute Certificate Frameworks*. 7th ed. International Standard, ISO/IEC 9594-8:2014. Geneva: ISO, 2014.

[4] *Information Security Glossary of Terms*. Issue 2. Recommendation for Space Data System Practices (Magenta Book), CCSDS 350.8-M-2. Forthcoming.

[5] R. Shirey. *Internet Security Glossary*. RFC 2828. Reston, Virginia: ISOC, May 2000.

[6] *Time Code Formats*. Issue 4. Recommendation for Space Data System Standards (Blue Book), CCSDS 301.0-B-4. Washington, D.C.: CCSDS, November 2010.

[7] K. Moriarty, ed. *PKCS #12: Personal Information Exchange Syntax v1.1*. RFC 7292. Reston, Virginia: ISOC, July 2014.

[8] *CCSDS Cryptographic Algorithms*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 352.0-B-1. Washington, D.C.: CCSDS, November 2012.

2 OVERVIEW

2.1 INTRODUCTION

Credentials consist of information that attests to the identity or other attributes of an individual or entity, called the subject of the credentials. Some paper credentials include passports, birth certificates, driver's licenses, and employee identity cards. The authenticity of credentials is established by complex mechanisms that are difficult to copy or forge.

CCSDS recommends two forms of credentials: X.509 certificates and protected simple authentication.

X.509 certificates provide a more secure mechanism than does protected simple authentication. X.509 is the prime recommended credential for CCSDS. However, a mission planer may elect to use protected simple authentication for a space system.

2.2 X.509 CERTIFICATES

The properties of X.509 certificates are specified by the IETF (references [1] and [2]). The CCSDS X.509 profile is specified in this document. A digital certificate binds a user or service's identity to a public key by providing information about the subject of the certificate.

Certificate Authorities (CA) are responsible for all aspects of certificates issued to users and devices. This includes control over the enrollment process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-keying. The CA signs its produced certificates and instructions.

A subscriber is the entity (the user to whom, or device to which, a certificate is issued) whose Distinguished Name (DN) appears as the subject in a certificate; the subscriber asserts that it uses the key and certificate in accordance with this policy. The term 'subscriber' refers only to those entities that request certificates for uses other than signing and issuing certificates or certificate status information. CAs ensure that all subscribers are informed of their security obligations. The consequences of not complying with those obligations include the revocation of the certificates of subscribers found to have acted in a manner counter to those obligations.

Subscribers include, but are not limited to, the following categories of entities that may wish to conduct official business:

- Personnel: including part-time, intermittent, and temporary employees, contractors, commercial vendors, and agents;
- Organizations, branches, departments and personnel, and their contractors and agents;
- Workstations, guards and firewalls, routers, trusted servers (e.g., database, domain controller, FTP, and WWW), and other infrastructure components. These components

must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key. A Public Key Infrastructure (PKI) sponsor fills the role of a subscriber for groups, organizations, disabled personnel, and non-human system components named as public key certificate subjects.

2.3 PROTECTED SIMPLE AUTHENTICATION

Protected simple authentication (reference [3]) is intended to provide local authorization based upon the DN of a user, a bilaterally agreed upon password, and a bilateral understanding of the means of using and handling a password within a single domain. Simple authentication is primarily intended for local use only, that is, for peer entity authentication between one Directory User Agent (DUA) and one Directory System Agent (DSA), or between one DSA and another DSA. Simple authentication may be accomplished by

a) the transfer of the user's DN, password, and a random number and/or a timestamp, all of which are protected by applying a one-way function; or

b) the transfer of the protected information described in a) together with a random number and/or a timestamp, all of which are protected by applying a one-way function.

This process is the basic protected logon activity. The user name and password are entered, and the computer adds data to protect the information that is sent to the server, which verifies the information and either accepts or rejects the connection.

3 CREDENTIAL SPECIFICATION

3.1 X.509 CERTIFICATE SYNTAX

3.1.1 X.509 V3 certificates shall be used.

3.1.2 X.509 V3 certificates shall use generalized time.

3.1.3 X.509 V3 certificates shall utilize the CCSDS Calendar Segmented Time Code (CCS) (reference [6]).

3.1.4 X.509 V3 output file format shall use personal information exchange syntax (PKCS12) (reference [7]).

3.1.5 X.509 V3 certificates shall use a digital signature algorithm specified in reference [8].

3.2 PROTECTED SIMPLE AUTHENTICATION SPECIFICATION

3.2.1 Protected simple authentication shall be implemented as stated in reference [3].

3.2.2 Protected simple authentication shall use a password as stated in reference [3].

3.2.3 Protected simple authentication shall utilize the CCSDS Calendar Segmented (CCS) time code formats (reference [6]).

3.2.4 Protected simple authentication shall use a cipher algorithm specified in reference [8].

ANNEX A

IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA

(NORMATIVE)

A1 INTRODUCTION

A1.1 OVERVIEW

This annex provides the Implementation Conformance Statement (ICS) Requirements List (RL) for an implementation of CCSDS 357.0-B-1. The ICS for an implementation is generated by completing the RL in accordance with the instructions below. An implementation claiming conformance must satisfy the mandatory requirements referenced in the RL.

A1.2 ABBREVIATIONS AND CONVENTIONS

CRL distribution point: A directory entry or other distribution source for Certificate Revocation Lists (CRL). A CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. It is a managed parameter within the X.509 credential.

A1.3 CONFORMANCE

The Conformance Requirements List consists of information in tabular form. The status of features is indicated using the abbreviations and conventions described below.

Item Column

The item column contains sequential numbers for items in the table.

Feature Column

The feature column contains a brief descriptive name for a feature. It implicitly means ‘Is this feature supported by the implementation?’

Status Column

The status column uses the following notations:

- M mandatory;
- O optional;

– C conditional;

– X prohibited;

– I out of scope;

– N/A not applicable.

Support Column Symbols

The support column is to be used by the implementer to state whether a feature is supported by entering Y, N, or N/A, indicating:

Y Yes, supported by the implementation.

N No, not supported by the implementation.

N/A Not applicable.

The support column should also be used, when appropriate, to enter values supported for a given capability.

A1.4 INSTRUCTIONS FOR COMPLETING THE RL

An implementer shows the extent of compliance to the Recommended Standard by completing the RL; that is, the state of compliance with all mandatory requirements and the options supported are shown. The resulting completed RL is called an ICS. The implementer shall complete the RL by entering appropriate responses in the support or values-supported column, using the notation described in A1.3. If a conditional requirement is inapplicable, N/A should be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference X*i*, where *i* is a unique identifier, to an accompanying rationale for the noncompliance.

A2 ICS PROFORMA FOR CCSDS 357.0-B-1

A2.1 GENERAL INFORMATION

A2.1.1 Identification of ICS

Date of Statement (DD/MM/YYYY)	
ICS serial number	
System Conformance statement cross-reference	

A2.1.2 Identification of Implementation Under Test

Implementation Name	
Implementation Version	
Special Configuration	
Other Information	

A2.1.3 Identification of Supplier

Supplier	
Contact Point for Queries	
Implementation Name(s) and Versions	
Other information necessary for full identification, e.g., name(s) and version(s) for machines and/or operating systems; System Name(s)	

A2.1.4 Identification of Specification

CCSDS 357.0-B-1	
Have any exceptions been required? NOTE – A YES answer means that the implementation does not conform to the Recommended Standard. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming.	Yes [ ] No [ ]

A2.2 REQUIREMENTS LIST

Item #	Feature	Status	Support
1	ASN1	M	
2	DER	M	
3	X.509.V3	M	
4	tbsCertificate	M	
5	Version	M	
6	Serial number	M	
7	algorithm identification	M	
8	Issuer Signature	M	
9	Validity from	M	
10	Validity to	M	
11	Subject	M	
12	Subject algorithm identification	M	
13	Subject public Key	M	
14	Issuer Unique ID	O	
15	Subject Unique ID Public Key Info	O	
16	Universal Time Coordinated Time Certificate	M	
17	Generalized Time	M	
18	object identifiers (OID)	O	
19	Policy Mapping	O	
20	Subject Alternative Name	O	
21	Certificate Revocation Lists distribution points	O	
22	signatureAlgorithim	M	
23	signatureValue	M	

ANNEX B

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

B1 SECURITY CONSIDERATIONS

B1.1 INTRODUCTION

CCSDS utilization of X.509 and protected simple authentication procedure codifies the mechanisms to be used to validate the identities of users, applications, and devices. CCSDS organizations employ technologies to convey identity and to attest to the claims and trust are associated with those identities.

There are risks to CCSDS systems utilizing credentials if an attacker gains control of the credential-management system and can issue credentials. If a compromised credential-management process results, then there is a need to invalidate existing credentials and re-issue all credentials.

A CCSDS credential-management program would result in higher levels of assurance of the credentials while ensuring interoperability and ease the deployments of systems that are pre-tested to integrate with the credential-management system. The system would provide unified administration, compliance, and auditing of the X.509 credentials.

B1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT

B1.2.1 Overview

Standard credential usage will provide CCSDS missions with a standard means of authentication of communicating entities.

B1.2.2 Data Privacy

Credentials provide a means of identifying/authenticating entities in order to provide accurate access controls to ensure data privacy.

B1.2.3 Data Integrity

Credentials enable the means by which data integrity may be provided.

B1.2.4 Authentication of Communicating Entities

Authentication is necessary to ensure that the exchange of information is between intended entities. This document specifies the protocols used for CCSDS-compliant systems.

B1.2.5 Control of Access to Resources

The authenticity of X.509 certificates and/or protected simple authentication password-based credentials is frequently the basis for assigning access rights to individuals, groups, and system services.

B1.2.6 Availability of Resources

This document deals with exchange protocols and not internal system resources.

B1.2.7 Auditing of Resource Usage

The authenticity of X.509 certificates and/or protected simple authentication password-based credentials is frequently the basis for establishing accountability to specific individuals for actions taken on a system. Non-repudiation of user actions cannot be assured if credentials cannot be assured.

B1.3 POTENTIAL THREATS AND ATTACK SCENARIOS

The authenticity of an X.509 certificate is dependent upon the digital signature of the CA attesting to the credential. If the digital signature algorithm used by the CA is of insufficient cryptographic strength, a credential may be spoofed.

Similarly, utilization of a weak cipher for carrying out protected simple authentication makes it possible for a ‘man in the middle’ adversary to intercept the ciphered authentication data during transmission and possibly reverse-engineer the original password.

B1.4 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY

If authentication is not implemented, an attacker could inject false or unauthorized commands into a communications path to the spacecraft’s command chain, and potentially take over control of the spacecraft. This could result in the loss of a mission.

B2 SANA CONSIDERATIONS

This document does not require any action from SANA.

B3 PATENT CONSIDERATIONS

Algorithms and processes referenced in this document are in the public domain, and there are no known patents that apply to the recommendations in this document.