CCSDS
The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

INFORMATION SECURITY GLOSSARY OF TERMS

INFORMATIONAL REPORT

CCSDS 350.8-G-1

GREEN BOOK
November 2012

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

INFORMATION SECURITY GLOSSARY OF TERMS

INFORMATIONAL REPORT

CCSDS 350.8-G-1

GREEN BOOK

November 2012

AUTHORITY

Issue:	Informational Report, 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 reflects the consensus of technical panel experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3).

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

FOREWORD

This document is provided as a central source of information security terms and their definitions. All information security documents issued by CCSDS will use this document as a normative reference.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report 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.

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.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 350.8-G-1	Information Security Glossary of Terms, Informational Report, Issue 1	November 2012	Original issue

CONTENTS

1 INTRODUCTION

1.1 PURPOSE

This document is issued to provide a central source of information security terms and their respective definitions. It is intended that this document will be included as a normative reference in all CCSDS security documents and any CCSDS documents referencing information security.

1.2 SCOPE

This document provides a glossary of information security terms which can be used by all CCSDS document authors.

1.3 APPLICABILITY

This document is applicable to all document authors requiring definitions for information security terms. It may be included as a normative reference in any document requiring the definitions of information security terms.

1.4 RATIONALE

In the past, each CCSDS security-related document generated and included its own glossary of information security terms. Often, because different sources of definitions were consulted, the definitions between documents were not consistent. The document-specific generation of such glossaries also consumed valuable resources. In order to minimize resource utilization and to ensure definition consistency, this document has been created for use as a normative reference by CCSDS document authors.

1.5 REFERENCES

The following documents are referenced in this Report. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Report 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] *Information Processing Systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture*. International Standard, ISO 7498-2:1989. Geneva: ISO, 1989.

[2] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*. International Standard, ISO/IEC 27001:2005. Geneva: ISO, 2005.

[3] *National Information Assurance (IA) Glossary*. CNSS Instruction No. 4009. Fort Meade, Maryland: CNSS, April 2010.

[4] *Glossary of Key Information Security Terms*. Edited by Richard Kissel. Revision 1. NIST IR 7298. Gaithersburg, Maryland: NIST, February 2011.

[5] Elaine Barker, et al. *Recommendation for Key Management—Part 1: General*. National Institute of Standards and Technology Special Publication 800-57. Gaithersburg, Maryland: NIST, March 2007.

[6] *Recommended Security Controls for Federal Information Systems and Organizations*. Revision 3. National Institute of Standards and Technology Special Publication 800-53. Gaithersburg, Maryland: NIST, August 2009.

[7] Department of Defense Dictionary of Military and Associated Terms. 8 November 2010 ed. Joint Pub 1-02. Washington, D.C.: U.S. Department of Defense, November 2010.

[8] *Glossary of INFOSEC and INFOSEC Related Terms*. Compiled by Corey D. Schou. Pocatello, Idaho: Idaho State U Simplot Decision Support Center, 1996.

2 GLOSSARY OF INFORMATION SECURITY TERMS

access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. [1]

access control mechanism: Those mechanisms which are used to enforce a policy of limiting access to a resource to only those users who are authorized. [1]

accreditation: Formal declaration by a senior official that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. [3]

active threat: The threat of a deliberate unauthorized change to the state of the system. [1]

Advanced Encryption Standard (AES): A symmetric block cipher using cryptographic key sizes of 128, 192, and 256 bits used to encrypt and decrypt data in blocks of 128 bits. [3]

anti-jam: The measures taken to ensure that transmitted information can be received despite deliberate jamming attempts. [3]

audit: An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [1]

audit trail: Data collected and potentially used to facilitate a security audit. [1]

authentication: The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data. [3] See also 1) peer entity authentication and 2) data origin authentication.

authorization: The granting of rights, which includes the granting of access based on access rights. [1]

availability: The property of being accessible and useable upon demand by an authorized entity. [3]

bulk encryption: The simultaneous (protocol-transparent) encryption of all channels of a multichannel telecommunications link. [3]

certificate: A digitally signed document that binds a public key with an identity. The certificate contains, at a minimum, the identity of the issuing certification authority (CA), the user identification information, and the user’s public key. [3]

certification: The comprehensive evaluation of the technical and nontechnical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. [3]

certificate authority (CA): Trusted entity authorized to create, sign, and issue public key certificates. By digitally signing each certificate issued, the user’s identity is certified, and the association of the certified identity with a public key is validated. [3]

certification authority (CA): See certificate authority.

cipher text: Data produced through the use of encipherment. The semantic content of the resulting data is not available. [1]

classification: The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. [7]

Common Criteria (CC): A standard (ISO/IEC 15408) providing a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. [3]

configuration management: (See configuration control.)

configuration control management: Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications prior to, during, and after system implementation. [3]

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [1]

cryptanalysis: Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. [5]

cryptography: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use. [1]

data integrity: The property that data has not been changed, destroyed, or lost in an unauthorized manner. [3]

data origin authentication: The corroboration that the source of data received is as claimed. [1]

Decipherment: The reversal of a corresponding reversible encipherment. [1]

Denial of Service: The prevention of authorized access to resources or the delaying of time-critical operations. [1]

digital certificate: See certificate.

digital signature: Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient. [1]

encipherment: See encryption.

encryption: The cryptographic transformation of data (see cryptography) to produce ciphertext. [1]

encryption algorithm: A set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key. [3]

End-to-End Encipherment: Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system. [1]

end-to-end security: The safeguarding of information in an information system from its point of origin to its intended destination. [3]

ephemeral key: A cryptographic key that is generated for each execution of a key establishment process and that meets other requirements of the key type (e.g., unique to each message or session). [5]

firewall: A system designed to prevent unauthorized access to or from a private network. [3] Firewalls can be implemented in both hardware and software, or a combination of both.

frequency hopping: The repeated switching of frequencies during radio transmission according to a specified algorithm to minimize unauthorized interception or jamming of telecommunications. [3]

hash function: A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties: 1) (One-way) it is computationally infeasible to find any input which maps to any pre-specified output; and 2) (Collision-resistant) it is computationally infeasible to find any two distinct inputs that map to the same output. [5]

Hash-based Message Authentication Code (**HMAC)**: A message authentication code that uses a cryptographic key in conjunction with a hash function. [3]

identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [3]

identity-based security policy: A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed. [1]

initialization vector: A vector used in defining the starting point of a cryptographic process. [5]

integrity: See data integrity.

Interconnection Security Agreement (ISA): Written management authorization to interconnect information systems based upon acceptance of risk and implementation of established controls. [3]

intranet: A private network that is employed within the confines of a given enterprise (e.g., internal to a business or agency). [2]

Intrusion Detection System (IDS): Hardware or software products that gather and analyze information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from with the organizations). [3]

key confirmation: A procedure to provide assurance to one party that another party actually possesses the same keying material and/or shared secret. [5]

key derivation: A function in the lifecycle of keying material; the process by which one or more keys are derived from a shared secret and other information.. [5]

key distribution: The transport of a key and other keying material from an entity that either owns the key or generates the key to another entity that is intended to use the key. [5]

Key-Encryption-Key (KEK): Key that encrypts or decrypts other keys for transmission or storage. [3]

key establishment: A function in the lifecycle of keying material; the process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement). [5]

key exchange: The process of exchanging public keys (and other information) in order to establish secure communications. [3]

key management: The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction. [5]

key management policy: The key management policy is a high-level statement of organizational key management policies that identifies high-level structure, responsibilities, governing standards and recommendations, organizational dependencies and other relationships, and security policies. [5]

key transport: A key establishment procedure whereby one party (the sender) selects and encrypts the keying material and then distributes the material to another party (the receiver). [5]

key wrapping: A method of encrypting keys (along with associated integrity information) that provides both confidentiality and integrity protection using a symmetric key. [5]

keying material: The data (e.g., keys and IVs) necessary to establish and maintain cryptographic keying relationships. [5]

link-by-link encipherment: The individual application of encipherment to data on each link of a communications system. [1]

malicious software (malware): Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS. [3]

masquerading: The pretense by an entity to be a different entity. [3]

master key: A symmetric master key is used to derive other symmetric keys (e.g., data encryption keys, key wrapping keys, or authentication keys) using symmetric cryptographic methods. [5]

meaconing: A system of receiving radio beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations. [7]

Memorandum of Understanding/Agreement (MOU/A): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. With respect to security, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection. [3]

Message Authentication Code (MAC): A cryptographic checksum that results from passing data through a message authentication algorithm. [3]

message digest: A cryptographic checksum typically generated for a file that can be used to detect changes to the file. Synonymous with hash value/result. [3]

multi-factor authentication (also known as “strong authentication): Authentication using two or more factors to achieve authentication. Factors include: 1) something you know (e.g., password/personal identification number [PIN]); 2) something you have (e.g., cryptographic identification device, token); or 3) something you are (e.g., biometric). [6]

nonce (“number used once”): A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing the transmittal of live data rather than replayed data, thus detecting and protecting against replay attacks. [3]

non-repudiation (also see repudiation): Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. [3]

one-time password: A password used only once and then permanently discarded.

padding: Fill data required by certain cipher modes.

passive threat: The threat of unauthorized disclosure of information without changing the state of the system. [1]

peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. [1]

plaintext: Unencrypted information. [3]

private key: In an asymmetric cryptography scheme, the private or secret key of a key pair which must be kept confidential and is used to decrypt messages encrypted with the public key or to digitally sign messages, which can then be validated with the public key. [3]

private network: See intranet.

public key: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign. [3]

Public Key Infrastructure (PKI): Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. [3]

Random Number Generator: A process used to generate an unpredictable series of numbers. Each individual value is called random if each of the values in the total population of values has an equal probability of being selected. [3]

replay attacks: An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. [3]

repudiation: Denial by one of the entities involved in a communication of having participated in all or part of the communication. [1]

residual risk: The risk remaining after risk treatment. [2]

risk: Possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. [3]

risk analysis: Systematic use of information to identify sources and to estimate the risk. [2]

risk treatment: Process of selection and implementation of measures to modify risk. [4]

rule-based security policy: A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. [1]

secret key: A cryptographic key that is used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and is not made public. The use of the term "secret" in this context does not imply a classification level, but rather implies the need to protect the key from disclosure. [3]

Secret (Symmetric) Key Infrastructure (SKI): Cryptographic key infrastructure used to generate and distribute secret (symmetric) keying material such as master keys, key encryption keys, and traffic protection keys.

secure hash algorithm (SHA): A hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. [3]

security policy: The set of criteria for the provision of security services (see also identity-based and rule-based security policy). [1]

security controls: Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [3]

session key: See ephemeral key.

shared secret: A secret value that has been computed using a key agreement scheme and is used as input to a key derivation function. [5]

secure hash standard: Specification for a secure hash algorithm that can generate a condensed message representation called a message digest. [3]

spoofing: See masquerading.

spread spectrum: A telecommunications technique in which a signal is transmitted in a bandwidth considerably greater than the frequency content of the original information. Frequency hopping, direct sequence spreading, time scrambling, and combinations of these techniques are forms of spread spectrum. [3]

static key: A key that is intended for use for a relatively long period of time and is typically intended for use in many instances of a cryptographic key establishment scheme. Contrast with an ephemeral key. [5]

symmetric key: See secret key.

threat: A potential violation of security. [1]

threat source: (See threat source.)

threat analysis: The examination of information to identify the elements comprising a threat. [3]

threat assessment: Formal description and evaluation of threat to a system. [3]

threat source: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. [4]

Traffic Encryption Key (TEK): Key used to encrypt plain text or to superencrypt previously encrypted text and/or to decrypt cipher text. [3]

traffic protection key: See traffic encryption key.

trap door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. [3]

Trojan horse: A program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. [3]

trust: Confidence that an entity, to which trust is applied, will perform in a way that will not prejudice the security of the system of which that entity is a part. [8]

Virtual Private Network (VPN): Protected information system link utilizing tunneling, security controls, and end-point address translation giving the impression of a dedicated line. [3]

virus: Self-replicating, malicious code that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [3]

vulnerability: Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited to violate system security policy and result in a security breach. [3]

vulnerability analysis: See vulnerability assessment.

vulnerability assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [3]

worm: A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread itself. [3]