The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

CCSDS RECOMMENDED PRACTICE FOR A KEY MANAGEMENT SCHEME

DRAFT RECOMMENDED PRACTICE

CCSDS 000.0-R-0

RED BOOK
SEPTEMBER 2007

AUTHORITY

Issue:	Red Book, Issue 0
Date:	September 2007
Location:	Not Applicable

(WHEN THIS RECOMMENDED STANDARD IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

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 Recommendations is detailed in the *Procedures Manual 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
Office of Space Communication (Code M-3)
National Aeronautics and Space Administration
Washington, DC 20546, USA

STATEMENT OF INTENT

(WHEN THIS RECOMMENDED STANDARD IS FINALIZED, IT WILL CONTAIN THE FOLLOWING 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 considered binding on any Agency.

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

- Whenever a member establishes a CCSDS-related **practice**, this **practice should** be in accord with the relevant **Recommended Practice**. Establishing such a **practice** does not preclude other provisions which a member may develop.
- Whenever a member establishes a CCSDS-related **practice**, that member will provide other CCSDS members with the following information:
  - The **practice** 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 Practice** nor any ensuing **practice** is a substitute for a memorandum of agreement.

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 standards 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**.

FOREWORD

[Foreword text specific to this document goes here. The text below is boilerplate.]

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 *Procedures Manual for the Consultative Committee for Space Data Systems*. 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.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (Roskosmos)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- 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.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Program Office (NSPO)/Taipei.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

PREFACE

This document is a draft CCSDS **Recommended Practice**. Its 'Red Book' status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DOCUMENT CONTROL

Document	Title	Date	Status and Substantive Changes
CCSDS 000.0-R-0	CCSDS Recommended Practice for a key management scheme, Issue 0	September 2007	Current Draft

1 INTRODUCTION

1.1 PURPOSE OF THIS RECOMMENDATION

This recommended practice provides the basis for use of a key management scheme for civilian space missions. This recommended practice does not specify where key management schemes should be implemented, nor does it specify when it should be used. Those specifics are left to the individual mission planners but suggestions for the use of authentication may be found in "*The Application of CCSDS Protocols to Secure Systems*" [GRN] and the CCSDS *Security Architecture for Space Data Systems* [ARCH]. However, by using standardized processes and schemes, high quality solutions are employed, interoperability is enabled, and the potential rewards of economies of scale are provided by the ability to by off-the-shelf products. Key management schemes are used to distribute and negotiate cryptographic keys that can then be used to provide certain security services between two or more entities.

1.2 SCOPE

The standard key management schemes are recommended practices for use by all civilian space missions that need to provide any kind of security process. Such process might be on the ground data network, the space link or both. Key management may happen between trusted, between untrused and between trusted and untrusted entities.

1.3 APPLICABILITY

1.3.1 APPLICABILITY OF THIS RECOMMENDED PRACTISE

This recommended practice is applicable to all civilian space missions with key management requirements.

1.3.2 LIMITS OF APPLICABILITY

While the use of key management schemes is encouraged for all missions, the results of a threat/risk analysis and the realities of schedule/cost drivers 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. Nevertheless, there are always concerns regarding the correctness of data received either on the ground from the spacecraft or on the spacecraft from the ground or between ground segment entities (i.e., what was transmitted is exactly what is received and any modifications are noticed and flagged) as well as concerning the confidentiality of information. Data that has been modified or corrupted without being noticed is of major concern. If this were to occur on commands to the spacecraft, catastrophic events could result. If the above mentioned security mechanisms are implemented, a need arises for secure distribution of cryptographic keys to support these functions. Without key management, it is not possible to

guarantee the proper operation of the above mentioned security services and serious threats to the mission may occur.

The recommended practices in this document specify proper deployment of key management procedure in the space and ground segment of civilian space missions.

1.5 DOCUMENT STRUCTURE

1.5.1 DOCUMENT ORGANIZATION

There are two sections that make up this document. Chapter 1 provides introductory and background information. Chapter 2 provides a recommended practice for space link key management while chapter 3 addresses the ground segment. Chapter 4 describes a hybrid key management scheme. Chapter 5 discusses key lifetime and revocation.

1.6 DEFINITIONS, NOMENCLATURE, AND CONVENTIONS

1.6.1 DEFINITIONS

Access Control: The process of granting access to the resources of a system only to authorized users, programs, processes, or other systems.

Access Control Mechanism: Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Authenticate: (1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authorization: The granting of access rights to a user, program, or process.

Controlled Network: A network that is enforces a security policy.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Configuration Management: Process of controlling modifications to the system's hardware, firmware, software, and documentation which provides sufficient assurance the system is protected against the introduction of improper modification before, during, and after system implementation.

Data Integrity: Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Denial of Service: Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service.

End-to-End Security: In the context of this book, this term refers to the provision of direct security between two entities and not between applications running on these entities. It therefore represents a data link layer definition.

Identification: The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Masquerading: Attempts to gain access to a system by posing as an authorized user or as a process. This is a form of spoofing.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk: A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. Note: Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service, loss of confidentiality or integrity), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.

Risk Analysis: An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of those events. The purpose of a risk assessment is to determine if countermeasures are adequate to reduce the probability of loss or the impact of loss to an acceptable level.

Security Policy: The set of laws, rules, and practices that regulate how information is managed, protected, and distributed. Note: A security policy may be written at many different levels of abstraction. For example, a corporate security policy is the set of laws, rules, and practices within a user organization; system security policy defines the rules and practices within a specific system; and technical security policy regulates the use of hardware, software, and firmware of a system or product.

Threat: Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

Threat Agent: A method used to exploit a vulnerability in a system, operation, or facility.

Threat Analysis: The examination of all actions and events that might adversely affect a system or operation.

Threat Assessment: Formal description and evaluation of threat to a system.

Trap Door: A hidden software or hardware mechanism that can be triggered to permit system protection mechanisms to be circumvented. It is activated in some innocent-appearing

manner; e.g., a special 'random' key sequence at a terminal. Software developers often introduce trap doors in their code to enable them to reenter the system and perform certain functions. Synonymous with back door.

Trojan Horse: A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

Virus: A program that can 'infect' other programs by modifying them to include a, possibly evolved, copy of itself.

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.

Vulnerability Analysis: The systematic examination of systems in order to determine the adequacy of security measures, identification of security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment: A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

1.6.2 NOMENCLATURE

The following conventions apply throughout this Recommendation:

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

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.

1.6.3 CONVENTIONS

TBD

1.7 REFERENCES

The following documents are referenced in the text of 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 Recommendations.

Applicable Document

[A1] NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General*, U.S. National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf, August 2005.

Referenced Documents

[1] *Procedures Manual for the Consultative Committee for Space Data Systems*. CCSDS A00.0-Y-9. Yellow Book. Issue 9. Washington, D.C.: CCSDS, November 2003.

[2] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. International Standard, ISO/IEC 7498-1:1994. 2nd ed. Geneva: ISO, 1994.

[3] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

[4] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460. Reston, Virginia: ISOC, December 1998.

[5] S. Kent and R. Atkinson. *Security Architecture for the Internet Protocol*. RFC 2401. Reston, Virginia: ISOC, November 1998.

[6] J. Postel. *Transmission Control Protocol*. STD 7. Reston, Virginia: ISOC, September 1981.

[7] J. Postel. *User Datagram Protocol*. STD 6. Reston, Virginia: ISOC, August 1980.

[8] Kevin Fall. "A Delay-Tolerant Network Architecture for Challenged Internets." In *Proceedings of ACM SIGCOMM 2003 (Karlsruhe, Germany)*. New York: ACM, August 2003.

[9] The Internet Key Exchange (IKE), RFC 2409

[10] NIST, *Specification for the Advanced Encryption Standard*, Federal Information Processing Standard 197 (FIPS-197), U.S. National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, November 2001.

[11] Security Architecture Document

[12] Authentication Blue (Green, Orange Magenta?) Book

[13] CCSDS, *Space Communications Protocol Specification (SCPS)—Security Protocol (SCPS-SP)*, CCSDS 713.5-B-1 Blue Book. Issue 1, May 1999

[14] Kent, *IP Encapsulating Security Payload (ESP)*, RFC 4303, http://www.ietf.org/rfc/rfc4303.txt, December 2005.

[15] Durst, Miller and Travis, *TCP Extensions for Space Communication*, 1996

[16] PSS Telecommand Encoder Specification, ESA PSS-04-111 Issue 1 September 1992

[17] Fischer, Merri, Engel, *Approach to the integration of data security in packet TM/TC standards, Spaceops 06*

[18] NIST Speical Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, U.S. National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf , October 1995.

[19] CCSDS, *Draft Recommended Practice for Symmetric Encryption*, CCSDS x.x-R-x Red Book.

[ARCH] CCSDS, *Draft Security Architecture for Space Data Systems*, CCSDS x.x-R-x Red Book.

[CONNECT] CCSDS, *Guide for Secure System Interconnection*, CCSDS 350.4-G-0 Green Book.

2 SPACE LINK KEY MANAGEMENT

In the following chapter, a recommended practise for key management schemes to be used in CCSDS compliant ground-to-space communications are presented.

2.1 SPACE SEGMENT KEY MANAGEMENT SCHEME

The recommended practise for a ground-to-space key management scheme is based on a Secret Key Infrastructure (SKI) and shall be independent of the underlying symmetric cipher. As a recommended practise, the cipher shall be chosen according to the CCSDS *Recommended Practice for Symmetric Encryption* [21].

It is recommended to deploy a SKI in the space segment with the spacecraft(s), ground station(s) and the control centre being the nodes that participate in it. The key management shall be based on a pre-installed seed of **master keys** onboard the spacecraft. Those master keys shall function as **key encryption keys (KEKs)** for the protection of uploaded **session keys**. They must not be used for any other purpose and their number shall be dependent on the number of different session keys, their upload frequency as well as the criticality and the lifetime of the mission. As an option, KEKs can also be handled as special session keys separate to the master keys to reduce their number and use frequency. The KEKs and master keys have to meet special design requirements concerning its robustness. Those requirements are defined by the underlying encryption algorithm and the mode of operation.

Session keys may be of the following types: **TC authentication keys**, **TC encryption keys**, **TM HK authentication keys**, **TM HK encryption keys**, **TM payload authentication keys** or **TM payload encryption keys**. Payload related session keys may again be divided into keys for different payload modules. A mission may choose to use a subset of the above list depending on its classification according to CCSDS *Security Architecture for Space Data Systems* [ARCH]. The lifetime of session keys shall be selected at to be at the minimum appropriate according the to amount and frequency of protected data.

This basic key management deployment is shown in Figure 2-1.

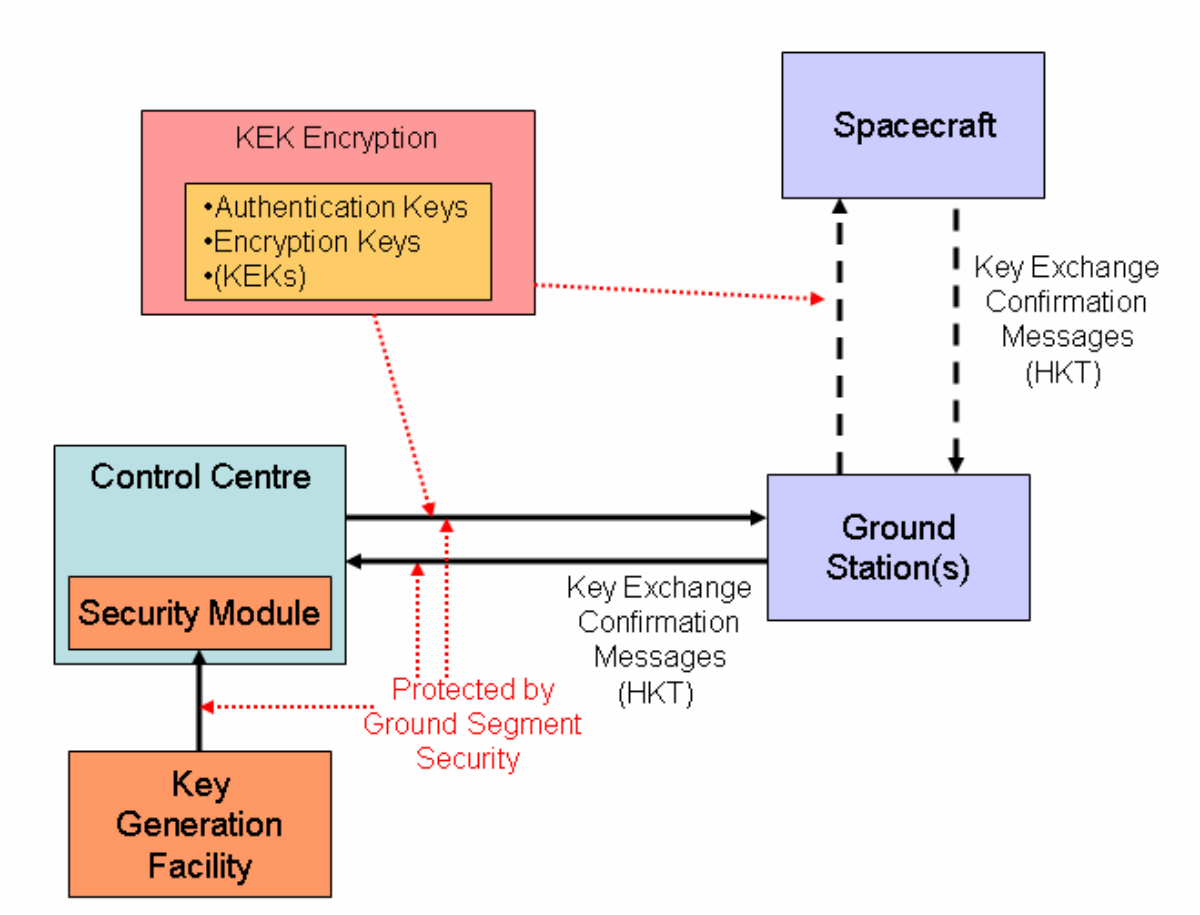

Figure 2-1 - *Space Segment SKI deployment*

2.2 SPACE SEGMENT KEY MANAGEMENT ALGORITHM

As a shared secret always exist between ground control and the spacecraft, the spacelink key management process is very straight forward. As a recommended practise, the following key exchange scheme shall be used for all session keys uploads as a basis:

1) CC→SC : $\{K_{new}, ID_{Knew}\}KEK_x, ID_{Knew}$

2) SC→CC: Confirmation_ ID_{Knew}

3) CC switch keys

CC denotes the control centre, SC the spacecraft, KEK_x is the valid KEK, K_{new} is the new session key to be uploaded, ID_{Knew} is the corresponding key identification and Confirmation_ ID_{Knew} denotes the key reception confirmation message for K_{new}. Here, a KEK may also be a master key.

For the upload of KEKs, a similar scheme applies:

1) CC→SC : {KEK_{new}, ID_{KEKnew}}MK_x, ID_{KEKnew}

2) SC→CC: Confirmation_ ID_{KEKnew}

3) CC switch keys

CC denotes the control centre, SC the spacecraft, MK_x is the valid master key, KEK_{new} is the new KEK to be uploaded, ID_{KEKnew} is the corresponding KEK identification and Confirmation_ ID_{KEKnew} denotes the KEK reception confirmation message for KEK_{new}.

The usage of the key identification tag is optional but may be required by some missions especially if they are multi spacecraft missions. In the above scheme the presence of a ground station is omitted and a direct end-to-end communication between the control centre and the spacecraft is assumed.

3 GROUND SEGMENT KEY MANAGEMENT SCHEME

In the ground network infrastructure, the recommended practise is to use existing and well established key management protocols depending on the underlying security architecture according to CCSDS *Security Architecture for Space Data Systems* [ARCH]. In this chapter, a mechanism for key management is presented as a recommended practise for the ground segment. For this purpose the ground segment shall be divided into two areas – the **core ground segment** and the **external ground segment**.

The core ground segment includes all equipment and nodes that are owned by the operating agency and can be fully trusted while the external ground segment consists of non-agency nodes such as customers, industry and research institutes. Depending on the interoperability contract (see CCSDS *Guide for Secure System Interconnection* [CONNECT]), equipment that is owned by another agency can be treated either as core nodes or as external nodes.

For this recommended practice, it is assumed that the ground segment network is based upon the internet protocol (IP). If other protocols are used on parts of the network (such as X25) it should be possible to use them to tunnel IP so that the key management recommendation can still be realised.

3.1 GROUND SEGMENT SETUP

3.1.1 CORE GROUND SEGMENT SETUP

In the core ground segment, a well established Public Key Infrastructure is assumed to be deployed and is required for the key management scheme. This means, that each node of the core ground segment has a valid private key and public key certificate that have been issued by this PKI. This recommended practise **does not** describe the deployment of the PKI as this is an implementation and PKI system issue.

3.1.2 EXTERNAL GROUND SEGMENT SETUP

The remainder of the ground segment consists of nodes that are not completely trustworthy in the view of the operating agency. They may or may not be part of the agency PKI. If they are, the setup in 3.1.2 applies. This recommended practise assumes that they are not and that session keys need to be negotiated between entities.

In some mission scenarios, external nodes might have an additional **non-repudiation** requirement. In this case they must be either part of the agency PKI or another PKI that is trusted by the agency PKI.

3.1.3 GROUND SEGMENT SESSION KEYS

All security sensitive data that is travelling between the nodes in the core and external ground segment shall be protected by symmetric session keys that have been distributed using the recommended practise for a key distribution algorithm. The lifetime of those session keys, their key length and other special properties is dependent on the security

policy, type and rate of the data that is being protected and the mission classification according to CCSDS *Security Architecture for Space Data Systems* [ARCH]. The encryption algorithm shall be selected according to CCSDS *Recommended Practice for Symmetric Encryption* [21].

3.2 KEY NEGOTIATION IN THE GROUND SEGMENT

For a maximum of security and interoperability, the **Internet Key Exchange (IKE)** [IKE] protocol is the recommended practise for the distribution of session keys. IKE is part of the IPSec security suite for the internet protocol; however this recommendation is independent of the underlying security mechanism. Therefore, keys negotiated with IKE might also be used with other security mechanisms such as TLS. It shall be noted that using IKE, session keys on the ground network are **NOT** generated by a central key management entity but they are negotiated by the entities that run the IKE protocol. If there is a need for a centralized key production facility, IKE established keys shall only be used for the distribution of the centrally produced session keys.

The following sections focus on the two phases of a key establishment using IKE. Phase 1 is run in main mode (not aggressive mode) and phase 2 is run in quick mode. The phase 2 is equal for the core ground segment and the external ground segment.

3.2.1 KEY NEGOTIATION IN THE CORE GROUND SEGMENT

For establishing secure key associations inside the core ground segment network, IKE phase 1 shall be used in main mode and with signature based authentication. This means, if two entities decide to establish a key the following process is applied:

1) The initiator sends on or more proposals for authentication and encryption algorithms:
   I→R: HDR, SA

2) The responder selects the safest one that he supports:
   R→I: HDR, SA

3) The initiator sends his public part of a Diffie-Hellman key exchange together with a nonce:
   I→R: HDR, KE, N_I

4) The responder sends his public part of a Diffie-Hellman key exchange together with a nonce:
   R→I: HDR, KE, N_R

The exchanged nonces are now used for mutual authentication in steps 5 and 6. The following equations lead to the signatures that are computed by the participants to provide mutual authentication:

- $SKEYID = MAC(N_I, N_R / g^{xy})$

- $SIG_I = \{MAC(SKEYID / g^{x_I}, g^{x_R}, Cookie_I, Cookie_R, ID_I)\}\_\Pr K_I$
- $SIG_R = \{MAC(SKEYID / g^{xr}, g^{xi}, Cookie_R, Cookie_I, ID_I)\}\_\Pr K_R$

Following this, steps 5 and 6 are as follows:

5) The initiator sends his signature and possibly his certificate to the responder:
   I→R: $HDR, ID_{ii}(CERT_I), SIG_I$

6) The responder sends his signature and possibly his certificate to the initiator:
   I→R: $HDR, ID_{ir}(CERT_R), SIG_R$

Having completed all six steps, the participants have now negotiated session encryption and authentication keys which are computed from SKEYID in an authenticated way. These keys are then used in phase 2 to protect to negotiation of the real session key(s).

3.2.2 KEY NEGOTIATION IN THE EXTERNAL GROUND SEGMENT

For all external ground segment entities that are supported by a PKI that is trusted by the agency the same procedure as in the core ground segment applies.

Otherwise it is the recommended practise to protect the key negotiation using a previously shared symmetric master key MK. This recommended practise does not specify how such a key is distributed to the network entities. A very common approach is the use of secure smart cards. Those master keys are only to be used for IKE authentication and therefore have a long lifetime which makes the physical exchange process possible even for remote locations.

IKE with secret key authentication is specified as following:

1) The initiator sends on or more proposals for authentication and encryption algorithms:
   I→R: HDR, SA

2) The responder selects the safest one that he supports:
   R→I: HDR, SA

3) The initiator sends his public part of a Diffie-Hellman key exchange together with a nonce:
   I→R: HDR, g^x, N_I

4) The responder sends his public part of a Diffie-Hellman key exchange together with a nonce:
   R→I: HDR, g^y, N_R

The exchanged nonces are now used for mutual authentication in steps 5 and 6. The following equations lead to the signatures that are computed by the participants to provide mutual authentication:

- $SKEYID = MAC(MK / N_I, N_R)$
- $HASH_I = MAC(SKEYID / g^{x_I}, g^{x_R}, Cookie_I, Cookie_R, ID_I)$
- $HASH_R = MAC(SKEYID / g^{xr}, g^{xi}, Cookie_R, Cookie_I, ID_I)$

Following this, steps 5 and 6 are as follows:

5) The initiator sends his signature and possibly his certificate to the responder:
   I→R: $HDR, ID_{ii}, HASH_I$

6) The responder sends his signature and possibly his certificate to the initiator:
   I→R: $HDR, ID_{ir}, HASH_R$

Having completed all six steps, the participants have now negotiated session encryption and authentication keys which are computed from SKEYID in an authenticated way. These keys are then used in phase 2 to protect to negotiation of the real session key(s).

3.2.3 IKE PHASE 2 (QUICK MODE) KEY NEGOTIATION

As stated above, the phase 2 is equal for both the core and external ground segment. The information exchanged in phase 2 is encrypted and authenticated by the keys that have been negotiated in phase 1. Other than that the process is very similar to that of phase 1 and at the end of the process the two entities have successfully negotiated one or more session keys (i.e. one for encryption, one for authentication). It is important to mark that multiple quick mode (phase 2) negotiations can follow after one main mode (phase 1) negotiation.

4 HYBRID KEY MANAGEMENT SCHEME

In some missions it might be desirable to provide **end-to-end key exchange or negotiation** between an (possibly external) entity and a spacecraft (subsystem) without the operating agency being able to access these keys. This section contains a recommended practise how such a process can be realised. This process applies only to TM payload session keys. It is the recommended practise that the end-to-end relationship is established between the external user and the telemetry subsystem onboard the satellite. Terminating the relationship already in the packet telecommand decoder on the spacecraft is not an option as this would able the operating agency to access that data.

Therefore the recommended practise is a space link key exchange process as described in chapter 2 only that is established end–to-end between the external users premises and the associate payload module onboard the satellite. Master keys are being burned into a secured area of the payload module memory prior to launch. It is especially important that the secure memory module is modelled in a way that it is impossible to access without proper encrypted command sequences that are based on these master keys. This realizes an access control scheme for the payload module. It is not in the scope of this recommended practise to define the concrete layout of such command sequences or their encryption strategy. This is a mission and especially end customer specific design question.

As these command sequences (which on the space link are realising the same process as in chapter 2) are encrypted, they can be delivered to the operating agency for uplink without the danger of disclosing any key material. In this case the encryption realises a secure tunnel between the customer and the payload module with the hosting agency network representing the insecure environment.

In order to reach the hosting agencies premises and to be protected against the more sophisticated attacks that are possible in the ground segment, the ground based security services are used here. However, these services make use of the key management system that is described in chapter 3.

To summarize, an external institution must run two key management processes. One between the payload module and itself and one between the agencies control centre and itself. In addition, the agency can decide to put another layer of security on top in the space link e.g. to be able to provide telecommand authentication.

5 KEY LIFETIME AND REVOCATION

The lifetime of the session keys that are generated from the recommended practice needs to be specified by security policies and is dependent on the data rate, security level of the communicated data and the mission classification according to CCSDS *Security Architecture for Space Data Systems* [ARCH].

A key revocation process must exist to prevent usage of already expired keys. For symmetric keys that are only used for encryption and authentication on communication channels and not for data storage the approach is quite straightforward. They are simply deleted. However before deleting a key it must be clear that this key is (1) no longer in use and (2) has been replaced by a confirmed new key. The deletion request for a set of session keys onboard the spacecraft shall be validated by a valid KEK or master key.