CCSDS
The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SPACE MISSIONS KEY MANAGEMENT CONCEPT

INFORMATIONAL REPORT

CCSDS 350.6-G-1

GREEN BOOK
November 2011

The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SPACE MISSIONS KEY MANAGEMENT CONCEPT

INFORMATIONAL REPORT

CCSDS 350.6-G-1

GREEN BOOK
November 2011

AUTHORITY

Issue:	Informational Report, Issue 1
Date:	November 2011
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

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 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.

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 350.6-G-1	Space Missions Key Management Concept, Informational Report, Issue 1	November 2011	Original issue

CONTENTS

Section Page

CONTENTS (continued)

Section Page

Figure

Table

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

This report has been has been prepared by the Consultative Committee for Space Data Systems (CCSDS) to provide the core concepts of cryptographic key management in the context of space missions. The concepts described herein are the baseline for the CCSDS standardization activities in respect to security services and, more concretely, key management schemes for space missions.

During the last decade, the importance of information security within the network and Internet community has been growing constantly. Every day, articles about new kinds of cyber crimes, from disclosure of confidential data to fraud, are published. As the world has become more and more connected, the topic has grown from a governmental or military concern to a day-to-day issue that affects everybody from governmental bodies down to private Internet users. Critical infrastructures have become attractive targets for cyber terrorism.

The same situation applies to space communication systems. Many space operating entities are realizing the growing importance of information security not only for military, governmental, and commercial missions, some of them considered part of above mentioned critical infrastructure, but also for peaceful scientific projects such as earth observation or planetary exploration. This development, together with the increasing usage of standardization, has led the operating entities to formulate security requirements for many of their missions’ telecommand and telemetry systems.

The security measures introduced as a consequence of above trends require the secure distribution of cryptographic material among authorized personnel and entities with varying access control levels. This process is called **key management** and is not a trivial task since it has to work smoothly with all the parts of the system, supplying different security implementations with cryptographic material. Aside from the technical implementation, key management incorporates also other aspects such as security policies, handling of keying material or key transportation.

This Report provides background information on existing terrestrial key management systems, key management infrastructures and their possible adaptations to space missions in both ground and space segment networks. It discusses example scenarios for space mission key management deployment.

1.2 DEFINITIONS

Security definitions can be found in the CCSDS Security Glossary (reference [18]).

1.3 RATIONALE

CCSDS has published a number of recommendations related to security for space missions, in particular concerning the use of cryptographic algorithms for encryption and authentication (reference [6]). As a prerequisite for using such a cryptographic algorithm, cryptographic keys must be distributed among the different parties involved in the secure communication. This is achieved by a process called key management and is of central concern for the construction of any secure communication system. The rationale of this informational report is to introduce key management concepts and their applicability to space data systems.

1.4 DOCUMENT STRUCTURE

In section 2, the main concepts of key management are outlined as an introduction to the subject followed by a list of operational examples. Key management infrastructures and key sharing concepts are discussed in section 3. Section 4, as the main part of this document, outlines the special properties of key management in the space communication environment and discusses different space key management approaches. Ground segment key management approaches are discussed in section 5. In section 6, the key management requirements of future real constellation missions are outlined. Section 7 concludes and summarizes the document.

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] *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.

[2] *Security Architecture for the Internet Protocol*. RFC 4301. Reston, Virginia: ISOC, December 2005.

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

[4] C. Kaufman, Ed. *Internet Key Exchange (IKEv2) Protocol*. RFC 4306. Reston, Virginia: ISOC, December 2005.

[5] *Security Architecture for Space Data Systems*. Draft Recommendation for Space Data System Practices, CCSDS 351.0-R-1. Red Book. Issue 1. Washington, D.C.: CCSDS, April 2011.

[6] *CCSDS Security Algorithms*. Draft Recommendation for Space Data System Standards, CCSDS 352.0-R-0. Red Book. Issue 0. Washington, D.C.: CCSDS, forthcoming.

[7] Robert C. Durst, Gregory J. Miller, and Eric J. Travis. “TCP Extensions for Space Communications.” In *Proceedings of the Second Annual International Conference on Mobile Computing and Networking (November 10-12, 1996, Rye, New York)*, 15-26. New York: ACM, 1996.

[8] *Telecommand Encoder Specification*. PSS-04-111. Noordwijk, Netherlands: ESA/ESTEC, September 1992.

[9] *An Introduction to Computer Security—The NIST Handbook*. National Institute of Standards and Technology Special Publication 800-12. Gaithersburg, Maryland: NIST, October 1995.

[10] *CCSDS Guide for Secure System Interconnection*. Report Concerning Space Data System Standards, CCSDS 350.4-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, November 2007.

[11] H. Harney, A. Colegrove, and A. Colegrove. *GSAKMP: Group Secure Association Key Management Protocol*. RFC 4535. Reston, Virginia: ISOC, June 2006.

[12] 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.

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

[14] Michel Abdalla and Mihir Bellare. “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-Keying Techniques.” In *Proceedings of the Sixth International Conference on the Theory and Application of Cryptology and Information Security (December 3-7, 2000, Kyoto, Japan)*, 546-559. Carson City, Nevada: IACR, 2000.

[15] W. Diffie and M. Hellman. “New Directions in Cryptography.” *IEEE Transactions on Information Theory* 22, no. 6 (1976): 644-654.

[16] *Communications Operation Procedure-1*. Recommendation for Space Data System Standards, CCSDS 232.1-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, September 2010.

[17] Gavin Lowe. "An Attack on the Needham-Schroeder Public-Key Authentication Protocol." *Information Processing Letters* 56, no. 3 (Nov. 10, 1995): 131-133.

[18] "CCSDS Security Glossary." Forthcoming. Space Assigned Numbers Authority (SANA). <http://sanaregistry.org/>

2 MOTIVATION AND SCENARIOS

2.1 OVERVIEW

This section introduces the key management concept and its basic elements. It further illustrates the complexity of space systems key management using a number of operational examples.

2.2 THE CONCEPT OF KEY MANAGEMENT

2.2.1 GENERAL

Figure 2-1 shows the three major pillars on which the concept of key management is built: **security protocols**, enforced **security policies**, and **key infrastructures**.

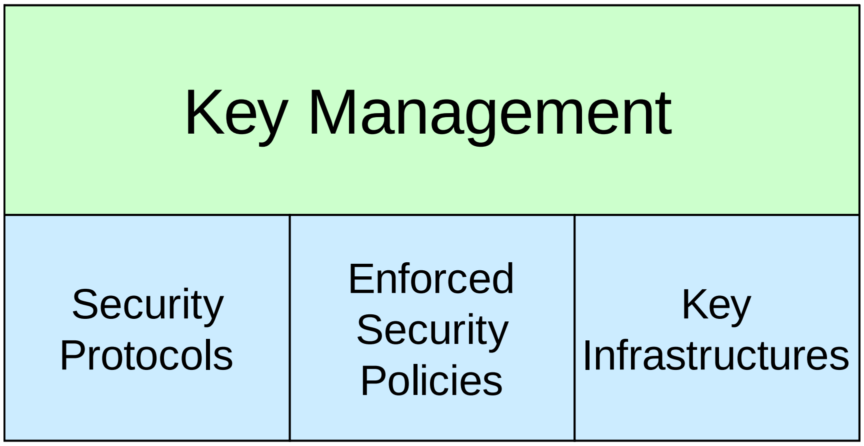

Figure 2-1: Key Management Concept

2.2.2 SECURITY PROTOCOLS

Security Protocols are specialized protocols that have been designed to achieve one or more security goals (for example, mutual authentication or cryptographic key establishment) between two or more communicating entities. A number of these protocols have been developed and are used within the Internet and also other specialized settings. The Internet Key Exchange (IKE) protocol (reference [4]), which is used within the IPSec protocol, is a prominent example for a key establishment protocol. Key management infrastructures are dependent on such protocols to generate, negotiate, distribute, establish, or exchange cryptographic keys in a secure and standardized manner. Security protocols can be specified using formal modelling languages and their correctness formally verified.

Internet (terrestrial) security protocols do not show a good performance in the space environment (reference [7]). In fact, space data systems currently lack suitable standardized key management protocol solutions.

2.2.3 SECURITY POLICIES

Security Policies are rules and regulations that describe the operational procedures required for proper key management. This includes the specification of rules for processes such as generation, distribution, and allowed use for cryptographic keys. Security policies need to be enforced by a dedicated body within the agency or company.

Security policies are living documents and it is important to keep them up to date. In this way they can adapt to a changing situation and can be compatible with new technologies.

The development of security policies is a long and difficult process, but a number of publications exist that can assist in this process (reference [9]).

2.2.4 KEY INFRASTRUCTURES

Key infrastructures provide the technical means for managing the key life cycles (see 2.3) as well as for the distribution of keys using security protocols or other means. Two main categories of key infrastructures can be identified: the **Secret Key Infrastructures (SKIs)** and the **Public Key Infrastructures (PKIs)**.

SKIs have no means to bind identities to a cryptographic parameter such as a key. Because of this, they cannot support any form of non-repudiation security services. However, in small infrastructures, an SKI is less complex than PKIs since it is based on symmetric cryptography.

PKIs are based on asymmetric cryptography and provide means to bind the identity of an entity to a key. These means are called **public key certificates**. PKIs are deployed in large networks and environments such as company and agency networks and also in wide area networks such as the Internet.

2.3 KEY MANAGEMENT LIFECYCLE OVERVIEW

Key management encompasses the entire life cycle of cryptographic keys and other keying material. Basic key management guidance is provided in reference [12]. A single item of keying material (e.g., a cryptographic key) runs through several states during its life, though some of these states may, in fact, be very short:

- **Pre-Operational:** The keying material is not yet available for nominal cryptographic operations. This phase includes the generation of the keying material. Pre-operational sub-phases include
  - *System and User Initialization*: The key management infrastructure is being set-up and required authorities are being nominated. This phase is only required once for the lifetime of a key management infrastructure.
  - *Entity Registration*: Registration of the entity that is requesting a key.

  - *Keying Material Installation*: The keying material is generated and installed in a secure form on an authorized medium. The key generation process and authorized media are defined by the security policies.

  - *Key Establishment*: Keys are established between the communication partners using the previously installed keying material.

  - *Key Registration*: Keys are registered by the key management infrastructure.

- **Operational:** The keying material is available for nominal use. Only in this phase are the cryptographic keys considered valid for security operations.

  - *Operational Storage:* Operational keys must be stored in a secure way as described by the security policies, but access to the protected data, which is subject to cryptographic operations, must be guaranteed. This is non-trivial since it requires the storage of the key in a system that processes data coming from or going to a potentially un-trusted source or destination.

  - *Operational Use*: The keying material is used for performing the cryptographic operations for which it has been authorized.

  - *Key Backup*: Keys must be backed up to ensure accessibility of encrypted data following a possible deletion of an operational or post-operational key.

- **Post-Operational:** The keying material is no longer in normal use. But access to the material is possible. This includes for example decryption of emails.

  - *Key Archive*: Keys must be archived to ensure access to legacy material if required. Unlike operational keys, archived keys can be stored in secure, non-accessible data storage.

  - *Key Recovery*: Archived keys must be capable of being restored for access to legacy material.

- **Obsolete/Destroyed:** The keying material is no longer available. All records of its existence have been deleted. Access to legacy material (e.g., encrypted emails) is no longer possible if this information has not been ‘ported’ to a new, operational or post-operational, key.

  - *Key Revocation*: Revocation of a key withdraws the authority to perform cryptographic operations with a certain key without necessarily destroying all instances of the key. This procedure can be used if a key is corrupted or disclosed. It should be noted that only public key infrastructures can support the revocation of a key. In symmetric infrastructures, revocation and destruction are identical concepts.

  - *Key Deregistration and Destruction*: Unrecoverable destruction of a post-operational key and its backups. The allowed procedures for key destruction are described in the security policies.

2.4 OPERATIONAL EXAMPLES

2.4.1 OVERVIEW

To illustrate the complexity of key management schemes and provide further motivation, a selection of mission examples and their respective requirements for a key management infrastructure are presented.

2.4.2 SPACE-LINK SECURITY SCENARIO

2.4.2.1 General

Many science/Earth-observation missions already have or in the near future will have requirements for telecommand authentication and/or payload telemetry encryption. The security services provide simple end-to-end security between the Operational Control Centre (OCC) and the spacecraft for command and control. In any case, cryptographic keys need to be distributed and synchronized between the OCC and the spacecraft. This setup represents the most basic security architecture for a civil space mission. The concept is illustrated in figure 2-2.

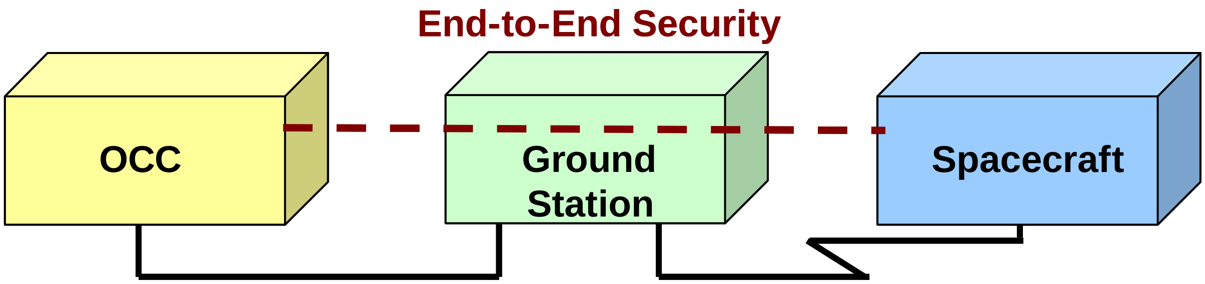

Figure 2-2: Basic Science Mission Security Infrastructure

Some key management options based on symmetric keys exist for the implementation of such a system:

- cryptographic operations with pre-shared master keys:
  - pre-shared master keys to derive Traffic Protection Keys (TPKs);
  - pre-shared master keys as Key Encryption Keys (KEKs) to encrypt TPKs for transport.

An alternative would be the deployment of an asymmetric key management scheme using a key establishment protocol such as Diffie-Hellman (reference [15]).

2.4.2.2 ESA PSS Telecommand Authentication Example

The ESA PSS telecommand decoder specification (reference [8]) is now obsolete; however, it provides a good example for a telecommand authentication mechanism based on KEKs. The standard supports two different key types with one key instance each at a time. One is the fixed key, which is stored in a read-only part of the spacecraft memory and cannot be changed or updated. It serves as backup and fallback key and allows recovery from corruption situations. The other, programmable key serves as a TPK and services the actual telecommand authentication. Only one programmable key can be stored on the spacecraft at a time. Upload of a new programmable key requires a number of telecommands that need to be authenticated and decrypted either by the current (and gradually changing) programmable key or by the fixed key (then taking the role of a KEK). Therefore, the fixed key is not really used as a master key and its special status is only exploited in emergency and recovery procedures. Nevertheless, this simple system represents a basic symmetric key hierarchy using a pre-shared master key. Modern symmetric key management schemes follow the same basic process; however, they are much more advanced.

2.4.3 SPACE-LINK SECURITY SCENARIO WITH EXTENSIONS

2.4.3.1 General

Many missions today produce telemetry with real-time or near real-time distribution requirements. In this case the telemetry is downlinked to a ground station and then directly forwarded to the end users over terrestrial networks. Thus the original end-to-end link, as described in 2.4.2 must be extended to include also the end users, at least for telemetry.

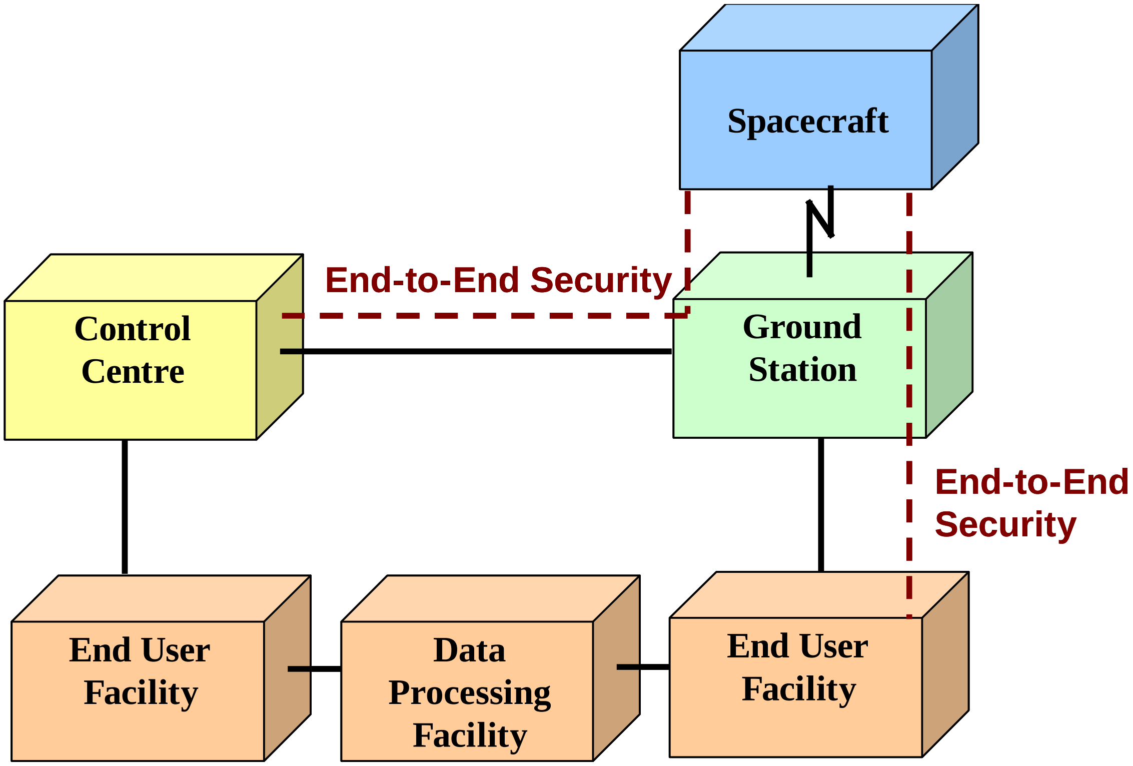

Figure 2-3: Space Link and Ground Segment Security Combined

Figure 2-3 shows the various entities that could be participating in the communication infrastructure of such a mission. The space-link security requirements are identical to those of the standard space-link security scenario (see 2.4.2). However, an additional ground segment key management system has to be deployed to satisfy additional security requirements dedicated to the extended security operations in the ground segment. Several ground segment entities may impose additional end-to-end security. If paying customers are involved, it might even be required to ensure non-repudiation.

Examples for such entities are payload data customers, scientific institutions, companies that just hire the agency for controlling their spacecraft or flying a payload, and real end users. It is obvious that a broad variety of possible end users can be present, not necessarily all having the same access rights or status. Different key management models can be employed to serve such a mission.

As soon as non-repudiation becomes an issue, symmetric key management is insufficient to solve the problem since it cannot support all of these requirements. Public key certificates on the other hand can be fitted with access right parameters and provide non-repudiation. Therefore, in order to best satisfy the requirements of this scenario, a combination of a PKI on the ground and an SKI on the space-link is required (this is discussed in section 4).

2.4.3.2 Crisis Management Scenario Example

A crisis management scenario is an example of an extended space-link security scenario.

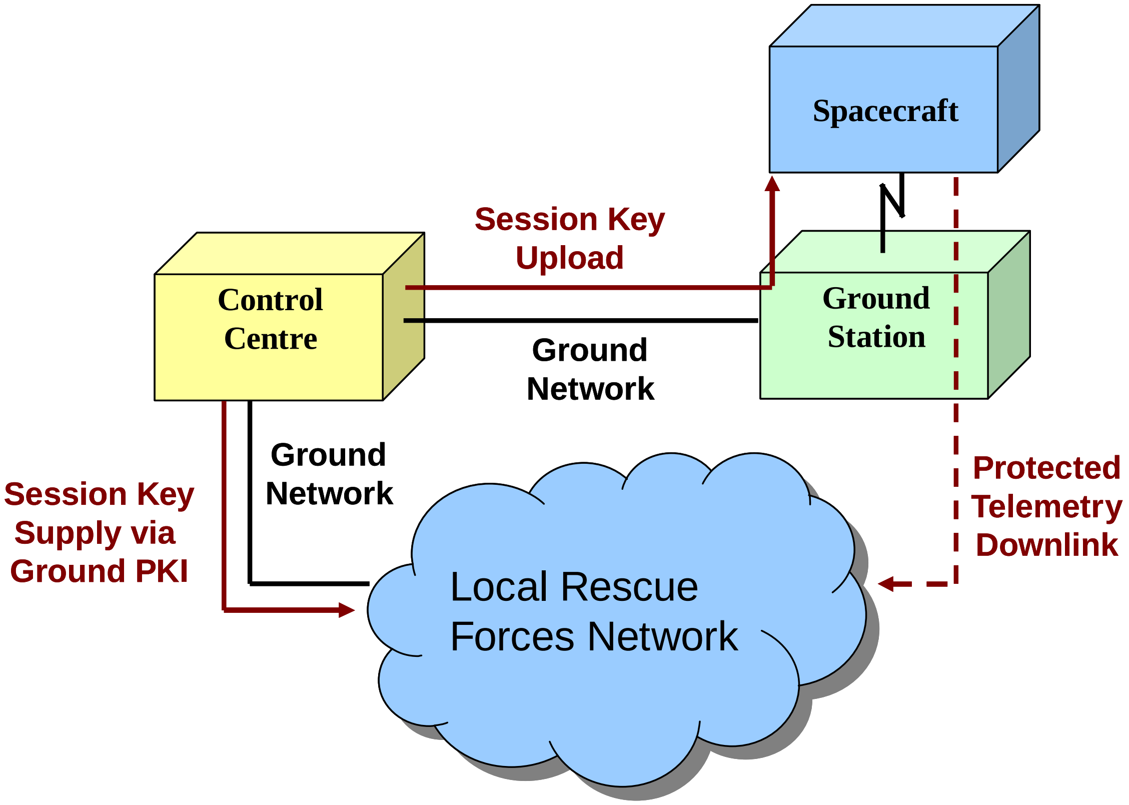
Spacecraft
Session Key Upload
Control Centre
Ground Station
Ground Network
Ground Network
Session Key Supply via Ground PKI
Protected Telemetry Downlink
Local Rescue Forces Network

Figure 2-4: Exemplary Crisis Key Management Scenario

In case of disasters or crisis situations that are related, for example, to environmental issues such as forest fires, rescue forces need direct, timely (in the best case real-time), and easy access to Earth observation data. As shown in figure 2-4, the key management system must be able to handle the distribution of payload data keys to the rescue forces via the ground network (public) key infrastructure and to the spacecraft via the space-link (secret) key infrastructure prior to the downlink of data from the spacecraft. The payload telemetry is then encrypted and potentially authenticated end-to-end between the spacecraft and the rescue forces. While the keys can be installed on-board the spacecraft anytime before the data is requested, the ground segment key management must be able to supply keys to rescue forces on demand and in real-time.

Compared to 2.4.2, a crisis management scenario introduces an additional level of complexity in the key management and interaction between the space-link and ground segment key management infrastructures. Should those infrastructures be owned by different agencies, there is a clear need for interoperability and for standardization.

2.4.4 SPACECRAFT CONSTELLATION SCENARIO

Spacecraft constellations are more complex, cascaded versions of the simple scenarios presented above. Today, only a few spacecraft constellations are in operation but with the deployment of common, space internetworks based on technologies such as DTN (reference [3]), this may change in the future. From a key management perspective, those networks resemble terrestrial intra- or Internet infrastructures. They may have more complex security requirements and as a consequence require more sophisticated solutions for key management.

In the case of constellations with multiple prime and backup control centres, the complexity of the key management infrastructure grows fast (see figure 2-5) and is not limited to the space segment. A network of interconnected ground stations maybe required to control the constellation. Two or more OCCs may be used, even if the second one is just for backup purposes. Often such spacecraft constellations, especially if they offer direct end-user services such as navigation, may also need an extended ground key dissemination system that extends to the end users. Such a system needs to be synchronized with the space segment in order to allow ground access to the provided services. All of the above mentioned elements have to be synchronized in terms of key management to guarantee secure operation of the constellation.

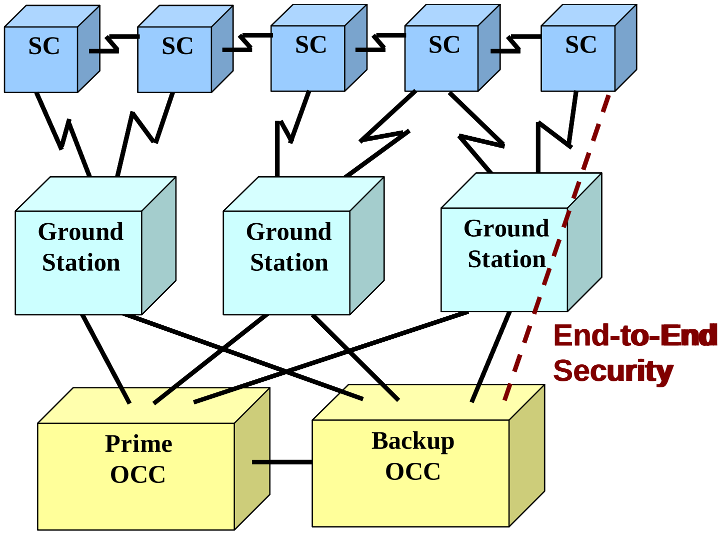

Figure 2-5: Spacecraft Constellation Example

3 KEY INFRASTRUCTURES

3.1 OVERVIEW

This section provides an introduction to key management infrastructures with special focus on highlighting the differences between secret and public key infrastructures. It also focuses on key types and key lifetime management. More detailed information on these subjects can be found in reference [12].

3.2 SECRET OR SYMMETRIC KEY INFRASTRUCTURES

3.2.1 GENERAL

Secret (or symmetric) key infrastructures (SKIs) make use solely of secret (or symmetric) keys. Symmetric keys dictate that participants in a secure communication use the same (secret) key for their cryptographic operations. Said another way, the decryption function is the exact reverse function of the encryption function. Since the symmetric key must never be disclosed to unauthorized entities, it cannot be distributed in plaintext over the communication channel, but must be distributed using a secure channel.

A secret key infrastructure is usually based on a hierarchy of symmetric keys. Three basic hierarchy levels exist:

– **Master Key Level**: Master keys represent the top of the hierarchy and are always distributed manually using a secure channel (e.g., using a smart card distribution mechanism or by pre-burning them into spacecraft memory before launch). They are the initial shared secret that allows the secure distribution of lower level keys.

– **Key Encryption Key Level**: This level may include multiple sub-hierarchies. Key Encryption Keys (KEKs) can be distributed via an insecure channel either under the protection of a master key or a higher level KEK.

– **Traffic Protection Key Level**: The lowest level in the hierarchy are the Traffic Protection Keys (TPKs). Those are keys that are used for the protection of the communication channel. They can be used to provide confidentiality, authentication, and other services. Thus different flavours of traffic protection keys may exist. In particular traffic protection keys can either be Traffic Encryption Keys (TEKs) or Traffic Authentication Keys (TAKs).

An SKI can only be deployed in environments where the secure distribution of master keys as initial shared secret is feasible since it forms the root of the key hierarchy. This means, if there is no possibility to securely distribute the initial master key (in plaintext) to all participants without corruption, the SKI cannot be established.

3.2.2 KEY GENERATION AND DISTRIBUTION

The SKI's top-level **key generation facility** is responsible for the proper generation of master keys. This process should use a validated and approved key generation mechanism with proper random number generators (see 3.5). In addition, a secure interface must exist to make the distribution of the master keys possible. Lower-level key generation facilities may also exist and make use of either a master key or a higher-level KEK to generate and distribute lower-level symmetric keys. In particular, higher level-keys can be used as input to key generation functions. In this case, the new key is **derived** from the higher-level key.

Traffic protection keys are often not generated by a key generation facility but may also be **negotiated** using an approved **key negotiation protocol**. Sometimes, an additional physical unit, the **key distribution facility,** implements the key distribution functionalities.

3.2.3 SKI ANALYSIS

The advantages of an SKI are as following:

– **Simplicity:** The architecture of an SKI is very simple and straight forward. It can be easily deployed.

– **Performance:** Secret key operations outperform public key operations in processing speed by a large factor (up to 1000 in hardware implementations). The amount of memory required to store symmetric keys is substantially lower than for public/private key pairs or even public key certificates.

SKIs suffer from the following drawbacks:

– **Requirement for an additional secure channel**: To provide a secure distribution of master keys, a secure additional (physical) channel is required.

NOTE – For spacecraft, this may be realised by pre-burning master keys into the spacecraft read-only memory.

– **Limited Scalability**: Since secret keys do not provide identity binding, for a full deployment, all entities in the infrastructure that wish to engage in secure communication must share the same secret key. This has a direct impact on the scalability of the system. Therefore, SKIs get more complex with an increasing number of participating entities and should therefore only be used in small environments. However, historically, SKIs have also been used in large environments, e.g., military networks.

– **Missing Identity Binding**: A secret (or symmetric) key cannot provide identity binding as a public key certificate can. This limits the functions that can be supported by an SKI.

3.2.4 SKI OPERATIONAL EXAMPLE

Figure 3-1 shows an example for an SKI as it might be deployed for a space mission which intents to provide authentication and confidentiality protection to its communication channels. At the lowest level, specialized TPKs (for encryption or authentication) are used for security cryptographic operations. They are transferred to the spacecraft under encryption by a KEK. The KEKs themselves are transported under the encryption of a top-level master key.

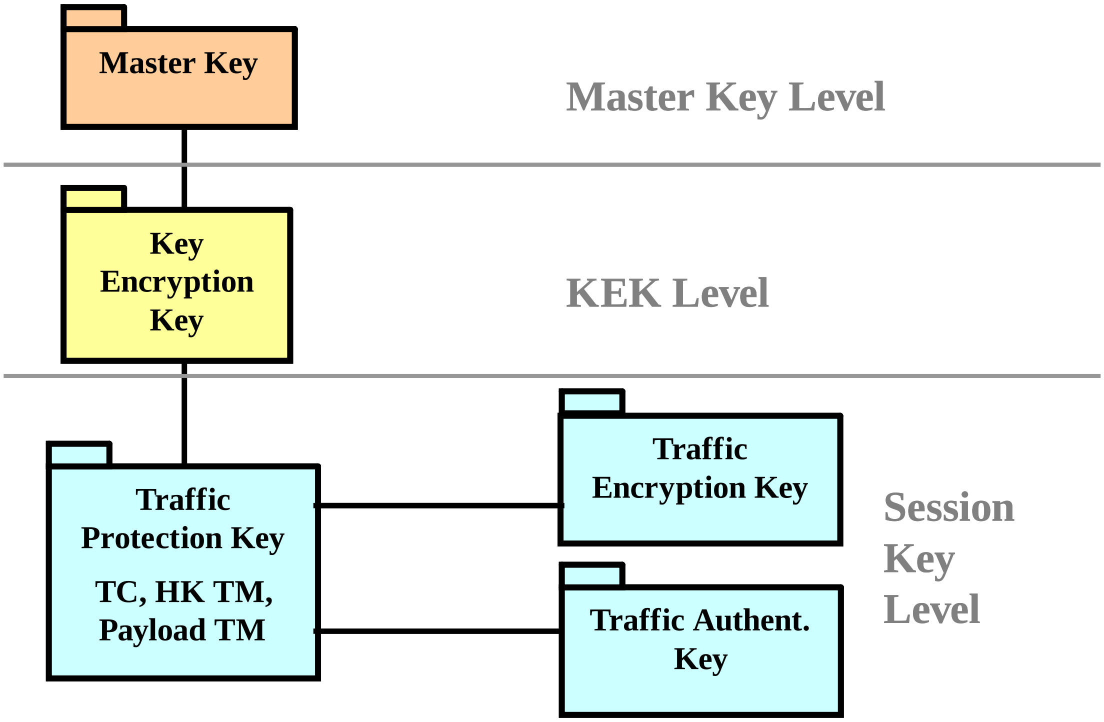

Figure 3-1: Exemplary Secret (or Symmetric) Key Hierarchy

3.3 PUBLIC KEY INFRASTRUCTURES

3.3.1 GENERAL

Public Key Infrastructures (PKI)s use public key pairs to establish secure channels between communicating entities. As opposed to an SKI, the underlying cryptosystem uses pairs of keys, private and public keys. These are inverse to each other with respect to cryptographic operations. A text encrypted with a public key can only be decrypted with the associated private key and vice versa. The biggest advantage of a PKI is that it provides the means to bind public keys to their respective owner entities by the means of public key certificates and helps in the distribution of reliable public keys in large heterogeneous networks. The main components of a PKI are:

– **Certification Authority (CA):** An entity that is trusted by all users of the PKI and that issues and revokes public key certificates and certificate revocation lists using its private key. A CA's private key has special security requirements since its corruption would result in the corruption of all public key certificates that have been issued by this CA.

– **Public Key Certificate*:*** An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity such as a Certificate Authority. Public key certificates are the mechanism for describing trust relationships in a PKI. Certificates may be issued to CAs or other end entities. Certificates issued to CAs indicate the certificate holder CA is trusted to issue additional certificates. Certificates issued to other end entities are appropriate for provisioning other security services, but are not trusted for issuing additional certificates. Certificates include an expiration date. However, if the CA ceases to trust the certificate holder before certificate expiration, the CA can revoke the certificate at any time.

– **Certificate Revocation List (CRL):** A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost, the owner leaves the company/agency, or the owner's name changes. CRLs also provide an important mechanism for documenting the historical revocation status of certificates. That is, a dated signature may be presumed to be valid if the signature date was within the validity period of the certificate, and the current CRL of the issuing CA at that date did not show the certificate to be revoked.

– **Registration Authority (RA):** An entity that is trusted by the CA to register or vouch for the identity of users to a CA.

– **Certificate Repository (DIR):** An electronic site that holds certificates and CRLs, CA post certificates, and CRL repositories. Users can access this information if they want to initiate communication with an entity that holds a certificate of the CA.

The general certification process is illustrated in figure 3-2. An entity who wants to acquire a certificate has to undergo an identity check at the nearest RA belonging to the PKI. There, a certificate request, which contains the user's credentials, is generated and sent to the CA for signing. The CA generates the key pair and user certificate and signs the user certificate with the CA's private key. The user then receives the certificate and key pairs on a secure channel. A copy of the user certificate is also placed in the PKI DIR. After revocation, the user certificate will be added to the CRL.

Another deployment option, which avoids the secure channel in the last step, is that the key pair is already generated at the RA and directly handed to the user. The user certificate can then be distributed later using insecure channels. A similar process applies for generating entity and machine certificates. This process, however, requires access to sophisticated key generation techniques in every RA.

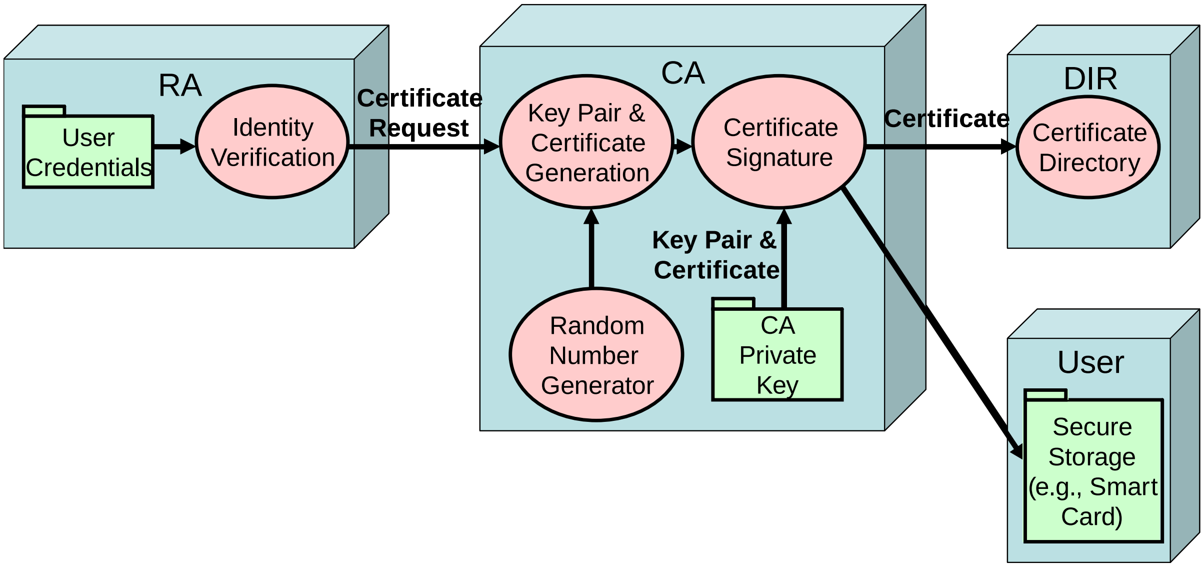

Figure 3-2: PKI Certificate Generation Process

3.3.2 PKI ARCHITECTURES

A PKI is often composed of many CAs that are linked by **trust relationships**. For example, a mission PKI could encompass CAs of two different space agencies.

Two main architectures exist to establish such relationships. The CAs may be arranged hierarchically under a 'root CA' that issues certificates to subordinate CAs (see figure 3-3). In those hierarchical models, a CA delegates trust when it certifies a subordinate CA. Trust delegation starts at a root CA that is trusted by every node in the infrastructure. The CAs can also be arranged independently in a mesh (see figure 3-4). In these mesh models, trust is established between any two CAs in peer relationships (**cross-certification**), thus allowing the possibility of multiple trust paths between any two CAs.

Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate.

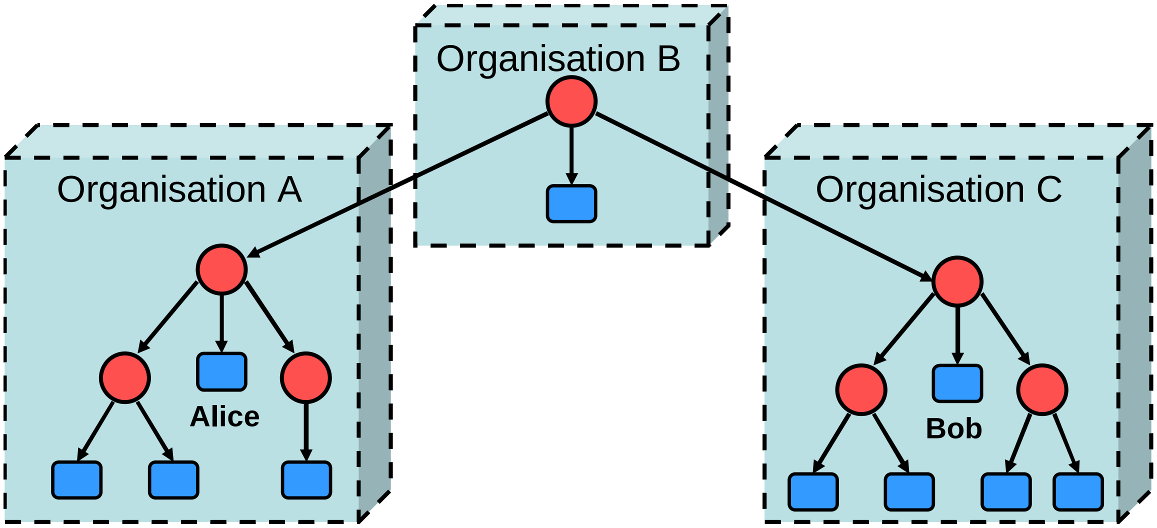

Figure 3-3: A Hierarchical PKI

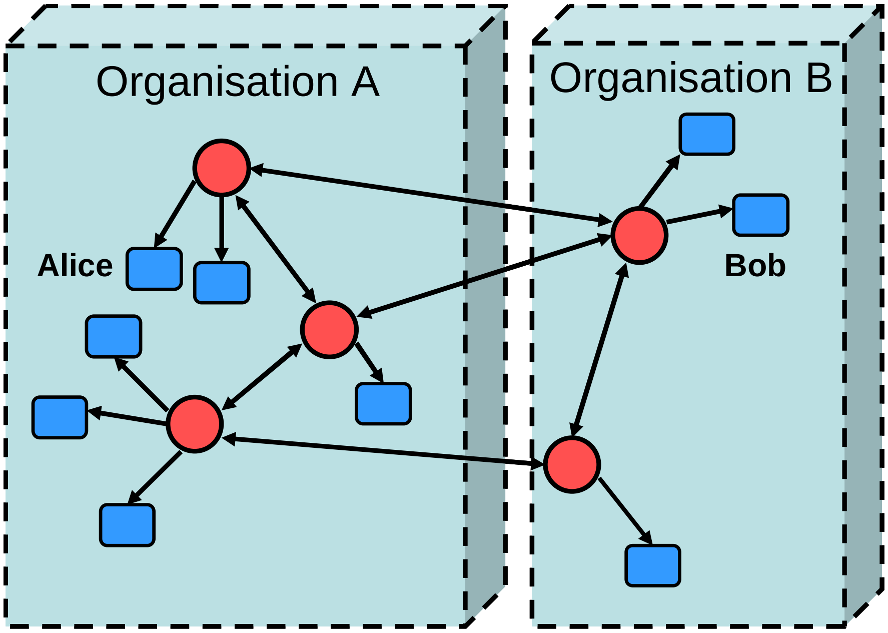

Figure 3-4: A Mesh-Based PKI

3.3.3 INTEROPERABILITY

To be useful in a global scale, PKI components need to interoperate regardless of the source of the equipment and the software involved. PKI technology promises to deliver security services across user communities, even where communication partners have not met face to face. However, the current PKI products and services fall somewhat short of this promise, and interoperability is one major reason for this. For example, incompatible transaction protocols and certificate formats prevent implementation of heterogeneous PKIs. PKI components from different vendors may be unable to communicate. PKI users may find they can communicate, but cannot process each other’s certificates. Although there have been several proposed formats for public key certificates, most certificates available today are based on the international standard **ITU-T X.509 version 3** (reference [13]). This standard defines a certificate structure that includes several optional extensions. The use of X.509v3 certificates is important because it provides interoperability between PKI components. Also, the standard’s defined extensions offer flexibility to support specific business needs. Reference [13] provides an implementation of ITU-T X.509 that is viable in the terrestrial Internet. X.509 could also be extended to the space segment. X.509-based spacecraft or instrument certificates would, for example, allow direct certificate-based authentication between spacecraft of different operating entities.

3.3.4 PKI ANALYSIS

The advantages of a PKI are as follows:

- **Identity Binding:** A PKI allows binding the identity of an entity to a public key (certificate). This allows advanced security concepts such as non-repudiation.
- **Scalability:** While the initial setup is substantial, the scalability of a PKI is much better for a large number of entities than that of an SKI.
- **Better Control:** Revocation list and revocation processes allow better control over the revocation and validity of cryptographic keys.
- **Initialization:** Although some form of initialization is required, key establishment in a public key cryptosystem is much easier than in a symmetric one, since no initial shared secret is required to be exchanged on a secure channel.

PKIs suffer from the following drawbacks:

- **High Complexity**: A PKI is composed from a large number of entities. These have to be properly deployed and configured. Thus a PKI is also very vulnerable to configuration errors.
- **Performance**: A PKI is based on asymmetric cryptography. However, secret key operations outperform asymmetric cryptography in processing speed by a large factor (up to 1000 in hardware implementations). The amount of memory required to store symmetric keys is substantially lower than for public/private key pairs or even public key certificates.

3.4 KEY TYPES AND MANAGEMENT

3.4.1 KEY MANAGEMENT POLICY

As mentioned already in 2.2.3, agencies that use cryptography are responsible for defining the **Key Management Policy** (KMP) that governs the lifecycle for the cryptographic keys. A **Key Management Practices Statement** (KMPS) is then developed based on the KMP and the actual applications supported. The KMPS should specify how key management procedures and techniques are used to enforce the KMP.

3.4.2 KEY USAGE

A cryptographic key should be used for only one purpose. For example, a given symmetric key may be used for the encryption of data OR the encryption of keys (key wrapping) OR the creation of a Message Authentication Code OR the generation of random numbers, but should not be used for more than one of these functions. A public/private key pair may be used for signing and verifying digital signatures OR establishing keys, but not both. The reason for this is that cryptanalysis is easier for an attacker if a key has multiple use cases.

3.4.3 KEY TYPES

Cryptographic keys exist in various forms, and each form is applicable to a specific operational area. It is important to formally differentiate between the following key types (more information on the various key types and their purpose is listed in annex A):

- signing and signature verification keys;
- public, secret, and private authentication keys;
- long and short term data encryption keys;
- random number generation keys;
- master key encrypting keys used for key wrapping;
- master key used for key derivation;
- keys derived from a master key;
- key transport public and private keys;
- secret, private, and public authorization key.

3.4.4 CRYPTOPERIODS

A **cryptoperiod** is the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system may remain in effect. A suitably defined cryptoperiod

- limits the amount of information protected by a given key that is available for cryptanalysis;
- limits the amount of exposure if a single key is compromised;
- limits the use of a particular algorithm to its estimated effective lifetime; and
- may limit the amount of time available for cryptanalytic attacks to be useful.

Trade-offs associated with the determination of cryptoperiods involve the risk and consequences of exposure.

Among the factors affecting the risk of exposure are:

- the strength of the cryptographic mechanisms (e.g., the algorithm, key length, mode of operation);
- the operating environment (e.g., secure limited access facility, open office environment, publicly accessible terminal);
- the volume of information flow or the number of transactions;
- the security function (e.g., data encryption, digital signature, key production or derivation, key protection);
- the number of nodes in a network that share a common key; and
- the threat to the information (e.g., who the information is protected from, and what are their perceived technical capabilities and financial resources to mount an attack).

In some cases, increased risk may suggest shorter cryptoperiods, while, in other cases, increased risk may suggest a need for longer cryptoperiods. For example, some cryptographic algorithms may be more vulnerable to cryptanalysis if the adversary has access to large volumes of stereotyped data that is encrypted under the same key. Particularly where a secret key is shared among several nodes, it may be prudent to employ short cryptoperiods for such algorithms. On the other hand, where the rekeying method is particularly subject to human error or other frailty, more frequent rekeying might actually increase the risk of exposure. It may be more important to have trusted expert invocation or supervision of the process than frequent repetition of the process.

The consequences of key exposure are measured by means of information sensitivity, the criticality of the processes protected by the cryptography, and the cost of recovery from the information or processes compromised. Sensitivity refers to the lifespan of the information being protected (e.g., 10 minutes, 10 days, or 10 years) and the potential consequences of a loss of protection for that information (e.g., the disclosure of the information to unauthorized entities). In general, as the sensitivity of the information or the criticality of the processes protected by cryptography increases, the length of the associated cryptoperiods should decrease in order to limit the damage that might result from each compromise. This is subject to the caveat regarding the security and integrity of the rekeying process. Particularly where denial of service is the paramount concern, and there is a significant potential for error in the rekeying process, short cryptoperiods may be counterproductive.

3.4.5 KEY ESTABLISHMENT

3.4.5.1 Overview

Key establishment constitutes the generation and sharing of cryptographic keys and other cryptographic material between communicating entities.

3.4.5.2 Secret (symmetric) Keys

Secret (symmetric) keys may be:

– generated and subsequently distributed either manually, using a public key transport mechanism, or using a previously distributed or agreed upon key encrypting key;

– determined using a key agreement scheme (i.e., the generation and distribution are accomplished with one process).

The symmetric keys must be determined by an approved method. The keys should be randomly generated and (optionally) distributed (transported) to another party, or may be determined by a key agreement mechanism. The confidentiality of the keys should be protected during distribution.

Key Generation: Symmetric (secret) keys should be generated using an approved key generation algorithm in a validated cryptographic module.

Key Distribution: Keys may be distributed manually or using an electronic key transport protocol.

– *Manual Key Distribution/Transport*: Keys distributed manually (i.e., by other than an electronic key transport protocol) should be protected throughout the distribution process using appropriate mechanisms defined by security policies. Master keys are always subject to manual distribution since they represent the top hierarchy level of an SKI.

– *Electronic Key Distribution/Transport*: Electronic key distribution/transport (via a communication channel, e.g., the Internet or a satellite transmission) requires the prior distribution of other keys higher in the hierarchy (i.e., KEKs) that will enable the distribution of the newly generated secret/symmetric keys. The key encrypting keys may be either secret keys used for key wrapping, or the public key of a public/private key pair.

3.4.5.3 Secret Key Agreement

Both the generation of keying material and the 'distribution' of that material may be accomplished using a **key agreement scheme**, which is actually a security protocol. Key agreement is used in a communication environment to establish keys using information contributed by all parties in the communication (most commonly, only two parties). Usually, such a key agreement protocol involves multiple communication round-trips between the communication partners and in some cases also a trusted third party that acts as a mediator between the two communication partners. A key agreement scheme and its associated key establishment protocol should provide the following assurances:

- entity authentication;
- key establishment;
- key confirmation;
- key recentness/freshness.

Examples for such protocols are the Needham-Schroeder-Lowe or the Yahalom-Lowe protocols (reference [17]).

3.4.5.4 Public/Private Key pairs

Generation: Public/private key pairs should be generated in accordance with the mathematical specifications of the appropriate approved standard. It is recommended that the key pairs be generated within an officially validated cryptographic module. Private signing, authentication and authorization keys should not be distributed to other entities. The use of self-signed certificates is not allowed.

Distribution: The distribution of the public key should provide assurance to the receiver of that key that:

- the true owner of the key is known (i.e., the owner of the public/private key pair);
- the purpose/usage of the key is known (e.g., RSA digital signatures or elliptic curve key agreement);
- any parameters associated with the public key are known (e.g., domain parameters);
- the public key has been properly generated (e.g., its mathematical properties are correct and the owner of the public key actually has the associated private key).

The private key is never distributed.

3.5 RANDOM NUMBER GENERATION

All cryptographic keys are generated based on random numbers. The quality of the random numbers that are generated by a random number generator directly propagates into the security of the keys. There are two kinds of random number generators:

– **Pseudo-Random Number (PRN) Generators**: These generators do not produce real random numbers but use a secret transformation function and a possible key input to produce numbers. They are sufficient for the generation of most low- to medium-level security operation keys.

– **Real Random Number Generators**: These generators use unpredictable physical effects (such as radioactive decay) to produce real random numbers. They are not implemented in software and are usually dedicated devices. They are required for high secure key production.

Random Number Generators and their specific properties are described in more detail in reference [12].

4 SPACE/GROUND KEY SHARING

4.1 OVERVIEW

This section describes different solution approaches for key management in the space segment (mostly in a point-to-point scenario, which is the standard security deployment for space missions today) and, more concretely, on the space-link extensions. It focuses on generation, exchange, and revocation of secret TPKs.

4.2 PROPERTIES OF THE SPACE ENVIRONMENT

The space environment is very different from communication environments on Earth such as the Internet. Special environmental constraints exist in the space domain and they pose specific challenges for the development of key management solutions. The following environmental properties are present in the space-link and can affect key management.

– **Asymmetric channels and bandwidth restrictions:** The physical communication channels between a ground station and a spacecraft are highly asymmetric. The uplink or telecommand channel is generally working at a bandwidth of 10-64 Kbit/s whereas the telemetry channel can support up to 2 Gb/s in modern missions. This asymmetry must be taken into account when designing space-link key management protocols.

– **Bandwidth** is a precious resource in space-link communication as it is directly connected to cost, energy consumption and frequency allocation. For key management, this means that traffic-intensive protocols should be avoided on the space-link.

– **Propagation Delay:** Because of the potentially enormous distance between the communication partners participating in a space-link communication session, the propagation delays can be quite substantial. Some key management protocols require multiple communication round-trips or include timestamps. Such protocols are not well suited for use in a space mission with high propagation delays.

– **Intermittent Connectivity:** Spacecraft generally do not have continuous connectivity to ground stations. Low Earth Orbit (LEO) missions can only communicate with a ground station when they are visible, whereas a planetary body may block deep space mission communication. Thus a hostile entity can attack the spacecraft while it is not visible by its operating agency and no active countermeasures can be taken.

– **Remote Location:** A spacecraft is operated completely remote in space. It is only connected to a ground station via a radio modulation link. Therefore, a compromised space segment results in loss of spacecraft control with no possibility of recovery. The remote location, however, has also benefits for key management. Since direct physical access to the spacecraft by an attacker is not possible, the installation of pre-shared information or secrets on-board the spacecraft is possible, which reduces the complexity of many key management protocols.

The same property indeed also nullifies the advantages of asymmetric key management systems for key exchange between the OCC and the spacecraft since there is no longer a need for establishing a key over an insecure medium.

– **Limited computational resources and memory:** Spacecraft on-board computers generally have limited computational power. Therefore, complex cryptographic operations such as those related to asymmetric cryptography should be avoided. In the case that the security system is located on a dedicated board, the number of gates required for symmetric key management protocols is also far less then for asymmetric protocols. Spacecraft memory is generally expensive and error prone. Therefore key management operations should only be using minimal memory resources.

The above properties imply that the use of secret key cryptosystems in space mission applications is more efficient than the use of public key cryptosystems.

4.3 SPACE-LINK KEY MANAGEMENT ENTITIES

The basic space mission setup as shown in figure 2-2 has only two entities that are involved in the key management process. This makes the system complexity very low. Those entities are

– the spacecraft;

– the Operational Control Centre (OCC).

The OCC acts as central key management and generation instance/facility. It is responsible for generating new keys, managing the key lifecycle and revoking old or corrupt keys. The spacecraft and the ground station(s) are usually not appropriate for this. The spacecraft has very limited resources and user intervention is only possible to a certain extent.

The spacecraft needs keys in order to execute security functions on incoming TC/AOS and outgoing TM/AOS data structures.

The following elements may optionally participate in the key management:

– the ground station(s);

– end user facilities.

Ground stations may only be participating as key management entities if they are working as security gateways. This may be the case if the COP-1 (reference [16]) loop is closed at the ground station. Additional end user facilities may be present in the network if the mission has payload data dissemination requirements.

4.4 SPACE-GROUND KEY DISTRIBUTION MODELS

4.4.1 GENERAL

Various models to establish, upload, or exchange traffic protection keys (TPKs) between the OCC and the spacecraft exist.

4.4.2 KEY GENERATION

It is assumed that the entity that is responsible for key generation is the OCC or a co-located authority. Therefore all (symmetric and asymmetric) key generation procedures and policies affect the ground segment only. All keys should be generated using a validated cryptographic module and a sufficiently secure random number generator (see 3.5). In addition, the key generation facility must be physically and logically access controlled and protected by security policy regulations. Special care has to be taken for the generation of master keys that are stored on-board the spacecraft before launch. As the OCC has also to maintain a copy, special protection of this data is crucial. It is recommended to store them on a highly secure storage device such as a smart card and in a physically protected place.

The generation of TPKs that are exchanged under master key encryption may take place directly inside the operational network as corruption of TPKs generally does not threaten the whole security infrastructure. In addition, it must be possible to automate the process.

4.4.3 SECRET KEY DISTRIBUTION MODELS

4.4.3.1 General

As for all SKIs, symmetric key management on the space-link requires the storage of an **initial shared secret on-board the spacecraft** before launch. Without this initial shared secret, secure key management is not possible on the space link. Figure 4-1 shows the key management between the OCC and the spacecraft based on a pre-launch key sharing.

In all of the cases below, the OCC is responsible for managing key references and triggers the key switch events by using telecommands. It is advisable to have a **security reporting mechanism** in place that reports, e.g., failed telecommand authentication to the control centre. The implementation specifics of such a mechanism are beyond the scope of this report.

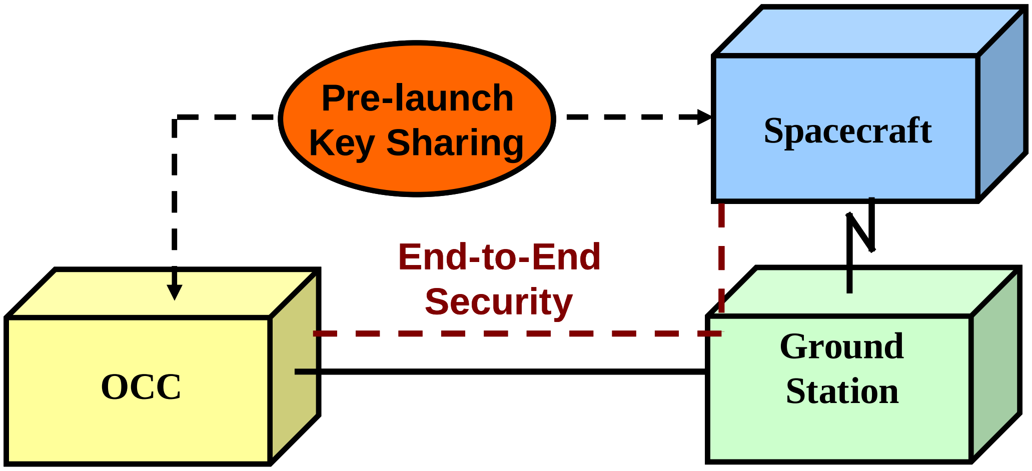

Figure 4-1: Pre-Launch Key Sharing

4.4.3.2 Initial Secret Storage

The initial shared secret consists of a certain number of master keys that are required for deriving or exchanging further static keys. These master keys require strong protection as they are of central importance and corruption might result in a loss of the security system. The number of pre-shared master keys is dependent on their proposed cryptoperiod and the resources available on the spacecraft. However, **a large number of keys does not necessarily result in the system's being more secure**. In case of ground master key storage corruption, all keys are compromised and insecure to use. Protection of the keys in the OCC implies **security aware personnel** and **strict security policies**. The master keys must never be used directly to protect telecommand or telemetry data, except when there are no other TPK types foreseen in a mission. Instead, they should be used either to generate or exchange new keys of a lower hierarchy level.

4.4.3.3 Usage of Master Keys as TPKs

In a configuration using master keys as TPKs, the master keys are directly consumed by the security functions on ground and on the spacecraft. Therefore, no other types of keys are present and the key hierarchy is reduced to one level. This solution is simplistic and straightforward to implement. All the key management operations are conducted prior to launch and only the frequent switching of keys must be cared for. Taking into account the lifespan of operational keys, this approach generally requires a large number of keys stored on-board, and the mission must make sure that there are enough spare keys to prevent it from running out of keys. This includes taking into account the possibly of extended mission lifetimes and key corruption through memory failures. If these master keys are depleted or all of them are corrupted, the security of the mission is void and the spacecraft cannot recover from this state. Therefore, a substantial amount of protected memory must be installed on the spacecraft that holds the keys.

4.4.3.4 Usage of Master Keys to derive TPKs

Master Keys can be used as an input to a one-way hash or similar cryptographic function to generate operational TPKs for the cryptographic operations. This configuration is called TPK **derivation from master keys**. Master keys are no longer directly exposed to the cryptographic operations and a classification difference between master and TPKs can be maintained. Also, the number of required master keys is reduced. It has been proven that the security of the master key can be significantly enhanced by this process (reference [14]).

However, as a drawback, the security of the mission is directly bound to the security of the derivation function. Corruption of a master key may still lead to a complete loss of the security system since the attacker can now compute all TPKs from this master key. A possible countermeasure to this threat is the usage a spacecraft-specific nonce such as a random number that is taken into account during the computation of the TPKs.

4.4.3.5 Usage of Master Keys as Key Encryption Keys

The configuration using master keys as key encryption keys best represents the hierarchical structure of an SKI. The master keys are used as KEKs and provide confidentiality for the upload of TPKs or lower hierarchy KEKs. This principle is called **key wrapping**. It reduces the amount of master keys that have to be pre-shared between the OCC and the spacecraft. Also, since master keys are only used for the encryption of other cryptographic material that has no direct semantic structure, cryptanalysis to break the master keys is a challenging endeavour and substantially more difficult than for data with semantic structure (such as a protocol header). This allows a further reduction of the number of master keys and saves spacecraft memory. If a large number of TPKs are required for the mission, an additional KEK hierarchy level can be introduced to further reduce the required number of master keys. This configuration allows different security classification levels and thus different key handling security policies for the hierarchy levels of the SKI. It also allows a clear separation between KEKs that handle different key types.

Master key encrypted TPK exchange is a common process in the spacecraft lifetime and must therefore be automated to a certain extent. Given the data rates, TM payload TPKs are much more frequently replaced than TC TPKs. In the optimal case, new payload TM TPKs are needed for every data transfer session. The key encryption process on the ground must take place in a secure environment inside the OCC that is connected to the rest of the environment via a set of well defined interfaces. A major challenge in key exchange is the **reception confirmation**. The simplest approach is to upload TPKs that are not immediately going into operation. This gives the communication infrastructure time to confirm successful key reception. The old operating key still protects the confirmation and no synchronization issues arise. If an uploaded TPK is intended for immediate usage, the system has to face the synchronization problem. An explicit implementation of the reception status report mechanism is not really necessary if one can exploit the previously existing reporting mechanisms such as the COP-1 (reference [16]) loop for that purpose. Of course, this limits the implementation possibilities for security mechanisms on-board the spacecraft.

Table 4-1: Space Link Key Management Overview

Key distribution mechanism	Benefits	Drawbacks
Master Keys as TPKs	Simple implementation	Classification problem Many master keys required Substantial amount of protected memory required
TPK Derivation	Fewer master keys required Security of master keys improved	Mission security bound to the security of the (secret) derivation function
TPK Wrapping	Allows key hierarchy and classification levels	Implementation more complex

4.4.4 ASYMMETRIC KEY EXCHANGE

While it is generally possible to use asymmetric key exchange models on the space-link, the disadvantages as outlined in 4.2 have to be taken into account. Should a mission still have a requirement for an asymmetric key establishment model, then traffic keys can be established using the **Diffie-Hellman** key establishment protocol.

The Diffie-Hellman (DH) key establishment protocol (reference [15]) establishes a shared secret between two communicating entities over an insecure channel. Figure 4-2 shows the establishment of a shared secret using DH between the OCC and the spacecraft. In a first step, the OCC generates a prime number *p* and a base *g*. Then it chooses a secret integer *a* (its private key) and computes the public key *A* as shown. Next, it sends *(g, p, A)* to the spacecraft. The spacecraft now generates its own private key *b*, computes the public key *B* and sends it to the OCC. Now both, the OCC and the spacecraft, can compute the established key *K*. The DH protocol can also benefit from a pre-shared master key secret to prevent man-in-the-middle attacks.

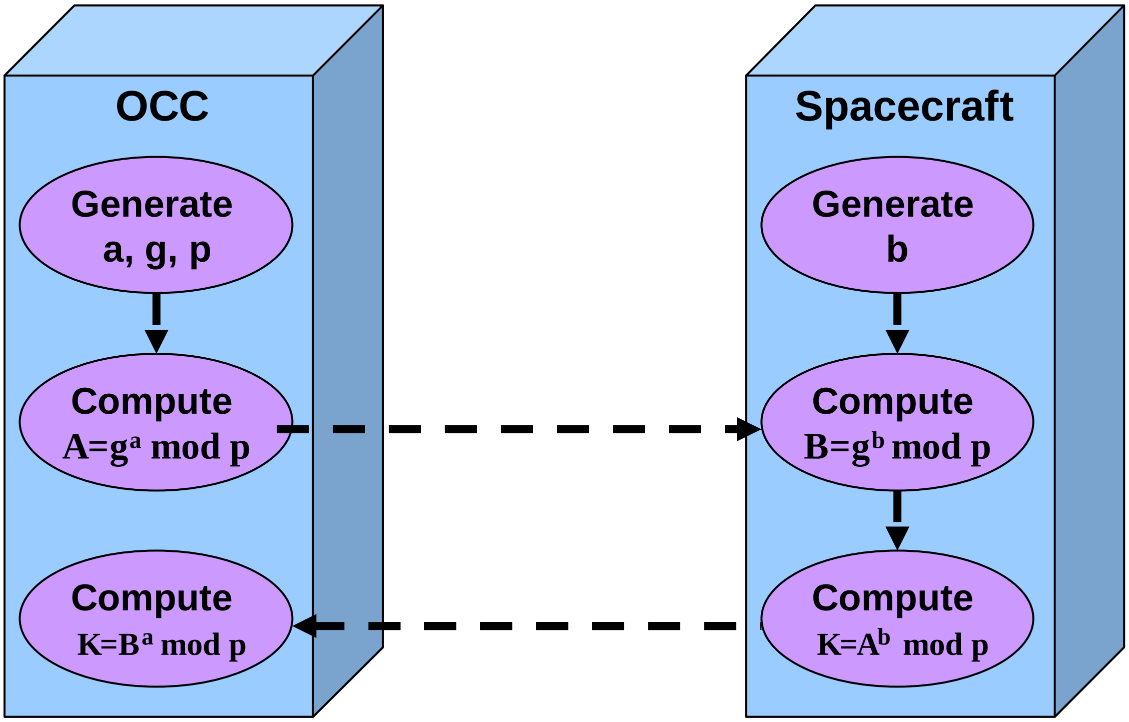

Figure 4-2: Diffie Hellman Key Exchange between OCC and Spacecraft

4.4.5 KEY REVOCATION

In the general case, keys get revoked if they are no longer in use or required. For space-link communication this can be achieved by simply **deleting the keys on the spacecraft** because they are not used for long term encryption or signatures. For archiving purposes, the keys can still be stored in the ground system. This prohibits misuse of old keys by an attacker who manages to break a key after a long time of cryptanalysis. A different situation unfolds for master keys. For emergency situation reasons they should not be deleted but only flagged as revoked if they are revoked. Key revocation is not identical with key switching on-board the spacecraft.

4.4.6 KEY MANAGEMENT DATA STRUCTURES

4.4.6.1 General

The upload of new keys over the space-link is connected to special requirements. Since an SKI is used to protect the space-link, keys **must not** be transmitted unprotected. They must be kept confidential and the associated transport data structure must be authenticated and checked for integrity. An appropriate encryption algorithm implements confidentiality while authenticity and integrity of the transporting command data structure is provided by an authentication algorithm. CCSDS provides recommendations for both algorithm types (reference [6]).

To provide the key transportation and protection services as addressed above, telecommand data structures need to be modified and certain security control command schemes and data structures need to be added. This is not part of the key management and thus not discussed here. *The Application of CCSDS Protocols to Secure Systems (*reference [1]) contains more information on the localization problem.

4.4.6.2 Key Management Related Security Commands

In order to command the security unit on-board the spacecraft in the context of key management and in the scenario described in 4.4.3.5, a number of special security commands are required. These are subject to specific mission security requirements. However, in order to guarantee secure key management, the following types of telecommands should be supported:

- **Upload of a new key**: uploads a new key or a set of new keys to the spacecraft security unit. The key(s) in this command must be protected by a key that is at least one hierarchy level higher than the key(s) to be uploaded. Each command may only contain keys that are of the same type.

- **Key revocation**: causes the revocation of one or more keys on-board the spacecraft. It must be authenticated by a key that is at least one hierarchy level higher than the key to be revoked (exception: master keys). The keys are to be identified by means of the Key ID (or a Key ID/Spacecraft ID (SCID) combination in case of multiple spacecraft missions).

- **Key switch**: triggers the switching of a specific key on-board the spacecraft with a key that has already been uploaded. It must be authenticated by a key that is at least the same hierarchy level as the key to be switched. The key is to be identified by a combination of the SCID and the Key ID. This command may be combined with the '*Upload of a new Key*' command if required by the mission.

For all of these commands, an appropriate reporting mechanism must be employed to notify the OCC of the outcome of the security operations on-board the spacecraft. If required according to the mission classification (see *Security Architecture for Space Data Systems* (reference [5])*)* the reporting must be secured by appropriate security functions as well.

4.5 EXTENSION TO PAYLOAD DATA DISSEMINATION MODELS

4.5.1 GENERAL

As stated in 2.4.3, from a key management perspective, missions with ground key dissemination requirements are an extension of the point-to-point space-link missions. In addition to key management requirements between the spacecraft and the OCC, these missions also require key management associations between different on-board payload units and a number of ground segment entities. Those ground segment entities may not always be under the control of the operating entity and may include, for example, end users or science data customers.

As a consequence, a differentiation has to be made between payload data dissemination key management that serves entities in the internal network (controlled by the spacecraft operating entity) and key management that serves entities in external networks. In this subsection, the changes with respect to the space-link key management are addressed while ground segment issues are only mentioned for the sake of clarity and completeness.

4.5.2 OCC KEY MANAGEMENT GATEWAY WITH CENTRAL STORAGE

The OCC key management gateway with central storage solution, in which it is required that the operating entity is considered to be trustworthy by all possible ground segment entities, is the most straight-forward and widely used key management solution for secure telemetry data distribution. Figure 4-3 illustrates this setup. Two individual and separate key management systems are employed. The first is associated with the space link and is identical to one-hop key management as described in 4.4.3. All other key management associations are handled by a separate ground key management system that is based on a PKI. The OCC takes on the responsibilities of a CA for the ground segment PKI. Keys are distributed and negotiated using well-known Internet standards such as the Internet Key Exchange Protocol (IKE) (reference [4]).

All telemetry that is communicated from the spacecraft is pre-processed and stored in a telemetry database in the OCC. The OCC can then manage an access control database and assign access rights to the individual external entities that have received a public key certificate. If end users want access to a certain telemetry data set, they have to request it using their public key certificate. The OCC can then validate the certificate and potentially grant access to the requested data.

NOTE – The access control database is separate from the database which controls access to the telemetry database. It should be noted also that access control requires additional security services that are outside the scope of this report.

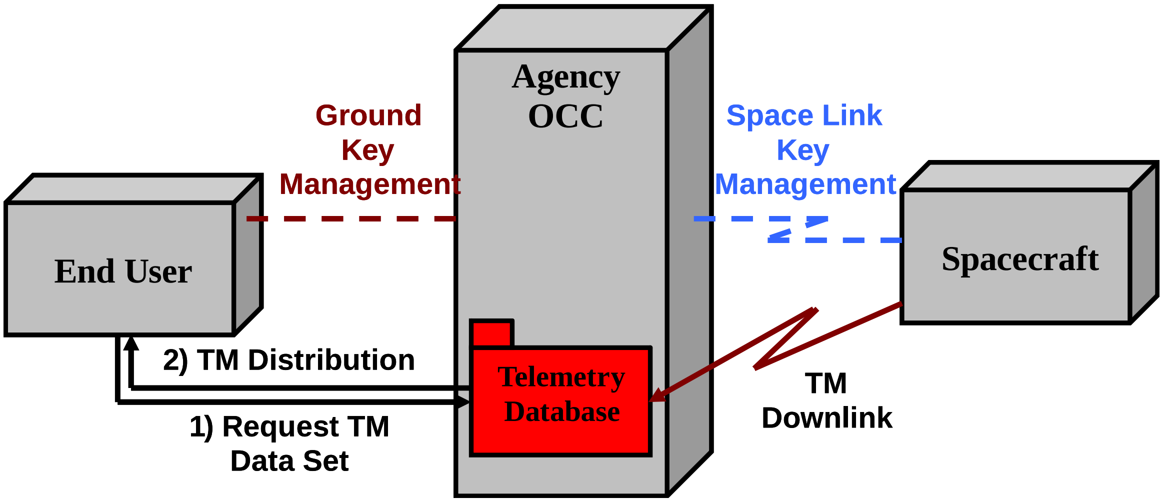

Figure 4-3: Centralized Ground Station Telemetry Dissemination

The benefit of this solution is that the two key management systems are completely separated. Thus they can be bought as COTS products and do not require any modification. On the downside, such a system is extremely inflexible and has a number of drawbacks. First, telemetry cannot be delivered in real time to end users. For some scenarios this is a crucial requirement. Further, end users have to (1) trust the operating entity and (2) have to be part of the operating entity's PKI.

4.5.3 OCC KEY MANAGEMENT WITH DIRECT KEY ASSOCIATIONS

In the OCC key management with direct key associations setup, illustrated in figure 4-4, the end users can have access to real-time telemetry that is directly forwarded from the spacecraft (either through an operating entity antenna or a user-owned antenna). To achieve this, it is required that the users, after appropriate authentication and authorization, receive the space-link telemetry decryption keys. A major challenge here is the definition of the amount of data for which a given space-link decryption key is valid. A logical assumption is that one decryption key is valid for the duration of one downlink session. Other validity periods can be used as well. Following the assumption, a user who receives a decryption key can access all telemetry of this particular downlink session. If such a classification is not good enough, an individual end-to-end key management solution is needed (see 4.5.4).

To gain access to a specific telemetry session, a user must:

a) Request the decryption key for a telemetry downlink session from the OCC before the download session begins. User authentication and authorization credentials must be provided (either through the public key certificate or otherwise, e.g., proof of payment). If possible, the decryption key can also be delivered via manual key distribution using smart cards or other secure transport devices.

b) Receive, after successful authentication and authorization, the (protected) TPK from the OCC.

c) Access the telemetry data stream (potential authentication using public key certificate required) and decrypt telemetry data with the valid TPK.

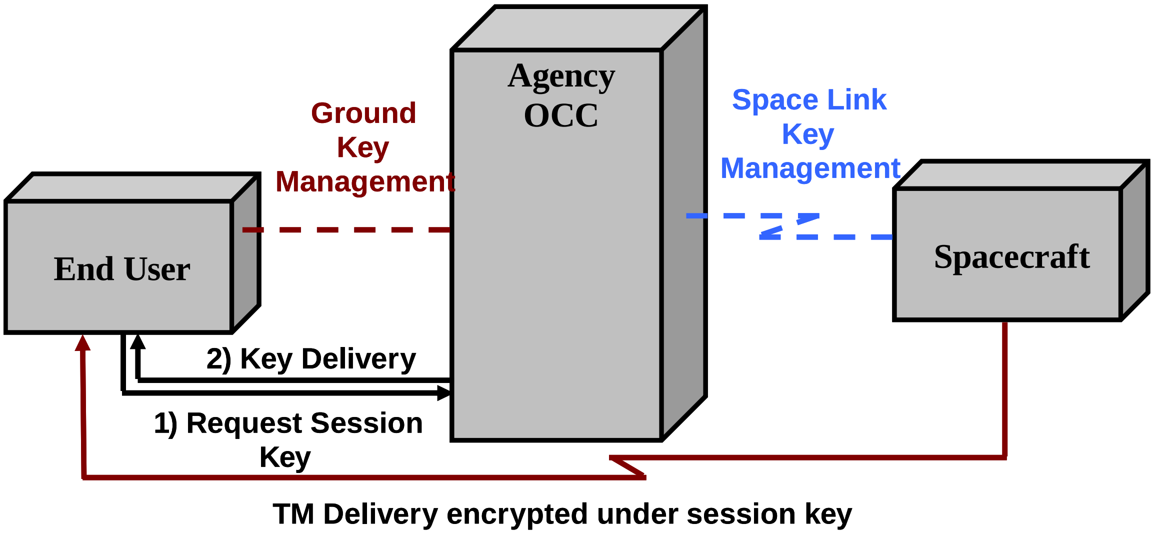

Figure 4-4: Key Management with Direct Key Associations

4.5.4 INDIVIDUAL END-TO-END KEY MANAGEMENT

In the case that authentication per session is not sufficient but user access should be restricted to a specific data reception, the spacecraft must encrypt each data reception with a new key. While this leads to a significant increase in key material on-board the spacecraft, it provides maximum flexibility for user access to live telemetry. The process for the key distribution on the ground is identical to the process described in 4.5.3.

The following possibilities exist to reduce the resulting key management complexity on the spacecraft. The TPKs for the encryption of individual data reception can be derived from the initial TPK using a secure transformation function (such as XOR), a seed, and a transformation key. As a result, there would still be only one TPK per downlink session required and the individual data reception encryption keys are a function of this transformation. The same function, transformation keys, and seed are present in the OCC and can be used to compute the data take keys for the end users. Figure 4-5 illustrates this concept.

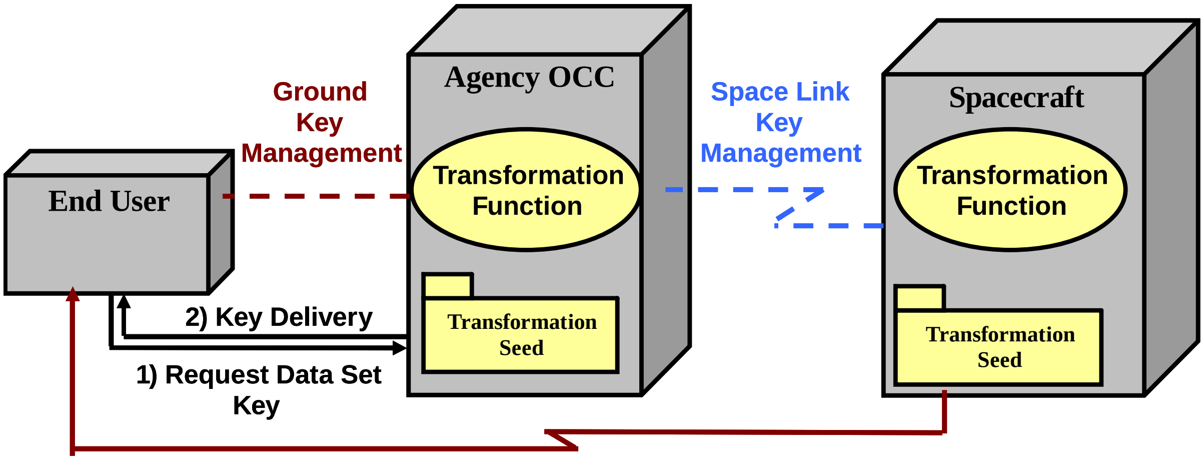

Figure 4-5: Individual End-to-End Key Management

4.5.5 USER-OWNED PAYLOAD MODULES WITH OWN CRYPTO SYSTEMS

In some cases, a user may own a payload instrument on-board the spacecraft and is only using the spacecraft bus and spacecraft control as a service provided by the operating entity. In such a case, the payload instrument may host its own crypto unit and the operating entity may not have access to this crypto unit or the keys that are stored in it. Thus the user wishes to build a secure encryption and authentication tunnel through the telemetry channel that is under the control of the operating entity as is shown in figure 4-6. As a consequence, the operating entity may no longer serve as a central key management institution since it is not considered to be trusted by the user.

The user can execute key wrapping or other key management processes with his payload crypto unit by providing a set of *encrypted* TPKs to the agency. The operating entity can then embed those keys in one or more telecommands addressed for the payload crypto unit. It should be noted that the operating entity cannot access these keys, since they are encrypted under the KEK to which the agency does not have access. The connection between the user and the OCC is therefore characterized by multi-layer security. On the one hand, there is the direct encryption of the TPKs by the KEK, and on the other hand, the communication session between the end user and the OCC is protected using the capabilities of the operating entity PKI. Should the payload be controlled directly from the users premises, the encrypted TPKs can already there be incorporated into telecommands before being sent to the OCC for uplink.

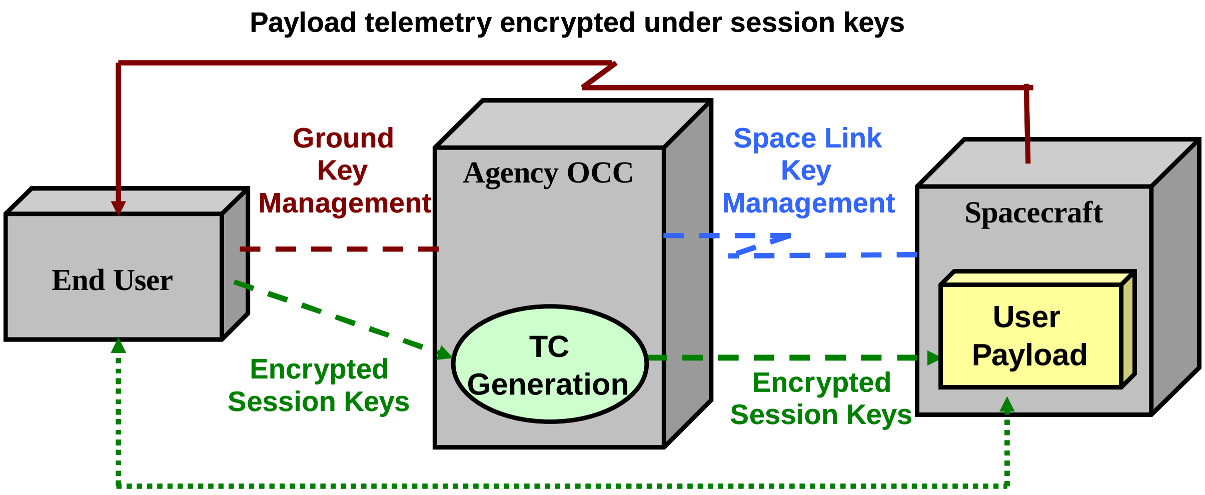

Figure 4-6: User-Owned Payload Modules with Own Crypto Systems

4.5.6 EXTENSION FOR PAYLOAD DATA DISSEMINATION SUMMARY

The previous subsections have discussed a number of possible key management models for payload data dissemination between the spacecraft and the end users. The most appropriate model is clearly dependent on the mission requirements defined by the user and by the operating entity.

4.6 SPACECRAFT CONSTELLATIONS

4.6.1 GENERAL

Spacecraft constellations have the most complex key management requirements. Two levels of complexity exist for a spacecraft constellation key management system: **Individual key management** and **spacecraft constellation management**. However, while full spacecraft constellations that are based on space internetworking using the DTN bundle protocol (reference [3]) or other internetworking technology will certainly be a topic of central importance in future space missions (see section 6), they are not widely used today.

4.6.2 INDIVIDUAL KEY MANAGEMENT

If each spacecraft in the constellation is commanded independently, the overall key management system can be broken down into a number of isolated key management systems that have the same layout as in the previously addressed scenarios. Since this is not a full spacecraft constellation using internetworking, but each spacecraft is controlled individually and independently from the other spacecraft, it simplifies key management and allows re-use of legacy solutions. Ground stations act as transparent routing entities and are therefore not part of the key management.

Should the constellation be controlled by a single OCC, then it serves as a central key management centre and operates a space-link key management system with each spacecraft individually. Often, however, spacecraft constellations are controlled by two or more OCCs. In this case, each OCC acts as an instance of a mesh-based PKI. Those instances must be directly synchronized using secure connections. This allows hot redundancy and handovers of spacecraft.

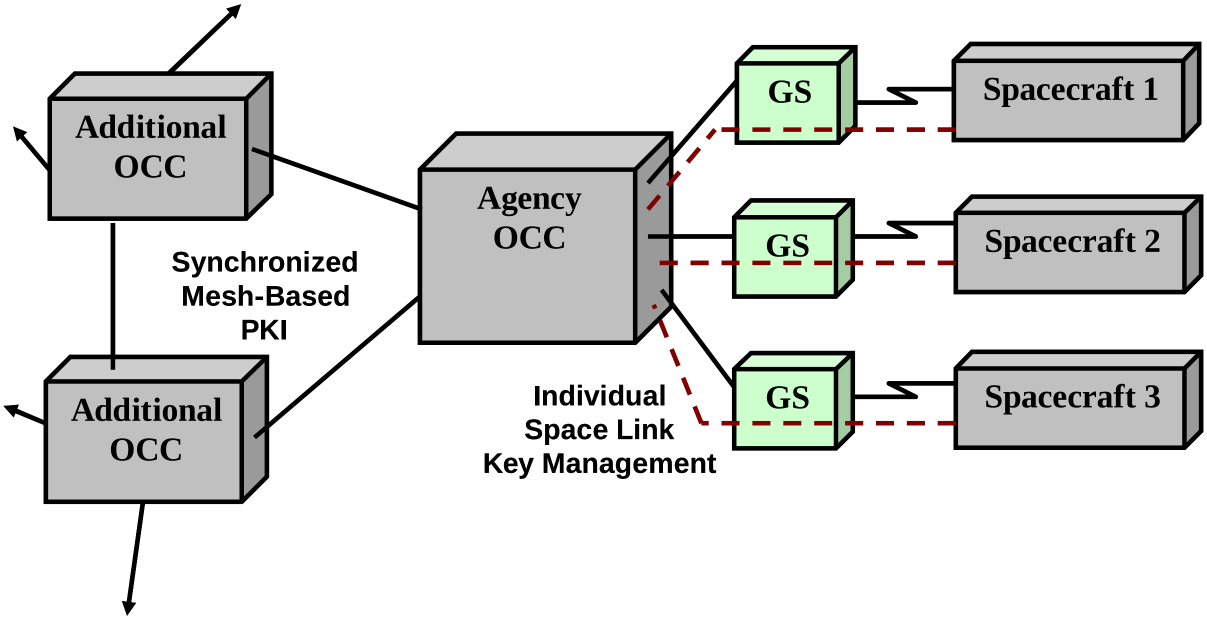

Figure 4-7: Constellation with Individual Key Management

This scenario can be subject to the different ground data dissemination extensions for key management that were introduced in 4.5.

4.6.3 FULL INTERNETWORKING CONSTELLATION KEY MANAGEMENT

In full constellation scenarios that make use of internetworking technology, where each spacecraft, ground station, OCC, and end user are individual nodes in a global network topology, and each group of nodes may potentially need to establish a key management association, an Internet-inspired key management solution must be employed. The nodes may have different rights to manipulate the key management system and also different access rights to data streams. This requires a full identity hierarchy and complex key negotiation protocols. Group key management will become an issue and group key management protocols similar to GSAKMP (reference [11]) may need to be employed. They need to be backed up by space network equivalents of the IKE (reference [4]) and IPSec (reference [2]) protocols. A lot of research is currently going on in the area of spacecraft internetworking, and it remains to be seen whether Internet key management solutions can be easily adapted to the space environment or new concepts have to be developed.

4.7 CONTINGENCY OPERATIONS AND CLEAR MODE

Should a spacecraft be subject to direct environmental hazards or erroneous commanding, it may start tumbling or be otherwise negatively affected. Also, failures of on-board processing hardware may occur at any time. In such situations, a spacecraft usually enters ‘safe mode’, where all but the most vital commanding functions are disabled. This may also affect the spacecraft security unit. Current practice in low to medium security space missions is either the complete deactivation of the security functions or the bypass of the security functions.

If security functions are disabled, the upload of new keying material becomes impossible. The reason for this is that the spacecraft operates in clear mode and can no longer decrypt and authenticate keys. Also, keys can obviously not be transmitted in plaintext. In this case, a **fallback set of master keys** must exist on-board the spacecraft. This set of master keys is used to securely re-enable security functions and upload new sets of TPKs after the spacecraft is back to normal operation. If those master keys do not exist, secure upload of new keys is impossible. Depending on the mission requirements, they may need to be specifically flagged as fallback keys. It has to be noted that the fallback master keys must not be used to encrypt semantic data structures (such as packets). Otherwise, they cannot be used more than once and a new master key has to be relocated after each safe mode situation. It should be noted further that the number of master keys on-board the spacecraft is usually limited and they cannot be re-uploaded. Another possibility for the spacecraft is to restore the internal state that is had before it entered safe mode. This works only in the case that the on-board key memory was not deleted or damaged and that the attacker could not have accessed it during clear mode.

Should the security unit be bypassed only, it is still active and the bypass can be deactivated using special authenticated commands. These commands are authenticated with special master keys that are designated only to this task.

To summarize, space missions must take into consideration the special influence of safe mode and contingency operations on the security functions and key management in particular. Special master keys must be provided to ensure the re-establishment of security following a safe-mode operation. Failure to include such requirements may lead to a critical security vulnerability in the space mission security concept.

5 GROUND SEGMENT KEY MANAGEMENT

In the ground network infrastructure, it is desirable to use existing and established key management protocols. The ground segment is divided into two areas: the **core ground segment** and the **external ground segment**. Figure 5-1 illustrates that concept.

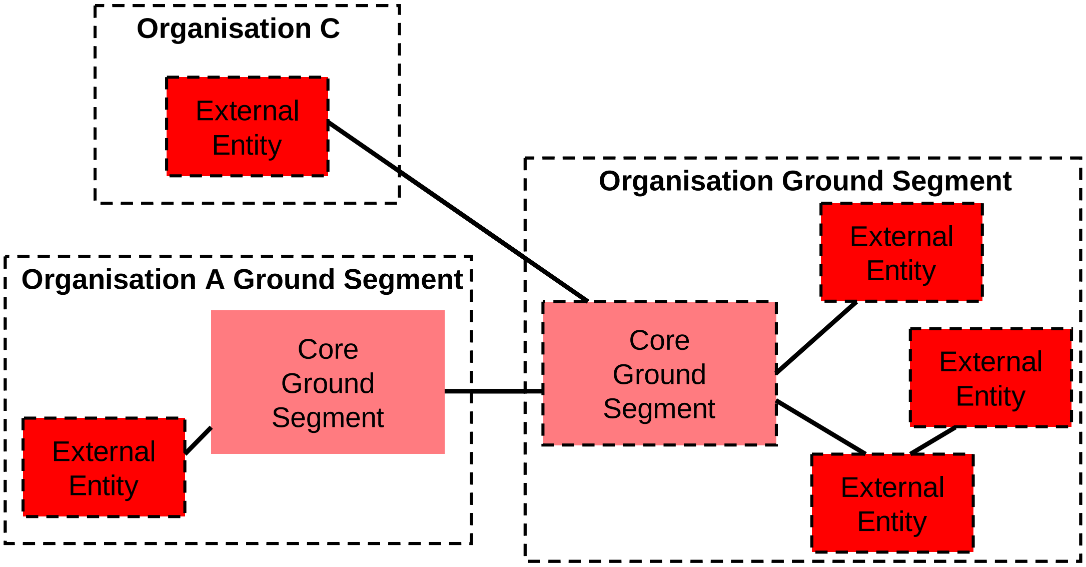

Figure 5-1: Ground Segment Division

The core ground segment includes all equipment and nodes that are owned by the operating entity 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 *Guide for Secure System Interconnection*, reference [10]), equipment that is owned by another agency can be treated either as core nodes or as external nodes. 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 Space-Link Extensions (SLE) or the bundle protocol) it should be possible to use them to tunnel IP so that the key management can still be realised.

For key distribution and establishment procedure, the **Internet Key Exchange Protocol (IKE)** (reference [4]) is the best solution because of its widespread deployment and because it is a widely recognized standard.

For the key management process within the ground segment, an agency or governmental owned PKI is deployed inside the trusted ground segment. Following this, the first phase of the IKE protocol can be executed based on public key certificates. In the external ground segment, a shared secret has to be in place before the IKE protocol is initiated. This secret can be distributed through a secure external channel. Certificates may be used here as well, as long as they are issued by a third party who is trusted by the agency. The second phase of the IKE protocol, the quick mode, is identical for the core and external ground segments.

6 FUTURE SPACE MISSIONS

It is anticipated that future, next generation space missions will no longer operate as isolated communication infrastructures, but rather as a 'network of space-based entities' formed with links between the different, heterogeneous nodes, similar to the full internetworking spacecraft network scenario described in 4.6.3. This will include spacecraft from different operating entities, as well as other planetary assets such as Lunar or Mars rovers and bases. Figure 6-1 shows a NASA illustration of such a communications architecture from reference [15].

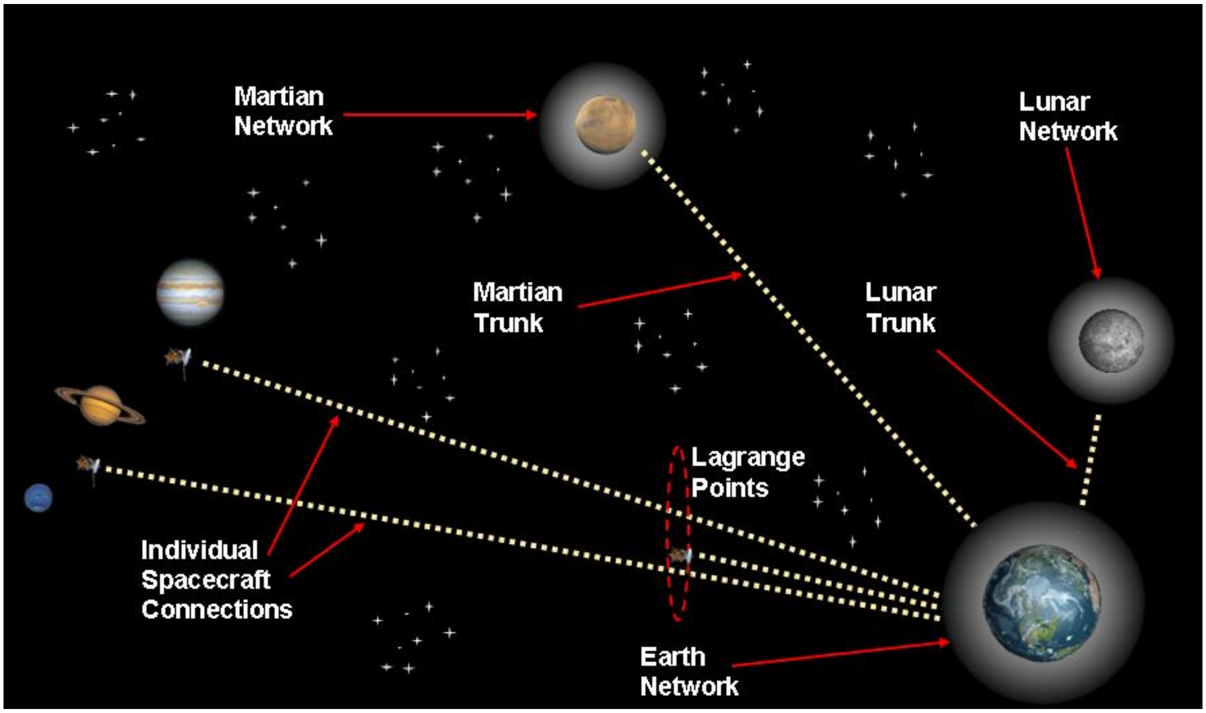

Figure 6-1: NASA Next Generation Space Network Vision

A space network will have substantially different and more complex key management requirements than current or near future space missions that have been discussed previously. No definitive architecture baseline has been agreed upon for such a network, although multiple approaches have been proposed and the DTN approach (reference [3]) may eventually qualify for this new baseline. However, since such a fixed baseline does not yet exist, this document cannot now propose or specify a key management architecture for these networks.[1]

Instead, rather than present different possible approaches, this section summarizes various environmental properties of future space networks and their influence on key management:

[1] Future revisions of this document may, however, incorporate such architecture, should the baseline be decided upon.

- **Number of Nodes:** The first and most obvious factor is the number of nodes that participate in such a network. It is no longer possible to assume a maximum of a handful of nodes. The network may scale to hundreds or even thousands of nodes. This has special impact on key management because the deployment of an SKI becomes increasingly difficult assuming that each two nodes potentially need to share a common secret. Therefore, **scalability will become a major issue** and may trigger the introduction of public key systems into the space segment.

- **Node Variety:** The nodes deployed in a future space network will be heterogeneous and will have varying resources at their disposal. This may enable the nomination of certain nodes with extensive resources to fulfil special roles in the key management process such as group operators (e.g., GSAKMP group key managers) or even key infrastructure central roles such as a CA. In particular, this also means that the OCC is no longer the single focal point for most key management and security operations.

- **Network/Bundle Layer Convergence:** It can be expected that next generation space networks will make use of extensive network layer functionalities such as routing. Also, Internetworking Protocols such as IP and the DTN bundle protocol overlay will likely be used in the space networks to ensure maximum interoperability. As a result, network or bundle layer-based key management solutions may also be employed in space networks.

Given these properties of future spacecraft networks, future key management architectures will most likely be very similar to an Internet solution with some extensions to handle special space-related environmental issues such as large propagation delays, link outages, etc. These extensions could be addressed by a special DTN key management protocol.

7 SUMMATION AND RELATION TO OTHER DOCUMENTS

7.1 OVERVIEW

This Report is concerned with the study of different strategies and models for key management in CCSDS-compliant space missions. In this section, cross-references to other security related CCSDS documents are provided where applicable.

7.2 MISSION PROFILES MAPPING

Security Architecture for Space Missions (reference [5]) includes a number of mission profiles. In the following, a mapping of these mission profiles to appropriate key management requirements and techniques is provided. The following mission classes can be distinguished:

a) **Meteorological Missions (Weather, Earth Observation):** These missions typically use TC authentication, TC encryption, and potentially payload TM encryption. If the latter is not required, a simple space-link Over-The-Air-Rekeying (OTAR) key management scheme as described in 4.4.3.5 could be employed. Should payload data encryption be required, then a ground key management system must also be in place to cover the agency and all potential end users. This might also be extensible to include end users upon request (e.g., by issuing a certificate). Furthermore, depending on the configuration of the payload data dissemination system, one of the key management extensions for data dissemination as described in 4.5 must be in place.

b) **Communications Missions:** Depending on the use-case scenarios for a communication mission (private telecommunications, governmental, dual-use), different key management requirements may arise. A basic space-link OTAR key management scheme as described in 4.4.3.5 could be employed to support protection of the command and housekeeping telemetry links. In most cases the telecommunication payload on-board the spacecraft will only provide relaying or broadcasting services, but the communication endpoints are always located on Earth. Thus ground key management must be employed to equip the communication partners with keys and be completely independent of the space segment. Should a communication partner be located in a rural environment with no access to terrestrial infrastructure, then key management over the spacecraft link may be required (if two-way communications is supported by the spacecraft). But this requires only relay services by the spacecraft since the key negotiation is with the OCC.

c) **Science Missions:** Science missions usually do not have high security requirements other than authentication of the telecommand link. Therefore the storage of a fixed set of master keys as described in 4.4.3.3 may be the best solution.

d) **Navigation Missions:** Navigation Missions can be treated as constellation missions and therefore the key management extensions for such missions could apply. Here, it is especially important to determine whether the spacecraft are controlled individually or as a constellation.

e) **Manned Space Missions:** Manned space missions have special security requirements which are beyond the scope of this document.

ANNEX A

KEY TYPES AND CRYPTOPERIODS

A1 OVERVIEW

This annex summarizes the most important information from reference [12] that is relevant to space mission key management.

A2 KEY TYPES

Cryptographic keys exist in various forms and each form is applicable to a specific operational area. In order to understand some of the cryptographic infrastructure it is important to formally classify the key types:

- **Signing keys:** Signing keys are the private keys of a public/private key pair used by public key algorithms to generate digital signatures with possible long-term implications. When properly handled, signing keys can be used to assure authentication, integrity and non-repudiation. Signing keys require confidentiality and integrity protection, and correct association with any domain parameters. If multiple signing keys are used (e.g., for different applications), then provision must be made to ensure that each key is only used for the appropriate application or usage.

- **Signature verification keys:** Signature verification keys are the public keys of a public/private key pair used by a public key algorithm to verify digital signatures, either for non-repudiation purposes, to determine the integrity of data, to authenticate a user's identity, or a combination thereof. The integrity of these keys must be protected, and an association with any domain parameters, the usage or application, the public key owner, and the correct signing key must be assured. The key must be validated to ensure that the purported owner of the key has the private signing key (i.e., proof of possession must be established). The verification key needs to be available while any data signed using the associated private key may need to be verified. There is no requirement for the confidentiality of signature verification keys.

- **Secret authentication keys:** Secret authentication keys are used with symmetric key algorithms to authenticate users, messages, or communication sessions. These keys must remain confidential, and the integrity must be protected. The association with another entity using that key must be maintained in order to provide entity authentication. If multiple authentication keys are used (e.g., for different applications or different communication associations or different data), then provision must be made to ensure that each key is only used for the appropriate application, communication association, or data. If the associated protected data is to remain available, and its authenticity is to remain verifiable for an extended period of time, the authentication key must also remain available for that period.

- **Private authentication keys:** Private authentication keys are used with public key algorithms to authenticate users, messages, or communication sessions. Non-repudiation is not necessary for private keys used only for authentication. However, these keys must remain confidential, and the integrity must be protected. If multiple authentication keys are used (e.g., for different applications or different communication associations or different data), then provision must be made to ensure that each key is only used for the appropriate application.

- **Public authentication keys:** Public authentication keys are used with public key algorithms to authenticate users, messages, or communication sessions. The integrity, but not the confidentiality, of these keys must be protected. The association with the public key's owner must be maintained in order to provide entity authentication. If multiple authentication keys are used (e.g., for different applications or different communication associations or different data), then provision must be made to ensure that each key is associated with the appropriate application, communication association, or data. If the associated protected data is to remain available, and its authenticity is to remain detectable for an extended period of time, the authentication key must also remain available for that period.

- **Long term data encryption keys:** These keys are symmetric (secret) keys that are used with symmetric algorithms to protect the confidentiality of data over long periods. Keys used for the encryption of other keys are discussed below. These keys require confidentiality and integrity protection, and must remain available and associated with the encrypted data, communication association, or application as long as the data encrypted under these keys is maintained in its encrypted form.

- **Short term data encryption keys:** These keys are symmetric (secret) keys that are used with symmetric algorithms to protect the confidentiality of data over short periods, such as a communication session or a single message. Keys used for the encryption of other keys are discussed below. These data encryption keys are generated as needed. The confidentiality and integrity of these keys must be maintained until the entire session or message has been decrypted. Once they are no longer needed, they must be securely destroyed.

- **Random Number Generation (RNG) keys:** These keys are symmetric (secret) keys used with a symmetric algorithm to generate pseudorandom numbers. These keys require confidentiality and integrity protection, should be associated with the RNG application, and should be retained until replaced or no longer needed.

- **Master Key encrypting keys used for key wrapping:** Key encrypting keys used for key wrapping are used with symmetric key algorithms. This key encrypting key may encrypt either data encrypting keys or other key encrypting keys. These keys require confidentiality and integrity protection, and may need to remain available (for possible key recovery). These keys may also need to remain associated with the application, the other entity, and the keys they encrypt for the life of any key that is encrypted by the key encrypting key and the data associated with the encrypted keys (because of a possible compromise).

– **Master key used for key derivation:** A ‘master key’ may be used to derive other keying material. These keys require confidentiality and integrity protection, and may need to remain available (for possible key recovery). These keys may also need to remain associated with the application, the other entity, and the keys that are derived for the life of any derived key and the data associated with the derived keys (because of a possible compromise).

– **Keys derived from a master key:** These keys should be protected in accordance with their use, and may need to remain associated with the master key from which they are derived.

– **Key transport private keys:** Key transport private keys are used to decrypt keys that have been encrypted by the associated public key using a public key algorithm. They are usually used to establish multiple keys (e.g., data encrypting keys or MAC keys) and, optionally, other keying material (e.g., initialization vectors). These private keys require confidentiality and integrity protection. They may need to remain available (for possible key recovery), and may need to remain associated with the correct application or usage, and with the keys they decrypt (because of a possible compromise).

– **Key transport public keys:** Key transport public keys are used to encrypt keys using a public key algorithm. They are used to establish keys (e.g., data encrypting keys or MAC keys) and, optionally, other keying material (e.g., initialization vectors). These keys require integrity protection (but not confidentiality protection), and must be correctly associated with the key’s owner. These keys should be validated prior to their use, and should be retained until no longer needed (e.g., the public/private key pair is replaced, or key transport will no longer be required).

– **Secret authorization key:** Secret authorization keys are used to provide access privileges to an entity. The key is known by the access authority and an entity seeking access to resources. The secret authorization key requires confidentiality and integrity protection, and should be correctly associated with the usage and application, and with the entity seeking access.

– **Private authorization key:** Private authorization keys are used to provide access privileges to an entity. The key is known only by an entity seeking access to resources. The private authorization key requires confidentiality and integrity protection, and should be correctly associated with the usage and application.

– **Public authorization key:** Public authorization keys are used to verify access privileges by an entity that knows the associated private key. The public key may be known by anyone. The public authorization key requires integrity protection, and should be correctly associated with the usage and application, and with the entity seeking access.

A3 KEY TYPE CRYPTO PERIODS

NIST (reference [12]) suggests the following cryptoperiod determination strategies for the different key types of a key infrastructure:

a) **Signing key**: The cryptoperiod of a signing key should, in general, be shorter than the cryptoperiod of the corresponding signature verification key.

b) **Signature verification key:** The cryptoperiod of a signature verification key should, in general, be longer than the cryptoperiod of the corresponding signing key so that signed information could be verified at a later time than when it was signed.

c) **Secret authentication key:** The cryptoperiod of a secret authentication key depends on the sensitivity of the type of information it protects. For very sensitive information (e.g., information that one would not like to be compromised [unprotected] if the key used to protect other information were compromised), should have an authentication key that is unique to that protected information. Otherwise, suitable cryptoperiods may extend beyond a single use.

d) **Private authentication key:** A private authentication key would presumably be used multiple times. Its associated public key could be certified, for example, by a Certificate Authority or Attribute Authority. The cryptoperiod of the private authentication key and its associated public key would be the same, e.g., for the cryptoperiod of the certificate. An appropriate cryptoperiod for the key would be one to two years, depending on its use.

e) **Public authentication key:** The cryptoperiod would be the same as the associated private authentication key.

f) **Long term data encryption key:** A long term data encryption key is used multiple times over an extended period of time. An encryption key that is used to encrypt large volumes of information over a short period of time (e.g., for a link encryption) should have a relatively short cryptoperiod (e.g., a day or a week). An encryption key used to encrypt less information could have a longer cryptoperiod.

g) **Short term data encryption key:** The cryptoperiod of a short term data encryption key is very short, e.g., a single message or a communication session.

h) **Key encrypting key used for key wrapping:** A key encrypting key may be used multiple times over an extended period of time. A key of this type that is used to encrypt large numbers of keys over a short period of time should have a relatively short cryptoperiod (e.g., a day or a week). If a small number of keys are encrypted, the cryptoperiod of the key encrypting key could be longer.

i) **Master key used for key derivation:** A master key is used multiple times. Therefore, a suitable cryptoperiod depends on the considerations provided earlier in this section.

j) **Keys derived from a master key:** The cryptoperiod of a key derived from a master key is relatively short, e.g., a single use or a communication session or transaction.

k) **Key transport private key:** A key transport private key would presumably be used multiple times. The cryptoperiod of the key transport private key and its associated public key would be the same, e.g., for the cryptoperiod of the certificate. An appropriate cryptoperiod for the key would be one to two years.

l) **Key transport public key:** The cryptoperiod would be the same as the associated key transport private key.

m) **Secret authorization key:** An authorization key may be used for an extended period of time, depending on the resources that are protected and the role of the entity authorized for access. Suitable cryptoperiods should be less than two years.

Other keying material does not have well established cryptoperiods, per se.

- Domain parameters remain in effect until changed.
- An initialization vector is associated with the information that it helps to protect, and is needed until the information and its protection are no longer needed.
- Shared secrets should be destroyed when no longer needed to derive keying material.
- Seeds should be destroyed immediately after use unless needed for validation (e.g., as one of the elliptic curve domain parameters).