ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 042

November 1995

Source: ETSI TC-NA

Reference: DTR/NA-002601

ICS: 33.040

Key words: STAG, security

Security Technical Advisory Group (STAG); Baseline security standards; Features and mechanisms

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI). This TCR-TR has been endorsed by the 21st TC Chairmens' Co-ordination (TCC 21) meeting, and approved by the 23rd Technical Assembly (TA 23).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilized by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

Introduction

The main purpose of this TCR-TR is to assist ETSI standards groups to define and specify the security functions in their standards. The TCR-TR therefore defines the standard security features for use in ETSI standards and outlines the mechanisms for their implementation. More specifically, guidelines for the proper selection and application of security mechanisms are given.

The NA Security Technical Advisory Group (NA/STAG) by itself does not define nor describe any standards for security services or mechanisms. The purpose of this TCR-TR therefore is rather to list existing standards and to give evaluation criteria for their selection. For further details about the security mechanisms, the source of detailed information and in particular the source of the standard text is indicated. In case such documentation does not exist, a description of the mechanism is given in annex A of this TCR-TR.

The document will be updated as new security requirements or new methods for meeting them are developed.

Blank page

1 Scope

This Technical Committee Reference Technical Report (TCR-TR) lists all security features and mechanisms NA Security Technical Advisory Group (NA/STAG) has evaluated and which may be used in ETSI standards. However, this TCR-TR merely presents guidelines for the selection and application of specific security mechanisms in an annex. If more specific advice is needed, references to relevant sources of information are given. Moreover, the ETSI NA/STAG experts are ready to assist in case of questions and problems.

In many cases, the security mechanisms are not officially standardised themselves, but are registered for use. Many of them are not published because of security considerations, but may be used in specific ETSI-applications.

Since there is considerable activity in the fields of telecommunication and cryptology, this TCR-TR is to be revised and updated regularly.

2 References

2.1 Generic features and mechanisms

[1-1] ITAEGV, doc. M-IT 06 (issue 2.0), September 1994 (contains a comprehensive list of security related standards and ongoing work in the field information security).
[1-2] TCR-TR 028: "Network Aspects (NA); Security Techniques Advisory Group (STAG) Glossary of security terminology".
[1-3] ISO/IEC 7498-2 Security Architecture.
[1-4] ISO/IEC 10181 OSI - Security frameworks in Open Systems - Part1-7.
[1-5] ISO/IEC 9798 Entity authentication mechanisms - Part 1-5 (further parts may follow).
[1-6] ISO/IEC 9160 Data encipherment - Physical layer interoperability requirements.
[1-7] ISO/IEC 8372 Modes of operation for a 64-bit block cipher algorithm.
[1-8] ISO/IEC 10116 Modes of operation for an n-bit block cipher algorithm.
[1-9] ISO/IEC 9797 Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm.
[1-10] ISO/IEC 11770 Key management - Part1-4 (further parts may follow).
[1-11] ISO/IEC 9796 Digital signature scheme giving message recovery.
[1-12] ISO/IEC 10118 Hash-functions - Part 1-4.
[1-13] ISO/IEC 9594-8 The directory - Authentication framework.
[1-14] ISO/IEC 9979 Register of cryptographic algorithms.
[1-15] ISO/IEC 13888 Non-Repudiation - Part 1-3.
[1-16] ETSI TCR-TR NA-002602 STAG Security management techniques.

2.2 Specific system related features and mechanisms

[2-1] ITU-T Recommendation H.234 (Draft H.KEY): Key management and authentication for audiovisual systems.
[2-2] ITU-T Recommendation H.233: Confidentiality system for audiovisual services.
[2-3] ISO/TC68 Draft: Banking and related financial services; Catalogue of security related standards.
[2-4] ETSI/TC GSM 02.09: GSM Security aspects.
[2-5] ETSI/TC GSM 03.20: GSM Security related network functions.
[2-6] ETSI/TC GSM 12.03: GSM Security management.
[2-7] ETSI DECT BC-T-176: DECT security features.
[2-8] ETSI/RES6 RES60220: TETRA security aspects.

3 Definitions and abbreviations

For the purpose of this TCR-TR, the following definitions and abbreviations apply.

3.1 Definitions

Security service

A service provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers [1-2], [1-3].

Security mechanism

The logic or algorithm that implements a particular security function in hardware and software [1-2].

3.2 Abbreviations

TTP Trusted Third Party: 'A security authority, or its agent, trusted by other entities with respect to security related activities. In particular, a trusted third party is trusted by a claimant and/or a verifier for the purposes of authentication', [1-2].

In general, for abbreviations see [1-2].

4 Security features

4.1 Introduction

Security features reflect the top level means in the protection against potential security threats. This section outlines the security features which may be used within ETSI standards. It is closely related to the corresponding parts from the security architecture of ISO [1-3], where security features are referred to as security services.

The security mechanisms, which are understood as the building blocks of the security features, are described in the next section. Table B.1 looks upon the relationship between the security features and mechanisms, i.e. it indicates which mechanisms implement a specific security feature.

4.2 Overview of security features

The following gives a list of security features which may be used within ETSI standards. Statements in italics are taken from [1-2].

4.2.1 Authentication

Authentication may provide for authentication of the communicating parties and/or the source of data. Accordingly, two different authentication features can be distinguished:

- peer entity authentication: *the corroboration that a peer entity in an association is the one claimed;*

- data origin authentication*: the corroboration that the source of data received is as claimed.*

4.2.2 Confidentiality

Data confidentiality provides *that information is not made available or disclosed to unauthorised individuals, entities or processes.*

4.2.3 Integrity

Data integrity provides for *the property that data has not been altered or destroyed in an unauthorised manner.*

4.2.4 Access control

Access control provides for *the prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.*

4.2.5 Key management

Key management provides for *the generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.*

4.2.6 Non-Repudiation

Non-repudiation provides for a *proof of the sending or delivery of data by communicating IT assemblies which prevents subsequent false denials by a user of transmission or receipt, respectively, of such data or its contents.*

4.2.7 Security management

This topic is the subject of a dedicated document: [1-16].

5 Security mechanisms

5.1 Introduction

According to [1-2] a security mechanism is *the logic or algorithm that implements a particular security function in hardware and software*.

By security mechanism we understand methods to achieve certain security features. It may thus be seen as an intermediate building block of a security feature. In general, there will be different variants to implement such a specific mechanism (e.g. block ciphers, stream ciphers for encryption).

5.2 Overview of security mechanisms

Subsequently a list of security mechanisms is given which may be used within ETSI standards. The way individual security mechanisms are subdivided, e.g. authentication, follows whenever possible the structure of the relevant standards. Other classifications according to different criteria are certainly possible.

The distinguishing features listed for the individual mechanisms give some more detailed information which is considered to be relevant for a specific instance of the mechanism.

5.2.1 Authentication/Identification mechanisms

Biometrical methods:

Knowledge based methods:

Password/PIN;

One-time password.

distinguishing features:

- Password/PIN is encrypted/not encrypted for transmission.

Proof of knowledge based methods (Challenge-response):

- Secret Key based;
- Public Key based:
    - Certificate-based;
    - Identity-based;
    - Zero-knowledge.

distinguishing features:

- 1-2-3 path mechanism;
- with unilateral/mutual authentication;
- explicit/implicit authentication;
- with/without involvement of a trusted third party.

5.2.2 Confidentiality mechanisms

Encryption

- Secret Key based:
    - Stream Cipher;
    - Block Cipher.
- Public Key based.

distinguishing features:

- different modes for block ciphers: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB);
- with/without need for synchronisation;
- with/without error propagation;
- with/without extension of message length.

5.2.3 Integrity mechanisms

Hash function (message digest):

Secret Key based:

- Keyed Hash Function (cryptographic check value, message authentication code: MAC).

Public Key based:

- Digital Signature.

distinguishing features:

- digital signature with/without message recovery;
- probabilistic/deterministic signature schemes;
- signature scheme with/ without pre-computation;
- certificate/ID-based signature schemes.

5.2.4 Access Control mechanisms

- Control list based schemes;
- Capability based schemes;
- Label based schemes;
- Context based schemes.

5.2.5 Key Management mechanisms

Establishment of a shared secret key:

- Secret Key based;
- Public Key based.

distinguishing features:

- key agreement/key transport/key translation;
- 1-2-3 path mechanism;
- with/without key confirmation;
- with/without forward secrecy;
- with/without involvement of a trusted third party;
- with/without authentication.

Distribution of a public key

5.2.6 Non-Repudiation mechanisms

The current status of the relevant documents on non-repudiation mechanisms [1-15] is such, that a detailed description of the mechanisms seems premature.

5.3 Format of description

Each of the mechanisms is described with respect to the following criteria:

Overview	Gives a short description of the principles and functionality of the mechanism. For more details, the reader is referred to the documents indicated at the end of each description.
used for	Describes the (main) application areas of the mechanism.
management characteristics	Describes the security management functions necessary for the use of the mechanism (key management etc.)
limitations	Lists the limits and constraints of the mechanism in terms of - technical limitations - commercial limitations (patents, licensing, etc.) - legal limitations/constraints
implementation characteristics	Describes advantages/disadvantages of (existing/future) implementations of the mechanism in terms of complexity, power requirements, electrical environment etc.
further documentation	Lists the original documentation about the mechanism as far as publicly available.

Annex A: Description of mechanisms

Security mechanisms / Authentication/identification

Biometrical methods

Overview	Measurement of biological properties (fingerprint, eye retina, voice etc.) of the person to be authenticated.
Used for	Authentication of persons.
Management	All biometrical methods rely on the comparison between the actual and a stored pattern. The stored pattern must be accessible either from a database, or the person must carry it along with him/her (e.g. on a chip card).
Limitations	Technical: Generally fairly high cost for the measuring and processing equipment. Legal/commercial: None so far. Social: Reluctance of people against eye measurement for fear of eye damage.
Implementation	Hardware: Software:

Documentation

1) Benjamin Miller: Vital signs of identity. IEEE Spectrum 2(1994), p. 22 - 30. (Good overview of state of the art).

Security mechanisms / Authentication/identification / Knowledge based methods

Authentication with Passwords or Personal Identification Numbers (PIN)

Overview	User is authenticated by entry of password (or a number in the case of a PIN), which is transmitted and/or stored either in encrypted or plain form. Encrypted transmission/storage cannot be tapped and hence is more secure than plain text, but also more expensive.
Used for	Authentication of persons.
Management	Initial password/PIN entry is a critical phase to be managed between system operator and user using a first password/PIN being known to both. Password/PIN change must be possible and may even be enforced. Easily guessed passwords/PINs must be rejected automatically.
Limitations	Technical: Generally very low cost for equipment and software. Legal/commercial: None so far. Social: Passwords/PINs should not be written down, but should neither be easily guessed: Dilemma which frequently leads to rejection.
Implementation	Hardware: Keyboard (numerical or alphanumeric) and storage medium or transmission link needed. Software: If password is not encrypted, only centralised software necessary.

Documentation

1) ISO/IEC 9564/IS *Banking - Personal Identification Number Management and Security.*
2) FIPS PUB 112 National Institute of Standards and Technology. *FIPS PUB 112: Password usage.*

Security mechanisms / Authentication/identification / Knowledge based methods

One-time Passwords

Overview	One-time passwords avoid the necessity of password encryption, since they are used exactly once and never again to avoid replay attacks. Frequently these are used in conjunction with normal passwords and mostly for authentication over unprotected transmission channels.
Used for	Authentication of persons.
Management	One-time passwords are distributed by a trusted entity in the form of lists. This distribution needs extra security measures.
Limitations	Technical: Generally very low cost for equipment and software. Legal/commercial: None so far. Social: None, apart from being relatively tedious.
Implementation	Hardware: Keyboard (numerical or alphanumeric) and storage medium or transmission link needed. Software: Since password is not encrypted, only centralised software necessary.

Documentation

Security mechanisms / Authentication/identification / Proof of knowledge based methods

Secret key based

Overview	Proof of knowledge based methods do not authenticate the user, but an intelligent device he is using. One-pass authentication: The basic principle is to use the secret key as input for a transformation (e.g. one-way function, encryption) of one/several time variant parameters such as a time stamp, sequence number or random number. Multi-pass authentication: The basic principle is to send a random pattern to the intelligent device which transforms it into another pattern according to a rule known to both sides, and transfers it back to the originator: challenge-response.
Used for	Authentication of persons and/or devices (e.g. mobile telecommunication equipment) over unsecured channels, where eavesdropping/intrusion is a concern.
Management	There must be an initial communication between challenging and responding device to initialise the rule for transformation. The secret authentication data is held by the claimant as well as by verifier and has to be kept strictly confidential. Disclosure of authentication data requires its replacement.
Limitations	Technical: Claimant and verifier must have considerable processing power and storage capacity. Legal/commercial: None so far. Standards in negotiation. Social: None so far, except for multitude of (credit-like) cards.
Implementation	Hardware: Chip card, chip card reader and transmission link needed. Software: (Standardised) software on both sides. Depending of the particular implementation a common trusted time reference is required and/or a (true) random source to provide for challenge patterns. If sequence numbers are used both claimant and verifier need to maintain records of used/valid sequence numbers. Special procedures are needed to reset/restart counters after system failures.

Documentation

1) ISO/IEC 9798-1/IS Entity authentication mechanisms - Part 1: *General Model.*
2) ISO/IEC 9798-2/IS Entity authentication mechanisms - Part 2: *Entity authentication using symmetric Techniques.*
3) ISO/IEC 9798-4/DIS Entity authentication mechanisms - Part 4: *Entity authentication using a cryptographic check function.*
4) ISO/IEC 9594-8/IS The Directory - Part 8: *Authentication framework.* (CCITT Recommendation X.509).
5) ETSI/TC GSM Recommendation GSM 03.20: *GSM Security related network functions.*

Security mechanisms / Authentication/identification / Proof of knowledge based methods

Public key based / Certificate-based

Overview	Proof of knowledge based methods do not authenticate the user, but an intelligent device he is using. One-pass authentication: The basic principle is to use the secret key as input for a transformation (e.g. one-way function, encryption) of one/several time variant parameters such as a time stamp, sequence number or random number. Multi-pass authentication: The basic principle is to send a random pattern to the intelligent device which transforms it into another pattern according to a rule known to both sides, and transfers it back to the originator: challenge-response.
Used for	Authentication of persons and/or devices (e.g. mobile telecommunication equipment) over unsecured channels, where eavesdropping/intrusion is a concern.
Management	The verifier must have access to or be in possession of a valid public key of the claimant. The secret authentication data, private key, is held only by the claimant and has to be kept strictly confidential. The public key need not be kept confidential. However, the authenticity of the public key has to be guaranteed by a certificate signed by a trusted party. Disclosure of secret used by the trusted party to sign certificates requires replacement of certificates. Disclosure of secret authentication data requires its replacement and/or revocation of the certificate.
Limitations	Technical: Claimant and verifier must have considerable processing power and storage capacity. The requirements are much harder than for comparable secret key based methods. Legal/commercial: Many public key techniques are patented. The stringent technical constraints (in particular on smart cards) have so far prevented the use of public key techniques on a wide scale. However, the situation is changing. Social: None so far, except for multitude of (credit-like) cards.
Implementation	Hardware: Chip card, chip card reader and transmission link needed. Software: (Standardised) software on both sides. Depending of the particular implementation a common trusted time reference is required and/or a (true) random source to provide for challenge patterns. If sequence numbers are used both claimant and verifier need to maintain records of used/valid sequence numbers. Special procedures are needed to reset/restart counters after system failures.

Documentation

1) ISO/IEC 9798-1/IS Entity authentication mechanisms - Part 1: *General Model.*
2) ISO/IEC 9798-3/IS Entity authentication mechanisms-Part 3: *Entity authentication using asymmetric Techniques.*
3) ISO/IEC 9594-8/IS The Directory - Part 8: *Authentication framework.* (CCITT Recommendation X.509).

Security mechanisms / Authentication/identification / Proof of knowledge based methods

Public key based / Identity-based

Overview	Proof of knowledge based methods do not authenticate the user, but an intelligent device he is using. One-pass authentication: The basic principle is to use the secret key as input for a transformation (e.g. one-way function, encryption) of one/several time variant parameters such as a time stamp, sequence number or random number. Multi-pass authentication: The basic principle is to send a random pattern to the intelligent device which transforms it into another pattern according to a rule known to both sides, and transfers it back to the originator: challenge-response.
Used for	Authentication of persons and/or devices (e.g. mobile telecommunication equipment) over unsecured channels, where eavesdropping/intrusion is a concern.
Management	The secret authentication data, private key, is held only by the claimant and has to be kept strictly confidential. The public key need not be kept confidential. The public key may be recovered from the identity of the claimant alone or together with an additional parameter. No certificates are needed to guarantee for the authenticity of the public key. Disclosure of secret used by the trusted party to link identifier and public key in a non-forgeable way , requires replacement of all private keys based on this secret. Disclosure of secret authentication data requires its replacement.
Limitations	Technical: Claimant and verifier must have considerable processing power and storage capacity. The requirements are much harder than for comparable secret key based methods. Legal/commercial: Many public key techniques are patented. The stringent technical constraints (in particular on smart cards) have so far prevented the use of public key techniques on a wide scale. However, the situation is changing. Social: None so far, except for multitude of (credit-like) cards.
Implementation	Hardware: Chip card, chip card reader and transmission link needed. Software: (Standardised) software on both sides. Depending of the particular implementation a common trusted time reference is required and/or a (true) random source to provide for challenge patterns. If sequence numbers are used both claimant and verifier need to maintain records of used/valid sequence numbers. Special procedures are needed to reset/restart counters after system failures.

Documentation

1) ISO/IEC 9798-1/IS Entity authentication mechanisms - Part 1: *General Model.*
2) ISO/IEC 9798-3/IS Entity authentication mechanisms-Part 3: *Entity authentication using asymmetric Techniques.*
3) ISO/IEC 9594-8/IS The Directory - Part 8: *Authentication framework.* (CCITT Recommendation X.509).

Security mechanisms / Authentication/identification / Proof of knowledge based methods

Public key based / Zero-knowledge

Overview	Proof of knowledge based methods do not authenticate the user, but an intelligent device he is using. Zero-knowledge methods guarantee that the verifier in an authentication protocol run gains no bit of information he did not already have before the run (he cannot abuse the claimant as an oracle). In general a zero-knowledge authentication protocol consists of three passes: - claimant sends commitment. - verifier sends challenge. - claimant sends response. Other variants are possible.
Used for	Authentication of persons and/or devices (e.g. mobile telecommunication equipment) over unsecured channels, where eavesdropping/intrusion is a concern. Especially well suited for situations where authentication is required but no secret key exchanged.
Management	The verifier must have available a valid public key of the claimant. The secret authentication data, private key, is held only by the claimant and has to be kept strictly confidential. The public key need not be kept confidential. Both, certificate and identity-based mechanisms exist (see above).
Limitations	Technical: Claimant and verifier must have considerable processing power and storage capacity. The requirements are much harder than for comparable secret key based methods. Legal/commercial: Most zero-knowledge techniques are covered by patents. The technical constraints are less stringent than for other public key methods. Smart card implementations exist. Social: None so far, except for multitude of (credit-like) cards.
Implementation	Hardware: Chip card, chip card reader and transmission link needed. Software: (Standardised) software on both sides. A (true) random source to provide for the commitment and the challenge patterns is required.

Documentation

1) ISO/IEC 9798-1/IS Entity authentication mechanisms - Part 1: *General Model.*
2) ISO/IEC 9798-5/WD Entity authentication mechanisms-Part 5: *Entity authentication using zero-knowledge protocols.*

Security mechanisms / Confidentiality / Encryption

Secret key based / Stream Ciphers

Overview	Symmetric encryption method based on a single secret key, operating on a one-bit level. Synchronous stream ciphers require perfect time synchronisation between sender and receiver but show no error propagation. Self-synchronising stream ciphers require no synchronisation but show error propagation.
Used for	Encryption of all kind of data, in particular for contiguous files or messages and for (digital) speech encryption.
Management	As both the encryption and the decryption party need the same secret key, this key must be transmitted beforehand using either symmetric or asymmetric encryption methods, or by another medium deemed secure (courier etc.).
Limitations	Technical: Generally low processing power required, very high throughput reachable (> 1 Gbit/s). Legal/commercial: There are numerous algorithms in use today, most of them proprietary or secret, some of them public.
Implementation	Hardware: Chips available either as dedicated hardware (1 Mbit/s up to > 1 Gbit/s) or single-chip processors. Software: >100 kbit/s on current general purpose processors, up to 1 Mbit/s on signal processors. Stream ciphers may be based on block ciphers run in OFB- or CFB-mode.

Documentation

1) ISO/IEC 9979 Register of cryptographic algorithms.
2) ISO/IEC 8372/IS Modes of operation for a 64-bit block cipher algorithm.
3) ISO/IEC 10116/IS Modes of operation for an n-bit block cipher algorithm.

Security mechanisms / Confidentiality / Encryption

Secret key based / Block Ciphers

Overview	Symmetric encryption method based on a single secret key, operating on n-bit blocks. Different modes of operation: Electronic Codebook Mode, Cipher Block Chaining Mode, Cipher Feedback Mode or Output Feedback Mode.
Used for	Encryption of all kind of data. Caution has to be taken as soon as the data to be encrypted has fairly regular or repetitive structure (only in ECB mode).
Management	As both the encryption and the decryption party need the same secret key, this key must be transmitted beforehand using either symmetric or asymmetric encryption methods, or by another medium deemed secure (courier etc.).
Limitations	Technical: Generally low processing power required, high throughput reachable. Depending of the chosen mode error propagation may be of concern. Loss of block borders (e.g. bit slip) requires re-synchronisation. For certain modes padding may be necessary. Legal/commercial: There are numerous algorithms in use today, most of them proprietary or secret, some of them public (DES, IDEA, FEAL).
Implementation	Hardware: Chips available either as dedicated hardware (1 Mbit/s up to 1 Gbit/s) or single-chip processors. Software: >100 kbit/s on current general purpose processors, up to 1 Mbit/s on signal processors.

Documentation

1) ISO/IEC 9979 Register of cryptographic algorithms.
2) ISO/IEC 8372/IS Modes of operation for a 64-bit block cipher algorithm.
3) ISO/IEC 10116/IS Modes of operation for an n-bit block cipher algorithm.
4) FIPS PUB 46 National Bureau of Standards: *Data Encryption Standard.*

Security mechanisms / Confidentiality / Encryption

Public key based

Overview	Asymmetric encryption methods are based on a pair (public/secret) of keys. The public key of an entity A can be used to encrypt messages intended for A. In contrast to symmetric encryption systems, the use of the secret key does not provide for confidentiality.
Used for	Encryption of small messages, mostly for key exchange.
Management	Public key encryption requires in general a set of publicly known security parameters and a set of secret security parameters. Examples: RSA [1]. ElGamal [2].
Limitations	Technical: Requires much computing power. Legal/commercial: Nearly all known algorithms are patented by PKP in US, partially even world-wide.
Implementation	Hardware: Today up to few 100 kbit/s, with key length of 512 bits. Software: 1 kbit/s on current general purpose processors, up to few 10 kbit/s on signal processors.

Documentation

1) PKCS#1 RSA Data Security Inc., *PKCS#1: RSA Encryption Standard*, Version 1.4, June 1991.

2) ElGamal T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. on Inf. Theory*, 31, 1985.

3) Elliptic Curves A. Menezes, "Elliptic Curve Public Key Cryptosystems", *Kluwer Academic Publishers*, 1993.

Security mechanisms / Integrity

Hash function (message digest)

Overview	Requirements for a strong hash function: - one-way function mapping an arbitrary message on a message of a fixed length (e.g. 128 bits); - collision-resistant; - calculation does not require any secret information and can be done very efficiently.
Used for	Protection of integrity. Building block for digital signatures.
Management	The application of a hash function requires in general the knowledge of the padding rules used and possibly a initializing value.
Limitations	Technical: Generally low processing power and storage capacity required. Legal/commercial: Few known hash functions are patented.
Implementation	Hardware: Today up to 100 Mbit/s. Software: Up to 10 Mbit/s on current general purpose processors. Implementations on smart cards available.

Documentation

1) ISO/IEC 10118-1/IS Hash-functions - Part 1 : *General.*
2) ISO/IEC 10118-2/IS Hash-functions - Part 2 : *Hash functions using an n-bit block cipher algorithm.*
3) ISO/IEC 10118-3/WD Hash-functions - Part 3 : *Dedicated Hash Functions.*
4) ISO/IEC 10118-4/WD Hash-functions - Part 4 : *Hash functions using modular arithmetic.*
5) FIPS PUB 180 *Secure Hash Standard.*

Security mechanisms / Integrity

Secret key based / Keyed hash function (message authentication code: MAC)

Overview	Based on a secret key known to both the sending and receiving entity. Requirements: - maps an arbitrary message on a message of a fixed length (e.g. 32, 64 bits); - calculation very efficient; - MAC of a message not computable without knowledge of the secret key. In general a MAC is not suitable to be used as digital signature. Block ciphers running in CBC- or CFB-mode may be used as keyed hash functions.
Used for	Protection of integrity and authenticity. Building block for authentication mechanisms.
Management	As both the sending and the receiving party need the same secret key, this key must be transmitted beforehand using either symmetric or asymmetric encryption methods, or by another medium deemed secure (courier etc.).
Limitations	Technical: Generally low processing power required, high throughput reachable. Legal/commercial: Numerous block cipher algorithms in use today. Most of them proprietary or secret, some of them public.
Implementation	Hardware: Chips available either as dedicated hardware (1 Mbit/s up to 1 Gbit/s) or single-chip processors. Software: >100 kbit/s on current general purpose processors, up to 1 Mbit/s on signal processors.

Documentation

1) ISO/IEC 9797/IS *Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm.*
2) ISO/IEC 9979 Register of cryptographic algorithms.
3) ISO/IEC 8372/IS Modes of operation for a 64-bit block cipher algorithm.
4) ISO/IEC 10116/IS Modes of operation for an n-bit block cipher algorithm.

Security mechanisms / Integrity

Public key based / Digital signature

Overview	Two main classes of digital signature schemes may be distinguished: 1 schemes with message recovery: - signature (or part of it) and message to be signed are identical; 2 schemes without message recovery: - signature has to be appended to the message. Performance figures for generation/verification vary considerably for different signature schemes.
Used for	Protection of integrity and authenticity. Building block for authentication schemes. Building block for non-repudiation mechanisms.
Management	The verifier must have available a valid public key of the claimant for the verification of the signature. The secret key to carry out the signature transformation, is hold only by the claimant and has to be kept strictly confidential. The public key need not be kept confidential. However, depending of the chosen cryptosystem, the authenticity of the public key has to be guaranteed by a certificate signed by a trusted party. Disclosure of secret used by the trusted party to sign certificates requires replacement of certificates. Disclosure of secret authentication data requires its replacement and/or revocation of the certificate.
Limitations	Technical: Claimant and verifier must have considerable processing power and storage capacity. Legal/commercial: Many public key techniques are patented. The stringent technical constraints (in particular on smart cards) have so far prevented the use of public key techniques on a wide scale. However, the situation is changing.
Implementation	Hardware: Chip card, chip card reader needed. Software: (Standardised) software on both sides. Depending of the particular implementation a (true) random source is required.

Documentation

1) ISO/IEC 9796/IS *Digital signature scheme giving message recovery.*
2) ISO/IEC /WD Digital signature with appendix - Part 1 : *General. Model.*
3) ISO/IEC /WD Digital signature with appendix - Part 2 : *Identity-based mechanisms.*
4) ISO/IEC /WD Digital signature with appendix - Part 3 : *Certificate-based mechanisms.*
5) FIPS Pub *Digital Signature Standard.*

Security mechanisms / Access control

Control list based schemes

Overview	The initiator requesting access has an identity which is provided to the access control decision function (which makes the decision to grant or deny the requested access). The targets (to which access is requested) are characterised with a set of pairs (initiator identity, allowed/denied operation type). Based on this information and an appropriate access control policy, the access control decision function grants or denies the requested access. The identity of the initiator can be an individual, group or role identity. Different variations of this basic scheme are possible, e.g. including context information, or handling groups of targets instead of individual targets.
Used for	Access of an initiator to a target. This scheme is appropriate, when there are few initiators or groups of initiators.
Management	Management of the information can be handled more easily on a per-target basis than on a per-initiator basis, e.g. access rights to a target or group of targets can be revoked easily, but revocation of access rights of an individual or a group of individuals is more complex. Therefore, the scheme is not appropriate when the population of individuals or groups of individuals changes frequently. However, dynamic changes in the population of the targets can be handled easily.
Limitations	Technical: none Legal/commercial: The information on the access rights is stored somewhere near the targets, especially not at the side of the initiators. This means, that in the case of human initiators, the respective laws concerning the use and storage of human user related information have to be respected. Social: none
Implementation	Hardware: Software:

Documentation

1) ISO/IEC 10181-3/CD OSI - Security frameworks in Open Systems - Part 3 : *Access Control.*

Security mechanisms / Access control

Capability based schemes

Overview	The initiator requesting access provides the access control decision function (which makes the decision to grant or deny the requested access) with a list of allowed operations on an identified set of targets (this list is called a capability). This information has usually to be signed by an appropriate authority. A variation of this basic scheme is the use of a capability without specified operations, allowing all kind of access to the initiator, if access is granted at all. In another variant, the authority issuing the capability is only allowed to grant limited access rights. It then also has to be checked, if these limits are not exceeded.
Used for	Access of an initiator to a target. This scheme is appropriate, when there are few targets or groups of targets and many users or groups of users, being in different domains.
Management	Management of the information can be handled more easy on a per-initiator basis than on a per-target basis, e.g. access rights of a individual or a group of individuals can be revoked easily, but revocation of access rights to a target or a group of targets is more complex. Therefore, the scheme is not appropriate when the population of targets or groups of targets changes frequently. However, dynamic changes in the population of the initiators can be handled easily.
Limitations	Technical: none. Legal/commercial: The information on the access rights is stored at the side of the initiators. Therefore, in the case of human initiators, they have more control over the use of these data than in the case of the control list scheme. Social: none.
Implementation	Hardware: Capabilities of human users are usually stored on. Software:

Documentation

1) ISO/IEC 10181-3/CD OSI - Security frameworks in Open Systems - Part 3 : *Access Control.*

Security mechanisms / Access control

Label based schemes

Overview	Security labels can be assigned to initiators and targets and to data which pass between systems. Control of data flow within one security domain can be achieved. Also, this scheme can be used to provide access control between domains. The allowed operations are not explicitly bound to the initiator or the target, but are instead defined as part of the access control policy. If the initiator is a human user, the label bound to him/her is often called a clearance, and the label bound to the target is called classification.
Used for	Access of an initiator to a target. This scheme is appropriate, when there are many users accessing many targets, and only a coarse granularity of access control is required.
Management	The following mechanisms can be used for the input to the access control decision function (which makes the decision to grant or deny the requested access) to derive the clearance of the initiator: - use of access control certificates or tokens (giving the clearance of the initiator), - use of authentication and look up (the clearance of the initiator is looked up with the help of an authenticated initiator identity); - use of a labelled channel (the clearance of the initiator is implied from the used channel); - use of labelled data (the clearance of the initiator is implied from the security labels of the operands of the access request).
Limitations	Technical: none. Legal/commercial: none. Social: none.
Implementation	Hardware: Software:

Documentation

1) ISO/IEC 10181-3/CD OSI - Security frameworks in Open Systems - Part 3 : *Access Control.*

Security mechanisms / Access control

Context based schemes

Overview	Contextual information (e.g. time, location) is used for access control. This scheme can be used together with other schemes or as an independent scheme. For the access control, context control lists are used. In a context control list, the contextual conditions (e.g. time, route) are given together with the allowed operations. The contextual information itself (valid for a specific access request) is obtained from the context where the access request is performed. A variant is a scheme where the first qualifying entry in the context control list determines the search.
Used for	Access of an initiator to a target. This scheme can be used to enforce rules that apply to all initiators.
Management	
Limitations	Technical: none. Legal/commercial: none. Social: none.
Implementation	Hardware: Software:

Documentation
1) ISO/IEC 10181-3/CD OSI - Security frameworks in Open Systems - Part 3 : *Access Control.*

Security mechanisms / Key management / Establishment of a shared secret key

Secret key based

Overview	Two basic mechanisms for the establishment of a shared secret key between two entities may be distinguished: 1) without key centre: - entities share a common secret key beforehand. Depending on whether one of the communicating parties controls the key or not key agreement and key transport mechanisms may be discerned; 2) with key centre: - each entity shares a common secret key with the key centre but not among themselves. Key centre acts as trusted third party to either generate keying material or translate keying material sent by one of the entities.
Used for	Secret key may be used to provide for: - subsequent confidential communication; - integrity an authenticity of subsequently exchanged messages.
Management	The cryptographic keys used subsequently to establish shared secret keys usually progress through a series of states referred to as key life cycle. This transitions between the different stages require specific management actions [1].
Limitations	Secret key based cryptosystems will always require a mutual trust between the entities sharing a common secret key. This precondition may limit the functionality of the cryptosystem (e.g. digital signature).
Implementation	

Documentation
1) ISO/IEC 11770-1/CD Key Management - Part 1 : *Framework.*
2) ISO/IEC 11770-2/CD Key Management - Part 2 : *Mechanisms using symmetric techniques.*
3) ISO/IEC 11568-3/IS Banking - Key Management (Retail) - Part 3 : *Key management techniques for symmetric ciphers.*

Security mechanisms / Key management / Establishment of a shared secret key

Public key based

Overview	Establishment of a shared secret key between two entities may be achieved by: 1) key agreement: - the secret key is the result of the execution of a protocol between the two entities, neither of them can predetermine its value; 2) key transport: - the secret key is chosen by one entity and transferred to the other entity protected by asymmetric techniques.
Used for	Secret key may be used to provide for: - subsequent confidential communication; - integrity an authenticity of subsequently exchanged messages.
Management	The cryptographic keys used subsequently to establish shared secret keys usually progress through a series of states referred to as key life cycle. This transitions between the different stages require specific management actions [1].
Limitations	With public key based cryptosystems each secret keys is held by only one entity and need not be shared with any other entity. The counterpart of the secret key is the so-called public key of which only an authentic copy need be made available to parties wishing to communicate.
Implementation	

Documentation

1) ISO/IEC 11770-1/CD Key Management - Part 1 : *Framework.*
2) ISO/IEC 11770-3/CD Key Management - Part 3 : *Mechanisms using asymmetric techniques.*
3) ISO/IEC 11568-3/IS Banking - Key Management (Retail) - Part 4 : *Key management techniques using public key cryptography.*

Security mechanisms / Key management / Distribution of public keys

Overview	Distribution of authentic public keys over an insecure channel can be achieved by making use of certificates. Two basic distribution mechanisms can be distinguished: - without a trusted third party; - involving a trusted third party (e.g. certification authority).
Used for	Distribution of authentic public keys is a basic requirement for many applications and allows the subsequent use of these keys for purposes such as authentication, establishment of a shared secret key, etc.
Management	The use of certificates requires the availability of an authentic copy of the public key of the certification authority. The distribution of this public key requires an authenticated channel. Certificates usually progress through a series of states referred to as certificate life cycle. The transitions between the different stages require specific management actions [2,3].
Limitations	The use of certificates to provide for authenticity of public keys assumes that the entity issuing the certificates is trusted by all parties.
Implementation	

Documentation

1) ISO/IEC 11770-1/CD Key Management - Part 1 : *Framework.*
2) ISO/IEC 11770-3/CD Key Management - Part 3 : *Mechanisms using asymmetric techniques.*
3) ISO/IEC 9594-8/IS The Directory - Part 8: *Authentication framework.* (CCITT Recommendation X.509).

Annex B: The relationship of security features and mechanisms

In [1-3] a table showing the mapping of security features on security mechanisms is given. The security features considered there are more refined (e.g. four different confidentiality services) than the ones considered in the present document. We do not exactly follow this approach here, but instead base the mapping on the features described in chapter 4. of this document. This is more in line with currently available documents on security frameworks and security mechanisms.

It should also be mentioned that some of the security mechanisms mentioned in [1-3], e.g. Traffic Padding and Routing Control, are not considered here.

Table B.1: Mapping of security features on security mechanisms

Mechanisms / features	Authentication	Encryption	Access control	Integrity	Non-repudiation	Key management
Authentication	Y	Y				
Confidentiality		Y				
Access control			Y			
Integrity	Y	Y		Y		
Non-repudiation	Y			Y	Y	
Key management		Y				Y

NOTE 1: Security audit is not included in the above table, since no single specific security mechanism can be used to provide this feature. Audit mechanisms may be characterised as procedures based on a number of management and operational approaches, cf. [1-4, part 7].

NOTE 2: Security management is the subject of a dedicated document: ETSI TCR-TR 02602.

History

Document history			
May 1995	Draft for endorsement by	TCC 20	1995-05-29 to 1995-05-31
September 1995	Final draft for approval by	TA 23	1995-11-07 to 1995-11-09
November 1995	First Edition		