ETSI TS 102 224 V11.0.0 (2018-09)

Smart Cards;
Security mechanisms for UICC based Applications
Functional requirements
(Release 11)

Reference
RTS/SCP-R0282v1100

Keywords
security, smart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

It is based on work originally done in the 3GPP in TSG-terminals WG3 and ETSI SMG.

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x: the first digit:

0 early working draft;

1 presented to TC SCP for information;

2 presented to TC SCP for approval;

3 or greater indicates TC SCP approved document under change control.

y: the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z: the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides standardized security mechanisms in conjunction with the Card Application Toolkit for the interface between a Network Entity and a UICC.

The security mechanisms which are specified are independent of applications.

The present document describes the functional requirements of the security mechanisms with the implementation detail of these mechanisms being described in ETSI TS 102 225 [2].

Within the scope of the present document, the UICC refers here to an ICC which support at least one application in order to access a cellular network.

The ICC is considered as a platform, which is based on ETSI TS 102 221 [5].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

- In the case of a reference to a TC SCP document, a non specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

[2] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[3] ETSI TS 131 111: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Universal Subscriber Identity Module Application Toolkit (USAT) (3GPP TS 31.111)".

[4] Void.

[5] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

[6] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".

[7] ETSI TS 102 127: "Smart cards; Transport protocol for CAT applications; Stage 2".

[8] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[9] ETSI TS 102 412: "Smart Card; Smart Card Platform Requirements Stage 1".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

[i.1] ETSI ETR 330: "Security Techniques Advisory Group (STAG); A guide to legislative and regulatory environment".

3 Definitions and abbreviations

3.1 Definitions

For the purpose of the present document, the following terms and definitions apply:

application layer: layer above the transport layer on which the application messages are exchanged between the sending and receiving applications

application message: package of commands or data sent from the sending application to the receiving application, or vice versa, independently of the transport mechanism

NOTE: An application message is transformed with respect to a chosen transport layer and chosen level of security into one or more secured packets.

counter: mechanism or data field used for keeping track of a message sequence

NOTE: This could be realized as a sequence oriented or time stamp derived value maintaining a level of synchronization.

cryptographic checksum: string of bits derived from some secret information, (e.g. a secret key), part or all of the application message, and possible further information (e.g. part of the security header)

NOTE: The secret key is known to the sending entity and to the receiving entity. The Cryptographic checksum is often referred to as Message Authentication Code (MAC).

digital signature: string of bits derived from some secret information (e.g. a secret key) the complete application message, and possible further information (e.g. part of the security header)

NOTE: The secret information is known only to the sending entity. Although the authenticity of the digital signature can be proved by the receiving entity, the receiving entity is not able to reproduce the digital signature without knowledge of the secret information owned by the sending entity.

receiving application: entity to which the application message is destined

receiving entity: entity where the secured packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated toolkit server) and where the security mechanisms are utilized

NOTE: The receiving entity processes the secured packets.

redundancy check: string of bits derived from the application message and possible further information for the purpose of detecting accidental changes to the message, without the use of any secret information

secured packet: information flow on top of which the level of required security has been applied

NOTE: An application message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

security header: that part of the secured packet which consists of all security information

EXAMPLE: Counter, key identification, indication of security level, checksum or digital signature).

sender identification: simple verification of the identity of the sending entity by the receiving entity comparing the sender identity with an a priori stored identity of the sender at the receiving entity

sending application: entity generating an application message to be sent

sending entity: entity from which the secured packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated toolkit server) and where the security mechanisms are invoked

NOTE: The sending entity generates the secured packets to be sent.

status code: indication that a message has been received (correctly or incorrectly, indicating reason for failure)

transport layer: layer responsible for transporting secured packets through the network

NOTE: The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

unsecured acknowledgement: status code included in a response message

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 121 905 [1] and the following apply:

CAT	Card Application Toolkit
CAT_TP	Card Application Toolkit Transport Protocol

4 Introduction

The Card Application Toolkit (CAT) as described in ETSI TS 102 223 [6] is a set of applications and related procedures that may be used during a card session. It allows operators to create specific applications resident on the UICC. There exists a need to secure Card Application Toolkit (CAT) related communication over the network, (e.g. SMS, USSD, and future transport mechanisms) with the level of security chosen by the network operator or the application provider.

It is assumed in the present document that the sending and receiving entities are in a secure environment.

The appropriate security mechanisms are described in the present document.

The security mechanisms cover the following security requirements:

- unilateral authentication from network to UICC;
- unilateral authentication from UICC to network;
- message integrity;
- replay detection;
- proof of receipt;
- message confidentiality.

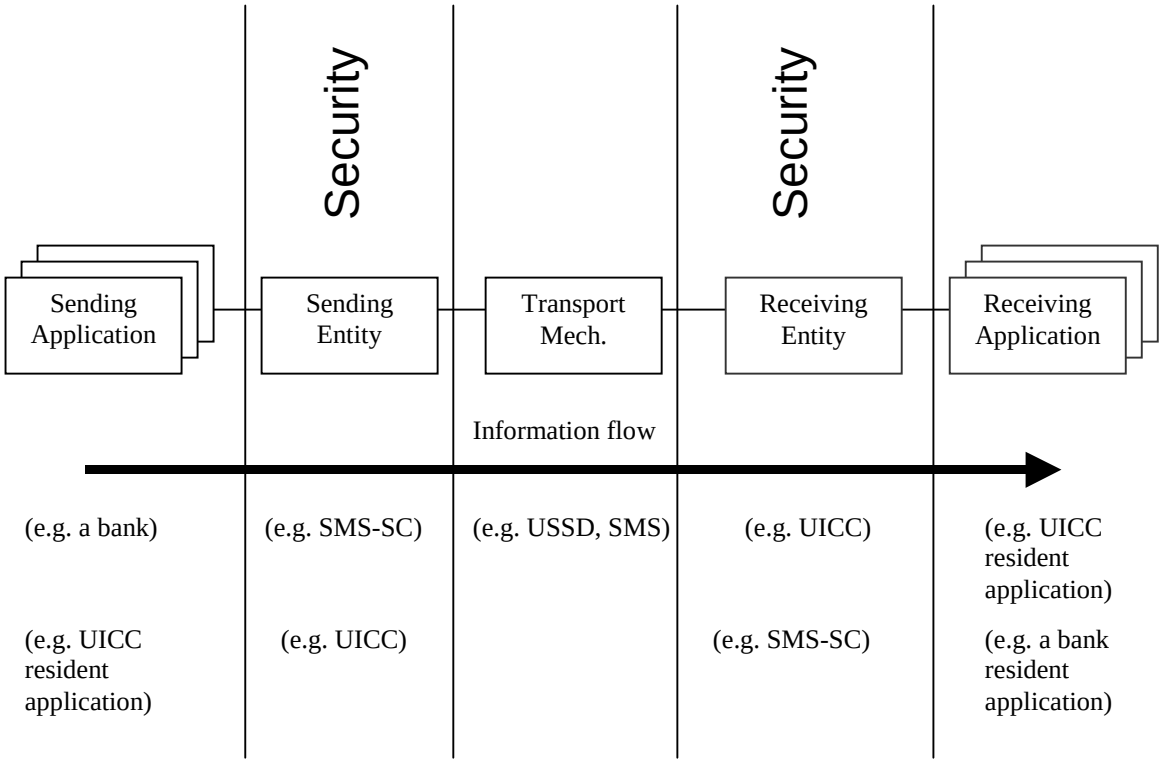

Figure 1: System overview

5 Security requirements

5.0 General

The application message is transferred from the sending application to the receiving application in one or more secured packets via a sending entity and a receiving entity, or group of receiving entities. The receiving entity is then responsible for reconstructing the application message from the received secured packets for presentation to the target receiving application. It is possible that there are several receiving entities and applications.

The sending application shall indicate to the sending entity the security mechanisms to be applied to the application message. This shall be indicated in the secured packet. The receiving entity shall indicate to the receiving application the security mechanisms applied to the secured packet, in a secure manner. The interface between the sending application and the sending entity, and the interface between the receiving entity and receiving application are not defined.

The security requirements to satisfy when transferring application messages from the sending entity to the receiving entity that have been considered are:

- authentication;
- message integrity;
- replay detection and sequence integrity;
- proof of receipt and proof of execution;
- message confidentiality;
- indication of the security mechanisms used.

Mechanisms to satisfy the above requirements will be governed by the following assumptions:

- in general, security is provided for each secured packet transmitted (an application message may be broken into several secured packets, each of which shall have identical security mechanisms applied to it);
- there should be the ability to turn mechanisms on and off on a per application message basis, with an indication of the status transmitted with the message;
- security related information used should be independent of that used with existing network keys;
- third party applications may have access to the sending entity, however this is considered to be an internal network security issue and therefore outside of the scope of the present document.

5.1 Authentication

5.1.1 Definition

Authentication is the verification of an entity's claimed identity by another entity. A first level of authentication is "unilateral authentication" which provides the receiver with proof of the sender's identity. A higher level is "mutual authentication", where both entities are provided with proof of each other's identity.

For mutual authentication purposes the sending and/or receiving entities have to generate and exchange dedicated authentication messages. Due to the unidirectional nature of current transport mechanisms mutual authentication is not considered in the present document.

5.1.2 Purpose

The purpose of authentication is to protect sending and receiving Entities and applications against unauthorized use. Authentication assures that only authorized parties can perform actions at the UICC, and it prevents unauthorized parties from having access to entities on the network side (or even behind it) via a Card Application Toolkit (CAT) feature.

5.1.3 Functional requirements

For the purposes of sender identification and unilateral authentication the sending entity shall be uniquely defined and addressed.

Unilateral authentication can be achieved by the use of a cryptographic checksum or digital signature attached to the message. The distinguishing identifications of the receiving and sending entities should be linked to them for the entire life time of these entities. (If for some reason, the identity of any of the entities is changed, then all other entities involved in the authentication procedure shall be informed of the new identity.)

5.2 Message integrity

5.2.1 Definition

Message Integrity detects that no corruption, accidental or intentional, of the content of the message has occurred.

5.2.2 Purpose

The purpose of this mechanism is to detect any corruption of the application message or the whole secured packet.

5.2.3 Functional requirements

The integrity of the application message or whole secured packet may be achieved as follows:

- by adding a Redundancy Check in the security header to protect against accidental corruption (the redundancy check mechanism on its own only protects against accidental corruption. In conjunction with encryption it can be used to provide message integrity);
- by adding a cryptographic checksum in the security header. In certain circumstances the authentication of the sending entity is achieved implicitly by the verification of the cryptographic checksum;
- by calculating and verifying a digital signature on the application message to be transferred. In this case the authentication of the sending entity is achieved implicitly by the verification of the digital signature.

5.3 Replay detection and sequence integrity

5.3.1 Definition

Replay detection is a mechanism which provides the receiving entity with a means of recognizing that it has received the same secured packet(s) previously.

Sequence integrity is a mechanism which ensures that no changes, accidental or intentional, have occurred to the intended sequence of secured packets.

5.3.2 Purpose

Replay detection protects the receiving entity against replay attack and secured packet duplication.

Sequence integrity protects the receiving entity against message suppression and loss of secured packets.

5.3.3 Functional requirements

The implementation of these mechanisms shall be achieved by including a counter in the security header. The protection of the counter shall be achieved by including it in the calculation of the checksum (cryptographic checksum or encrypted redundancy check) or digital signature when used.

The sending entity and the receiving entity shall maintain synchronization for their counters.

5.4 Proof of receipt and proof of execution

5.4.1 Definition

Proof of receipt proves to the sending entity that the receiving entity has correctly received a secured packet, has performed the necessary security checks and forwarded the contents to the receiving application.

Proof of execution proves to the sending application that the receiving application has performed an action that the sending application initiated. Proof of execution is not applicable at the transport layer.

5.4.2 Purpose

The purpose of proof of receipt is to prove delivery of a secured packet to the receiving entity in an unambiguous way. This allows detection of non-delivery due to network error, message corruption, validation failure etc. to be indicated to the sending entity using a status code in the proof of receipt response.

5.4.3 Functional requirements

Proof of receipt shall be requested by the sending entity. Proof of receipt is returned from the receiving entity in an acknowledgement to a secured packet transmitted by the sending entity. The acknowledgement shall take the form of a status code in a response message, which may be secured by either a cryptographic checksum or digital signature.

The sending entity shall send an indication of proof of receipt to the sending application upon successful delivery of the application message, or indicate the reason for failure upon unsuccessful delivery of the application message. The behaviour at the receiving entity is elaborated in ETSI TS 102 225 [2].

The Sending and receiving entity shall be uniquely defined and addressed.

The proof of receipt may be carried in a bearer dependant manner for optimization purposes, e.g. in the case of SMS transport, proof of receipt may be carried in the short message acknowledgement as defined in ETSI TS 131 111 [3] (SMS data download mechanism).

5.5 Message confidentiality

5.5.1 Definition

Message confidentiality ensures that the messages contents exchanged are not made available or disclosed to unauthorized individuals, entities, or processes.

5.5.2 Purpose

This security function prevents any external party from extracting any useable information from secured packets.

5.5.3 Functional requirements

Message confidentiality is achieved by encrypting the message. In order for the recipient to use the content of the message it has to be decrypted.

Some of the security parameters that make up the Security Header (digital signatures, counters and other security parameters) may be encrypted.

NOTE: There may be legal constraints for the implementation of message confidentiality mechanisms entirely resident on the UICC, see ETSI ETR 330 [i.1].

5.6 Security management

The security mechanism applied to the secured packet shall be indicated in the security header, and this indication may be integrity protected to prevent it from malicious alteration.

Security parameters (e.g. counters, keys) at the receiving and sending entity shall be stored in a secure manner such that no unauthorized parties or applications can read, modify or use these parameters.

Procedures for key management (e.g. key update) should be foreseen for transport level.

5.7 User Notification

5.7.1 Definition

User notification notifies the user that the processing of application data has succeeded or failed (e.g. the UICC is transferring a success or error message to be displayed by the mobile).

5.7.2 Purpose

The user notification is a way to inform the user that some application data were processed, successfully or not.

5.7.3 Functional requirements

User notification is requested by the sending application.

If requested, after the processing of application data, a user notification shall be available e.g. the display of a string on the mobile at the end of the processing. In this case, the user shall be notified that the processing was successful or failed, depending on the execution result.

The notification text, if any, should be either included in the script or pre-stored in the UICC.

Optionally, there may be a mechanism to notify the user before or during the processing of application data.

6 Normal procedures

6.1 Security mechanisms

6.1.0 General

From the security requirements described in clause 5, the following clauses define security mechanisms on the transport layer. Some of the security mechanisms fulfil more than one security requirement.

6.1.1 Authentication mechanisms

Mechanisms ensuring authentication are:

- cryptographic checksum (b1);
- digital signature (b2).

The cryptographic checksum mechanism is suitable for authentication when the secret information is shared only by the communicating entities.

6.1.2 Message integrity mechanisms

Mechanisms ensuring message integrity are:

- Redundancy check.
- Cryptographic checksum (b1).
- Digital signature (b2).

The redundancy check mechanism on its own only protects against accidental corruption. In conjunction with encryption it can be used to provide message integrity.

6.1.3 Replay detection and sequence integrity mechanisms

Mechanisms ensuring replay detection and sequence integrity are:

- Simple counter.
- A counter included in the calculation of the cryptographic checksum (d1).
- A counter included in the calculation of the digital signature (d2).

The simple counter mechanism protects against accidental loss or replay. In conjunction with encryption it can be used to protect against malicious loss or replay. There shall exist a specific counter value which indicates that the replay detection and sequence integrity mechanisms are inactive.

6.1.4 Proof of receipt mechanisms

NOTE: The proof of receipt mechanisms may frequently be used in conjunction with replay detection and sequence integrity.

Mechanisms ensuring proof of receipt are:

- unsecured acknowledgement;
- acknowledgement included in the calculation of the cryptographic checksum (f1);
- acknowledgement included in the calculation of the digital signature (f2).

6.1.5 Message confidentiality mechanisms

- Encryption mechanism (g).

6.2 Security mechanisms and recommended combinations

6.2.1 Non-cryptographic mechanisms

In the following a number of mechanisms are listed which are based on non-cryptographic mechanisms. These mechanisms offer no security against any deliberate attack, only detection of accidental corruption:

- redundancy check;
- unsecured acknowledgement;
- simple counter.

6.2.2 Cryptographic mechanisms

The security header, except the cryptographic checksum/digital signature, shall always be included in the calculation of the cryptographic checksum/digital signature:

- Cryptographic checksum (d1) or digital signature (d2).

  This security mechanism addresses the following security requirements: authentication, message integrity, replay detection and sequence integrity;

- Acknowledgement as cryptographic checksum (f1) or digital signature (f2).

  This security mechanism satisfies the security requirement proof of receipt.

- Encryption of the application data and possibly part of the security header (g).

  The encryption of the application data and possibly part of the security header corresponds to the requirement of message confidentiality.

Table 1: Overview of cryptographic mechanisms

Requirements	Mechanisms		
	Cryptographic checksum	Digital signature	Encryption
Authentication	(b1)	(b2)	
Message integrity	(b1)	(b2)	
Replay detection and sequence integrity	(d1)	(d2)	
Proof of receipt	(f1)	(f2)	
Confidentiality			(g)

When the security of a cryptographic algorithm from the technical specification is considered compromised, it may be deprecated.

When a new cryptographic algorithm becomes state of the art, its addition to the implementation specification shall be considered.

6.2.3 Recommended combinations of cryptographic mechanisms

Whilst it is recognized that many combinations of the above described security mechanisms are possible and feasible, for the purpose of the present document, in order to limit the complexity of implementation, a limited number of combinations is recommended:

- combinations employing cryptographic checksum:
  - combination 1: d1
  - combination 2: d1 + f1
  - combination 3: d1 + f1 + g
  - combination 4: d1 + g
- combinations employing digital signature:
  - combination 5: d2
  - combination 6: d2 + f2
  - combination 7: d2 + f2 + g
  - combination 8: d2 + g

It is recommended that encryption is employed only in conjunction with either a redundancy check, cryptographic checksum or digital signature in order to allow verification of the decryption.

If only authentication and message integrity are required this is indicated by a special counter value as described in clause 6.1.3.

7 Exceptional procedures

7.1 Authentication or integrity failure

In the case of authentication or integrity failure, the received message shall be discarded. If proof of receipt has been requested, then a status code indicating the reason for failure shall be returned to the sending entity.

7.2 Sequence and replay detection failure

There are several mechanisms whereby counter value synchronization can be maintained, or regained if synchronization is lost If synchronization cannot be regained, the receiving entity shall discard any secured packet with an unsynchronized counter value. In addition, if proof of receipt has been requested, then a status code indicating the reason for failure shall be returned to the sending entity.

7.3 Proof of receipt failure

The sending entity shall inform the sending application of the failure to deliver the application message, indicating the reason for failure.

8 Interfacing to the Transport Layer

In addition to network specific transport mechanisms (e.g. SMS, USSD), an encapsulation of the secured data to the following mechanism is required:

- CAT_TP according to ETSI TS 102 127 [7].

9 Remote Application Management over IP

9.0 General

A UICC, compliant with ETSI TS 102 483 [8] describing IP connectivity, may provide application remote management of the UICC over IP.

This feature delivers a management interface that allows a remote entity to manage applications in the UICC through an IP connection to the UICC.

9.1 Transport requirement

It shall be possible for an authorized remote entity to manage UICC applications and application data remotely over IP.

The following entities shall be able to initiate a connection between a remote entity and the UICC:

- the card issuer;
- a third party, if authorized by the card issuer (in the context of Confidential Application requirements mentioned in ETSI TS 102 412 [9]);
- or an application residing in the UICC, if authorized by the card issuer.

The transport layer shall ensure reliability of the transport layer, providing retry policy and failure report.

9.2 Functions requirements

The following functions shall be described:

- initiating the connection between the remote entity and the UICC;
- loading, activation and deletion of all types of existing applications (applet, web-application, servlet) and application resources (static pages, etc.);
- updating of provisioned security data (such as keys dedicated to application management) in a secure way;

- diagnosis function such as retrieving the list of applications in the card and the list and amount of memory areas available.

It shall be possible to reuse existing IP connection between the remote entity and the UICC.

The formatting of the message shall be independent of the APDU coding.

9.3 Security requirements

Security mechanisms shall provide:

- mutual authentication between the UICC and the remote entity;
- message confidentiality;
- message integrity;
- anti-replay attack protection.

The security shall be extensible as required.

Indication of proprietary security mechanism and key agreement shall be possible.

Several key sets and algorithms shall be available for the different parties managing this transport layer (card issuer, third party, etc.).

Once a connection has been open allowing application remote management, it shall be up to application in the UICC involved in the initiating the transport layer to check the security of the message, before forwarding the message to the receiving application.

9.4 Backward compatibility requirements

There shall be a mechanism to reuse legacy Remote Management commands over this new mechanism.

Annex A (informative): Change history

This annex lists all changes made to the present document.

History Table					
Date	**Meeting**	**Tdoc**	**Changes**	**Old**	**New**
2002-03	SCP#9	SCP-020055	Editorial changes after discussion at SCP#9. This version has been sent to the ETSI secretariat for publication in March 2002 as ETSI TS 102 224 V6.0.0. No technical changes compared to V2.0.0	2.0.0	6.0.0
2004	SCP#19	SCP-040457	Clarification for non-specific references	6.0.0	6.1.0
2005-12	SCP#23	SCP-050520	Requirement for user notification after execution of an OTA request.	6.1.0	7.0.0
2006-09	SCP#27	SCP-060490	Alignment with ETSI TS 102 225 concerning CAT_TP as transport layer	7.0.0	7.1.0
2008-07	SCP #38	SCP-080345	Addition of requirements for cryptographic algorithms	7.1.0	8.0.0
2008-07	SCP #38	SCP-080349	Introduction of Remote Management over IP requirements	7.1.0	8.0.0
2018-09			Automatic upgrade to release 9	8.0.0	9.0.0
2018-09			Automatic upgrade to release 10	9.0.0	10.0.0
2018-09			Automatic upgrade to release 11	10.0.0	11.0.0

History

Document history		
V11.0.0	September 2018	Publication