

ETSI TS 102 224 V18.0.0 (2024-04)



Smart Cards; Security mechanisms for UICC based Applications Functional requirements (Release 18)

ETSI TS 102 224 V18.0.0 (2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/b9f27425-08ac-4ad4-b9f7-e9840718cfad/etsi-ts-102-224-v18-0-0-2024-04>

ReferenceRTS/SET-R102224vi00

Keywordssecurity, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<https://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights5

Foreword.....5

Modal verbs terminology.....6

1 Scope7

2 References7

2.1 Normative references7

2.2 Informative references.....8

3 Definition of terms, symbols and abbreviations.....8

3.1 Terms.....8

3.2 Symbols.....9

3.3 Abbreviations9

4 Introduction9

5 Security requirements.....10

5.1 Introduction10

5.2 Authentication11

5.2.1 Definition.....11

5.2.2 Purpose11

5.2.3 Functional requirements11

5.3 Message integrity11

5.3.1 Definition.....11

5.3.2 Purpose11

5.3.3 Functional requirements12

5.4 Replay detection and sequence integrity12

5.4.1 Definition.....12

5.4.2 Purpose12

5.4.3 Functional requirements12

5.5 Proof of receipt and proof of execution.....12

5.5.1 Definition.....12

5.5.2 Purpose12

5.5.3 Functional requirements13

5.6 Message confidentiality.....13

5.6.1 Definition.....13

5.6.2 Purpose13

5.6.3 Functional requirements13

5.7 Security management13

5.8 User Notification13

5.8.1 Definition.....13

5.8.2 Purpose14

5.8.3 Functional requirements14

6 Normal procedures14

6.1 Security mechanisms14

6.1.1 Introduction.....14

6.1.2 Authentication mechanisms14

6.1.3 Message integrity mechanisms14

6.1.4 Replay detection and sequence integrity mechanisms14

6.1.5 Proof of receipt mechanisms.....15

6.1.6 Message confidentiality mechanisms15

6.2 Security mechanisms and recommended combinations15

6.2.1 Non-cryptographic mechanisms15

6.2.2 Cryptographic mechanisms.....15

6.2.3 Recommended combinations of cryptographic mechanisms16

7 Exceptional procedures16

7.1	Authentication or integrity failure	16
7.2	Sequence and replay detection failure	17
7.3	Proof of receipt failure	17
8	Interfacing to the Transport Layer.....	17
Annex A (informative): Change history		18
History		19

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 102 224 V18.0.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/b9f27425-08ac-4ad4-b9f7-e9840718cfad/etsi-ts-102-224-v18-0-0-2024-04)
<https://standards.iteh.ai/catalog/standards/etsi/b9f27425-08ac-4ad4-b9f7-e9840718cfad/etsi-ts-102-224-v18-0-0-2024-04>

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Secure Element Technologies (SET).

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 SET and may change following formal TC SET approval. If TC SET 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 SET for information;
 - 2 presented to TC SET for approval;
 - 3 or greater indicates TC SET 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.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 102 224 V18.0.0 \(2024-04\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/b9f27425-08ac-4ad4-b9f7-e9840718cfad/etsi-ts-102-224-v18-0-0-2024-04>