



**Cyber Security (CYBER);
Consumer Mobile Device;
Part 4: Preloaded Applications Protection Profile Module**

get full document from standards.iteh.ai

Reference

RTS/CYBER-00154

Keywords

cybersecurity, mobile, privacy, terminal

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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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 of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	8
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	9
3.3 Abbreviations	9
4 TOE Definition.....	9
4.1 TOE Overview	9
4.1.1 Introduction.....	9
4.1.2 Preloaded Application Requirements.....	10
4.1.3 Preinstalled Application Requirements.....	10
4.2 Usage and Major Security Features.....	10
4.3 PP-Module Identification	11
4.4 Base-PP Identification	11
4.5 Conformance Claim	11
5 Security Problem Definition.....	11
5.1 Assets and interfaces of the TOE	11
5.2 Threat agents and threats.....	12
5.3 Organizational Security Policies	12
5.4 Assumptions	12
6 Security Objectives.....	12
6.1 Security Objectives for the TOE	12
6.2 Security Objectives for the Operational Environment.....	12
6.3 Security Objectives Rationale	12
7 Extended Components.....	13
7.1 Definitions.....	13
7.1.1 Definition of the Class FAP: Applications	13
7.1.2 Definition of the family Application Lifecycle (FAP_LFC_EXT).....	14
7.1.3 Definition of the family Application Permissions (FAP_PRM_EXT)	14
7.1.4 Definition of the family Application Risk (FAP_RSK_EXT)	15
7.1.5 Definition of the Identification of applications on device (ALC_PAL_EXT).....	18
8 Security requirements.....	19
8.1 Conventions.....	19
8.2 ETSI TS 103 732-1 Security functional requirements.....	20
8.3 TOE Security functional requirements	20
8.3.1 Applications (FAP).....	20
8.3.2 Application Risk (FAP_RSK_EXT).....	20
8.4 ETSI TS 103 732-1 Security assurance requirements	21
8.4.1 Modified SARs	21
8.4.2 Processed Data Minimisation (ADV)	21
8.5 Security assurance requirements	22
8.6 Security requirements rationale.....	22
8.6.1 Rationale for choosing the SARs.....	22
8.6.2 The SFRs meet all the security objectives for the TOE	23
8.6.3 Dependency analysis.....	23

8.7	Consistency rationale	23
8.7.1	TOE type consistency	23
8.7.2	Consistency of Security Problem Definition	23
8.7.3	Consistency of Objectives	24
8.7.4	Consistency of Requirements	24
History		25

Sample Document

get full document from standards.iteh.ai

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 IPR online database](#).

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™**, **LTE™** and **5G™** logo 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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [5].

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.

Introduction

Consumer mobile devices like smartphones are becoming the entrance to digital services, such as mobile banking, electronic identity verification, digital key management, etc. Preloaded applications installed on the device provide many of these services for the user from the time the device is setup. As these applications are either included in the main OS or installed before the user completes the device set up, the manufacturer provides a measure of trustworthiness by documenting the preloaded applications and verifying the preloaded applications do not introduce security threats.

The present document identifies key focus areas around the applications preloaded on a consumer mobile device in typical consumer usage scenarios and identifies security threats to be mitigated in those applications. The identified threats are mitigated by security objectives, which are in their turn fulfilled by implementing appropriate security functional requirements.

The present document is defined as a Protection Profile Module (hereafter called PP-Module) following the structure from the Common Criteria (CC) standards [7], [8], [9], [10], [11] and [12] and therefore can be used for third party CC security assessments and certification. Notice that the present document has not been evaluated or certified as a formal PP-Module.

The requirements in the present document take published standards, recommendations and guidance in clause 2 into consideration.

Sample Document

get full document from standards.iteh.ai

1 Scope

The present document defines a PP-Module for Consumer Mobile Device (CMD) which adds additional security requirements on preloaded applications and the functional capabilities (objectives and security functional requirements) that are required to mitigate threats from poor programming of those applications.

The present document is intended for CMD manufacturers implementing those security requirements for device certification and for third parties looking to assess the security functions on CMD such as evaluators.

The Target Of Evaluation (TOE) described by the present document is the set of preloaded applications included on a CMD.

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 in the [ETSI docbox](#).

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] Void.
- [2] Void.
- [3] Void.
- [4] Void.
- [5] [ETSI TS 103 732-1 \(V3.1.1\)](#): "Cyber Security (CYBER); Consumer Mobile Device; Part 1: Base Protection Profile".
- [6] [CCMB-2022-11-001](#) CC:2022 Revision 1, November 2022: "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model".
- [7] [CCMB-2022-11-002](#) CC:2022 Revision 1, November 2022: "Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components".
- [8] [CCMB-2022-11-003](#) CC:2022 Revision 1, November 2022: "Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components".
- [9] [CCMB-2022-11-004](#) CC:2022 Revision 1, November 2022: "Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities".
- [10] [CCMB-2022-11-005](#) CC:2022 Revision 1, November 2022: "Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements".
- [11] [CCMB-2022-11-006](#) CC:2022 Revision 1, November 2022: "Common Methodology for Information Technology Security Evaluation".
- [12] [CCMB-2025-001](#) Version 1.2, October 15, 2025: "Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)".