ETSI TS 103 732 V1.1.1 (2021-11)

TECHNICAL SPECIFICATION

CYBER;
Consumer Mobile Device Protection Profile

Reference

DTS/CYBER-0052

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:
http://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/CommiteeSupportStaff.aspx

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

Contents

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.

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).

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. Meanwhile more and more security attack vectors are being explored, such as malicious applications, network eavesdropping. Defining security and assurance requirements for mobile devices can mitigate potential risks and drive the mobile device security to an appropriate level in order to protect users of such mobile devices.

The present document identifies key assets to be protected in typical consumer usage scenarios and identifies security threats associated to these key assets. 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 (hereafter called PP) following PP structure from the CC standards [1], [2], [3] 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.

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

1 Scope

The present document defines a PP for Consumer Mobile Device (CMD), which is typically a user-customisable device utilising an operating system, supporting installation and maintenance of applications, with wireless internet connectivity, high computation power and rich user interface, such as smartphones or tablets, used for various purposes by the individual owner.

The present document identifies key assets of the CMD to be protected and identifies the threats associated to them and the functional capabilities (objectives and security functional requirements) that are required to mitigate those threats. Finally, the present document specifies the security assurance requirements against which the CMD security can be assessed in a CC security evaluation.

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 a consumer mobile device. The following items are excluded from the scope:

- all applications (apps) downloaded by a human user and pre-installed non-system permission apps which can be uninstalled by the human user;
- all peripheral devices, including any data residing on these devices and any services associated with these devices, for example memory card;
- CMD features related to cellular mobile communication, including secure element which stores user credentials for cellular mobile communication, for example UICC [i.6];
- features related to multiple authenticated human users using the same 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 at https://docbox.etsi.org/Reference/.

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] Common Criteria for Information Technology Security Evaluation: "Part 1: Introduction and General Model", version 3.1 revision 5, CCMB-2017-04-01, April 2017.

[2] Common Criteria for Information Technology Security Evaluation: "Part 2: Security Functional Components", version 3.1 revision 5, CCMB-2017-04-02, April 2017.

[3] Common Criteria for Information Technology Security Evaluation: "Part 3: Security Assurance Components", version 3.1 revision 5, CCMB-2017-04-03, April 2017.

[4] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, SOG-IS Crypto Working Group, version 1.2, January 2020.

[5] Common Methodology for Information Technology Security Evaluation: "Evaluation methodology", version 3.1 revision 5, CCMB-2017-04-04, April 2017.

[6] IETF RFC 2818: "HTTP over TLS".

[7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[8] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[9] IETF RFC 5288: "AES Galois Counter Mode (GCM) Cipher Suites for TLS".

[10] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[11] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[12] Bluetooth® SIG: "Bluetooth Core Specification, v4.1".

[13] Bluetooth® SIG: "Bluetooth Core Specification, v4.2".

[14] Bluetooth® SIG: "Bluetooth Core Specification, v5.0".

[15] Bluetooth® SIG: "Bluetooth Core Specification, v5.1".

[16] Bluetooth® SIG: "Bluetooth Core Specification, v5.2".

[17] IEEE 802.11™-2016: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[18] IEEE 802.1X™-2020: "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control".

[19] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

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.

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 not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EN 303 645 (V2.1.1): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.2] Secure Communications Alliance IoT PP Working Group: "IoT Secure Element Protection Profile", version 1.0.0, December 19, 2019.

[i.3] ISO/IEC TS 30104:2015: "Information Technology - Security Techniques - Physical Security Attacks, Mitigation Techniques and Security Requirements".

[i.4] ISO/IEC 30107-4:2020: "Information Technology - Biometric Presentation Attack Detection - Part 4: Profile for testing of mobile devices".

[i.5] Global Platform Security Evaluation Standard for IoT Platforms, version 1.0, March 2020.

[i.6] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 16)".

[i.7] GSMA SGP.22: "RSP Technical Specification".

[i.8] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture".

[i.9] ETSI TS 133 401: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture".

[i.10] ETSI TS 133 501: "5G; Security architecture and procedures for 5G System".

[i.11] Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC-PP-0084-2014.

[i.12] GSMA SGP.25: "Embedded UICC for Consumer Devices Protection Profile".

[i.13] GSMA SGP.08: "Security Evaluation of Integrated eUICC".

[i.14] GSMA SGP.24: "GSMA SGP.24: "RSP Compliance Process".

[i.15] NIST SP 800-90A Rev. 1: "Recommendation for Random Number Generation Using Deterministic Random Bit Generators".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

best practice cryptography: cryptography that is suitable for the corresponding use case and has no indications of a feasible attack with current readily available techniques

consumer mobile device: user customizable device utilising an operating system, supporting installation and maintenance of applications, with wireless internet connectivity, high computation power and rich user interface, used for various purposes by the individual owner

EXAMPLE: Smartphones and tablets are typical consumer mobile devices.

device ID: unique identity of a consumer mobile device, which is not resettable

EXAMPLE: International Mobile Equipment Identity (IMEI) and Serial Number (SN).

device unique key: unique key stored in the device hardware during the initial manufacturing of the device, which is used to derive or encrypt other keys

human user: physical person using the CMD including actions taken by an object on behalf of the physical person, such as a stylus pen

NOTE: Both physical person and external IT entity such as trusted peer device are users of the TOE as defined in [3], to differentiate the two types of users, the term "human user" is used to refer to a physical person. In the present document, user data refers to human user data.

security problem: statement, which in a formal manner defines the nature and scope of the security that the TOE is intended to address [1]

security objective: statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions [1]

security functional requirement: requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE [1]

security assurance requirements: description of how assurance is to be gained that the TOE meets the SFRs.

system permission: permission granted by the operating system to manage the operating system (such as power off), provide core functions (such as SMS and Telephone), or access to underlying software and hardware interfaces

target of evaluation: set of software, firmware and/or hardware possibly accompanied by guidance [1]

TOE security functionality: combined functionality of all hardware, software, and firmware of a TOE that are relied upon for the correct enforcement of the security functional requirements

TOE software: operating system and pre-installed system permission apps which are updated together from a Trusted Update Source

trusted peer device: device with a trusted relationship with the TOE for purposes of interaction with the TOE

EXAMPLE: Screen sharing, file sharing, moving the entire content from an old device to a new device.

trusted update source: central repository from which updates to the TOE software can be downloaded

NOTE: This repository is typically managed by the TOE developer/OEM and authenticity and integrity of updates are typically guaranteed by digitally signing the updates.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

API	Application Program Interface
CC	Common Criteria
CMD	Consumer Mobile Device
DEK	Data Encryption Key
DUK	Device Unique Key
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman
EEPROM	Electrically Erasable Programmable Read Only Memory
FAR	False Acceptance Rate
FCS	Functional class Cryptographic Support
FDP	Functional class user Data Protection
FIA	Functional class Identification and Authentication
FMT	Functional class security ManagemenT
FPR	Functional class PRivacy
FPT	Functional class Protection of the TSF
FRR	False Rejection Rate
FTP	Functional class Trusted Path/Channels
GCF	Global Certification Forum
GPS	Global Positioning System
GSM	Global System for Mobile
IT	Information Technology
JTAG	Joint Test Action Group
KEK	Key Encryption Key
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
OS	Operating System
PCS	Personal Communication Service
PIN	Personal Identification Number
PP	Protection Profile
PRF	Pseudo Random Function
QR	Quick Response
RNG	Random Number Generator
SAR	Security Assurance Requirement
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirement
SMS	Short Message Service
SoC	System-on-Chip
SOG-IS	Senior Officials Group Information Systems Security

ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functionality
UI	User Interface
USB	Universal Serial Bus
WLAN	Wireless Local Access Network

4 TOE Definition

4.1 TOE Overview

The TOE described by the present document is a subset of a CMD as shown in Figure 1. The CMD includes hardware, an operating system and apps. Apps are categorised as pre-installed system permission apps, pre-installed non-system permission apps, and downloaded apps. Examples of a CMD include smart phone, tablet and other device with similar capabilities. Human users can customise their CMDs (modify their UI appearance, download apps, etc.) and use these devices for a wide range of purposes.

The TOE includes hardware, the operating system and pre-installed system permission apps that are delivered with the CMD out of the box. Pre-installed non-system permission apps and apps that are installed later by the human user (downloaded apps) are not considered part of the TOE. However, if a pre-installed non-system permission app cannot be uninstalled by the human user, it is included in the TOE.

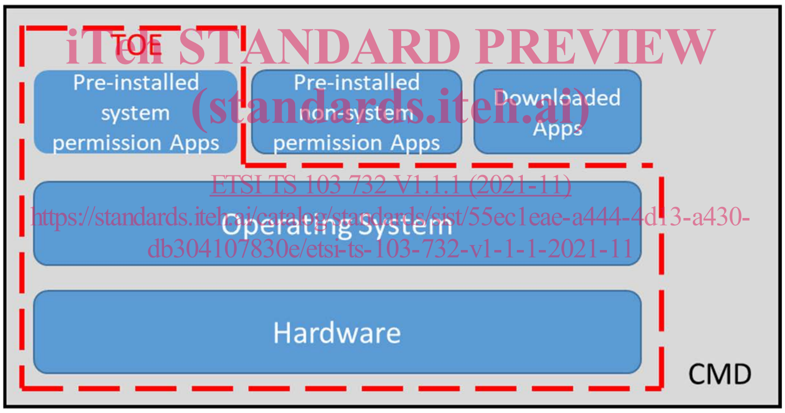
TOE
Pre-installed system permission Apps
Pre-installed non-system permission Apps
Downloaded Apps
Operating System
Hardware
CMD

Figure 1: TOE boundary

The hardware of the TOE includes the hardware platform, physical enclosure and peripheral components such as sensors and the display. The hardware does not include any devices removable by a human user, including any data residing on these devices and any services associated with these devices, for example a memory card.

Any data on these devices or services associated with these devices is out of scope of the TOE.

The operating system of the TOE controls and manages the hardware and the apps (both pre-installed and downloaded) and provides the user operation interface and application programming interface(s).

The pre-installed apps are apps that are already present on the CMD when it is delivered to the consumer. Pre-installed apps are divided into two kinds:

1) Pre-installed system permission apps: apps which have permissions to manage the operating system (such as power off), provide core functions (such as SMS and Telephone) or access to underlying software and hardware interfaces. These apps require permissions granted by the operating system and cannot be revoked by the human user. These permissions are denoted as system permissions for the purpose of the present document. System permission apps include apps that provide core operating system functionality or security enforcement functionality, apps signed by a platform key from the operating system provider, and other apps allowed by the TOE developer to get such permissions. System permission apps can also require permissions granted by the human user in addition to system permissions.

2) Pre-installed non-system permission apps: apps which do not require system permissions. Non-system permission apps can have permissions granted by human user to access to user data and/or permissions granted by the operating system which are necessary to the operation of apps. Non-privileged apps can usually be uninstalled.

Downloaded Apps are apps that are downloaded and installed by the human user and can subsequently be uninstalled by the human user. Downloaded Apps do not have system permissions.

Security functionalities of the TOE related to cellular mobile communication are defined in [i.8], [i.9], [i.10] and will be certified by Global Certification Forum (GCF) and PCS Type Certification Review Board (PTCRB). Security of a secure element which stores user credentials for cellular mobile communication, e.g. UICC, eUICC [i.7], and integrated eUICC is specified in [i.11], [i.12], [i.13] and [i.14], and will be certified by a CC Certification Body. Therefore, these functions are out of scope for the present document. It is assumed that the TOE meets applicable security requirements defined in these specifications and TOE developer should provide evidence for such assumption if the evaluation of the TOE depends on such evidence, such as certificate of eUICC.

Functionality related to multiple authenticated human users using the same CMD is also out of scope. Whether one human user can see or alter the user data of another human user, or whether one human user can delete the account of another human user is not covered in the present document.

The present document is intended to be used for TOE which does not carry an altered operating system which enables the user to manage system permissions, such as rooted device.

The TOE developer shall define the TOE clearly as part of submission for CC evaluation.

4.2 Usage and Major Security Features

The TOE is a subset of a CMD with wireless connectivity, high computation power and rich user interface. A human user can customise the device by downloading apps and changing settings. A human user can perform a wide range of actions with the TOE, such as make phone and video calls, perform various productivity tasks, play games, music and videos, and access the Internet.

The TOE interacts with its environment as shown in Figure 2.

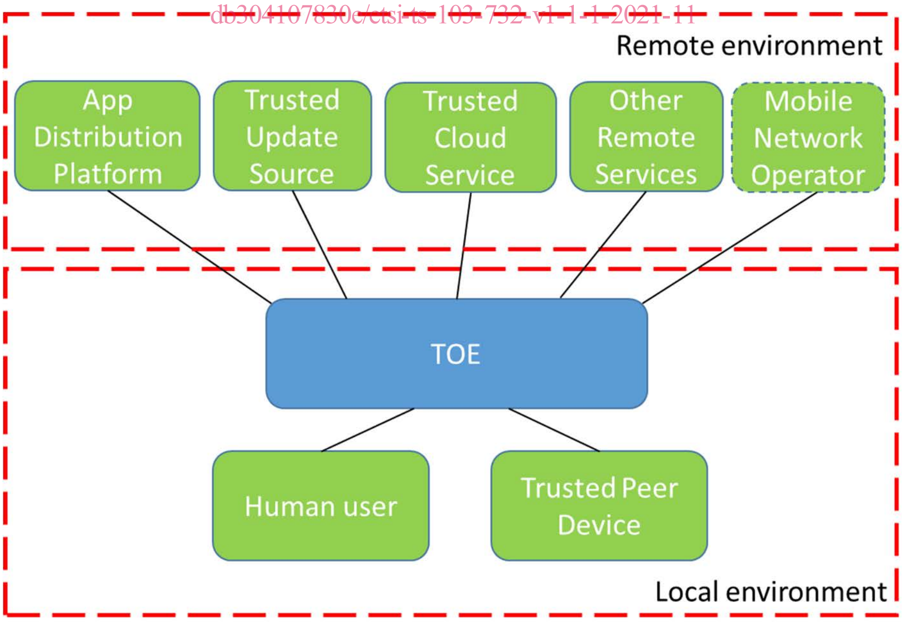

Figure 2: TOE environment

The TOE has a local environment with:

- A human user, who physically interacts with the TOE across its user interface(s).
- (Optionally) one or more Trusted Peer Devices, which can interact with the TOE in actions such as screen sharing or collaborative editing.

The TOE has a remote environment with:

- A Trusted Update Source, from which the TOE can download updates for TOE software. These updates are digitally signed, and the TOE checks whether this signature is correct.
- App Distribution Platform of the TOE developer and/or OS developer, from which the TOE can download and install apps. The App Distribution Platform will detect malicious in-app behaviour, conducts privacy disclosure inspections for apps that call, collect or upload sensitive data from human users without permission, as well as scans apps for the presence of loopholes, vulnerabilities or backdoors. How the App Distribution Platform performs security checks of applications is out of scope of present document. The App Distribution Platform application on the TOE is in scope. It is assumed that only App Distribution Platform applications from TOE developer and/or OS developer will be pre-installed. A human user may install additional App Distribution Platform applications, in which case the human user takes the responsibility for the security of apps downloaded and installed from any additional App Distribution Platforms.
- Trusted Cloud Service provided by the TOE developer. A human user can use cloud service to access user data in the TOE. It is assumed that the cloud service will be secure, and vulnerabilities of cloud service are not in scope of present document. The security of the connection from the TOE to any trusted cloud service is assured by trusted channel requirements defined in clause 8.1.7.
- Other Remote Services offered by third parties, such as enterprise services, additional App Distribution Platforms used by a human user, websites, gaming servers, etc. The present document provides no assurance in these remote services, so it is up to the human user to trust a particular remote service.
- (Optionally) one or more Mobile Network Operators when the TOE supports cellular radio connection. This will be assured by GCF and therefore it is assumed that the Mobile Network Operator will provide secure cellular communication with the TOE.

The major security features are:

- Authentication of human user: to ensure that the human user is authenticated by the TOE before he/she can fully use the TOE (it may be possible to make very limited use of the TOE before authentication, such as making emergence call).
- Authentication of Trusted Peer Devices: the TOE allows other devices to act as a trusted peer device for purposes such as screen sharing and collaborative editing. To be able to do this, these devices first authenticate themselves.

- Secure communication: the TOE offers one or more secure communication channels, protected against unauthorised modification and unauthorised disclosure. These channels can subsequently be used by apps and by the TOE itself for various communication purposes.
- Secure updating of TOE software: the TOE can update the TOE software by downloading an update from a Trusted Update Source to address known vulnerabilities in a timely manner.
- Secure updating of apps: the TOE can update pre-installed non-system permission apps and Downloaded Apps by downloading an update from the App Distribution Platform.
- Self-protection and integrity verification of the TOE: the TOE protects both itself and other apps against malicious apps who can try to hack into the TOE. The TOE also checks its own integrity every time it starts up to check whether it has been altered.
- Protecting user data at different levels of security: the TOE supports classification of user data according to risk levels and usage scenarios and protects user data to ensure it is accessed by the right person on the right device in the right condition.
- Permission management of apps: to ensure that apps can only access to user data on the TOE and services provided by the TOE which are essential to their operation and where permission has been granted by the human user and/or by the operating system.
- Protection against tracking by app developers and advertisers: The TOE can provide an alias to app developers and advertisers, so that they have limited tracking of the human user. The human user can replace that alias with another alias to limit this tracking.