3GPP TR 31.801 V15.1.0 (2020-09)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Technical requirements for the secure platform for 3GPP applications; (Release 15)

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG 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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

ETSI TC SCP has informed 3GPP (and other organisations) that it has started work on defining use cases and requirements for a new more efficient and flexible secure platform that is intended to provide a flexible and modern platform for various applications, including 3GPP applications like the USIM, ISIM, HPSIM. ETSI TC SCP also asked the recipients of their Liaison Statement (C6-160246) for input on application specific use cases and requirements

The UICC, which is used as the platform for 3GPP applications (USIM, ISIM, HPSIM) is based on specifications created in the 1980s. Many services having been or being developed in 3GPP are requiring the storage of large and complex amounts of data in the USIM. There are also other areas like e.g. IoT that create new requirements for power efficiency and hardware flexibility.

1 Scope

The present document studies and evaluates the technical requirements for a secure platform hosting 3GPP applications up to Release 14. It is the intention to feed the result of the work to ETSI TC SCP, so that it can be taken into account during the definition of their use cases and requirements for this new secure platform.

Requirements for 5G, i.e. Release 15 will be defined during the work on 5G and summarized in other specifications.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 41.001: "GSM Release specifications".

[3] 3GPP TS 24.383: "Mission Critical Push To Talk (MCPTT) Management Object (MO)".

[4] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to Proximity-services (ProSe) Function Protocol aspects; Stage 3".

[5] 3GPP TS 32.277: "Proximity-based Services (ProSe) charging".

[6] 3GPP TS 24.333: "Proximity-services (ProSe) Management Objects (MO)".

[7] ETSI TS 102 221 V14.0.0: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics ".

[8] ETSI TS 102 223 V13.2.0: "Smart Cards; Card Application Toolkit".

[9] 3GPP TS 24.385: "V2X services Management Object (MO)".

[10] 3GPP TR 31.970: "UICC power optimisation for Machine-Type Communication".

[11] ETSI TS 102 600 V10.0.0: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Symbols

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

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

I2C	Inter-Integrated Circuit
SPI	Serial Peripheral Interface

4 Existing features

4.0 Introduction

The following clauses describe existing features in 3GPP that make use of the UICC applications defined in 3GPP (USIM, ISIM, HPSIM…) and impose technical requirements that may not be optimally supported by the existing UICC as the platform.

4.1 File Storage

4.1.1 Introduction

In recent 3GPP releases, the number of configuration files for new 3GPP features that need to be stored in the UICC has consistently increased. In many of these cases, a complex and large XML schema is defined in 3GPP to provision the configuration into the device with OMA-DM. Due to existing requirements to have the possibility to configure the device also using the USIM, CT6 had to define ways to store the same information in the files of the USIM application or ISIM application.

In the past, most configuration files were coded in proprietary ways defined by CT6 (for example, using nested TLV objects). Anyway, that approach presented several drawbacks:

- A change in the specification that define the XML schema can have a potential large impact on the representation of the data in the UICC
- A device vendor is forced to implement two separate parsing functions to read the same configuration (i.e., using the XML schema and using the method defined by CT6)
- Some configuration files are so large and complex that it is difficult to convert them into a different format.

As a consequence of this, CT6 has started storing the configuration directly in XML format in the files of the USIM application or ISIM application. While this certainly solves the problems described above, it introduces new ones. More specifically, the access to the configuration files becomes problematic, due to the large size of the XML files.

CT6 is currently widely using the BER-TLV files defined in ETSI TS 102 221[7], but this approach has limitations, in the ability to retrieve the data. Access to the configuration files requires several commands that are performed in sequence. While the terminal can still perform some other operations that don't impact the file pointer (for example, authentication algorithm), the device would not be able to perform several other operations, thus leading to a potential bad user experience or even to failure of specific procedures.

Moreover, 3GPP had cases where the UICC was used as secure storage, to keep data that had to be transmitted to the server on the network while the device was unable to do (for example, out of coverage). When this occurs, the UICC needs to have sufficient space to internally store the data, waiting for the conditions to transmit it to the network.

4.1.2 Examples from 3GPP specifications

4.1.2.1 Configuration Parameters for MCPTT

The parameters stored in the USIM follow the specification of the Management Object for the ME as defined in 3GPP TS 24.383 [3]. The structure of the Management Object is, depending on the required services, complex and may therefore contain a large amount of data. The description of the Management Object is in XML, and the structure of the data cannot be easily reflected with the current file system design.

4.1.2.2 ProSe (Proximity Services) - Usage information storage

In the case of direct device to device communication without network coverage, the UE has to store the usage information according to the related configuration as specified in 3GPP TS 24.334 [4] and 3GPP TS 32.277 [5]. Depending on the configuration of which information needs to be included in the report, the amount of data to be stored may be large. On top of this, the longer the UE is out of coverage while using direct communication, the more likely it is that more than one report will need to be stored in the USIM. The data to be stored follows the specification of the related usage information Management Object as specified in 3GPP TS 24.333 [6]. With the current solution defined in 3GPP TS 31.102 [7] the ME sends the usage information report to the USIM and the USIM has to cater for storing the data received. The structure of the data cannot be easily reflected with the current file system design and due to the potential large amount of data the transmission of data may take a long time with the current interface between ME and UICC.

4.1.2.3 V2X (Vehicle-to-Everything

V2X requires to store configuration to enable the communication between a vehicle and other elements, such us other vehicles or infrastructure. The structure of the configuration is defined in TS 24.385 [9]: its structure is complex and may therefore contain a large amount of data. The description of the Management Object is in XML, and the structure of the data cannot be easily reflected with the current file system design.

4.4 Internet of Things

4.4.1 Power efficiency

4.4.1.1 Introduction

In the recent years, power consumption of the UE has become a very important aspect due to the rise of several IoT use cases that require that the device remains active for long periods of time, without the possibility to re-charge it. The overall power consumption is obviously composed by the sum of the power consumption of the ME and the power consumption of the UICC.

4.4.1.2 UICC suspension

3GPP conducted a study on the power consumption of the UICC, available in TR 31.970 [10]. This study was shared with ETSI SCP and was the basis to define the UICC suspension mechanism, specified in Release 14.

The UICC suspension mechanism allows the terminal to completely remove the power from the UICC and be able to restore the UICC status later on, when the UICC is required. Such a mechanism can significantly improve the power consumption when the duration of the suspension is sufficiently long, as described in the TR 31.970 [10], and so it is suitable mostly for devices that are idle for long periods of time.

3GPP CT6 expects that power consumption will remain a critical aspect also for the future, with even more use cases enabled by 5G technology. For this reason, the new secure platform should continue to support the suspension mechanism already introduced for the UICC, even if this might be implemented in a different way.

Also, CT6 encourages SCP to consider additional improvements to reduce the power penalty introduced by the UICC resume operation. This would have two benefits on the UE:

- further improve the power saving for devices that are idle for long periods of time

- ability to potentially extend the optimization to new classes of IoT devices that are idle for shorter periods of time.

4.4.1.3 Polling

As described in the TS 31.970 [10], the presence detection polling and the proactive polling performed by the ME are also causes of considerable power consumption. In the current 3GPP specifications, the presence detection polling can be suspended when the UE is idle, and the proactive polling can be disabled by the operator. These changes allows the device to avoid unnecessary polling, with the goal of saving power.

Polling should be taken into consideration while working on the new secure platform, in order to limit it only to cases where it is strictly required, trying to define solutions that allow complete disablement of polling, without compromising on the ability of the secure platform to initiate a proactive session or on the ability of the device to detect a removal of the secure platform (where the removal is possible at all).

4.4.1.4 Voltage

In the current 3GPP specifications, only two classes of operating condition are considered valid, that is class B (3.0V) and class C (1.8V). The voltage of the UICC has a clear impact on the amount of power that is consumed by the UICC itself and by the terminal.

Moreover, with the reduction in node technology on the terminals, support for class B has become more expensive, as it requires external power sources. For the same reason, also support for class C is currently at risk.

Since the new secure platform may potentially break backward compatibility with the UICC specification at electrical level, it is recommanded to avoid including any requirements for 3.0 Volts.

CT6 is not aware of specific electrical interfaces that ETSI SCP is considering for the new secure element, and if the existing UICC interface specified in TS 102 221[7] will continue to be used at all. In any case, if a specification for the electrical interface is defined, it is recommanded to consider also the addition of a new class that works below 1.8 Volts.

4.4.1.5 UICC access operations

In the existing UICC platform, there are several cases where the device needs to send multiple commands to perform what is logically a single operation. A good example for this is the access of the emergency numbers, stored in the USIM application. The terminal needs to first perform a SELECT command to retrieve the properties of the EF, such as the total number of records and the length of each record, and then needs to perform separate READ RECORD command for each record, regardless of the size of each one.

This access is inefficient in terms of delay and power, as it requires that the terminal is awake while it performs these operations, often waiting for the UICC to respond.

For this reason, SCP is encouraged to consider solutions that limit the number of commands required to access the content stored in the new secure platform, or to perform other operations.

4.4.1.6 Execution time

One of the aspects discussed in the recent years was the execution time of certain commands, as described in the LS C6-130181 that was sent to ETSI SCP. As a solution for the problem, the maximum power consumption of the UICC was increased starting with Rel.12.

A fast execution time of commands is an essential part for the new secure element. This is important not only to make sure that all procedures described by 3GPP are performed in a timely and correct way, but it also contributes to the overall power reduction, as the terminal needs to be awake waiting for a response from the UICC for a shorter time.

The execution time is a result of an optimsation between processor capabilities, power consumption and clock frequency. The current interface uses a clock provided by the ME. The power consumption that is allowed for the UICC is clearly defined, which is certainly required for the currently specified form factors for the UICC, especially the removable ones. Setting clear limits for the power consumption was necessary to ensure proper inter-operability.

With the integrated form factor, such inter-operability is not required, as the ME manufacturer is able to design the interface according to the requirements of the chosen secure platform and therefore an optimisation is possible.

Another aspect is the clock frequency. As said, in today's interface the clock is provided by the ME. An internal clock inside the secure platform would allow for faster execution.CT6 encourages SCP to consider solutions that minimize the execution time of commands sent to the new secure element, while still taking into consideration the requirements to save power.

4.4.2 Hardware flexibility

For many use cases in IoT, devices may be optimised in size, functionality and according to the specific needs of the IoT application they are intended for. Some devices may be very small, e.g. simple sensors and may have specific requirements related to size and power consumption.

For such devices it would be beneficial to have a flexible choice of form factor of a UICC that is optimally fitting to the design of such constraint devices. Due to the variety of IoT use cases a large variety of specialised device designs is envisaged. Aspects that are to be considered are for example the form factor, removability, the size, the location and number of contacts.

4.4.3 Electrical Interface and protocols

In several use cases for IoT it may also be beneficial for a device to not have to implement the current ISO interface to a UICC but rather rely on interfaces and protocols already in use inside the device. Examples of such interfaces are I2C or SPI.

Additional aspects to consider are:

- Number of wires
- Transmission speed
- Supply voltage
- Power efficiency (e.g. polling)

4.5 Toolkit4.5.0 Enhanced ability to make use of the ME capabilities

4.5.1 User-related applications

4.5.1.1 Interaction with user authentication

For Proximity Services the USIM may support the storage of Prose usage information. The Prose usage information is transmitted by the ME to the USIM via a dedicated ENVELOPE command, which requires the checking of the user verification status before it is performed and accepted by the USIM. There is today no standardised mechanism how the USIM could verify the user verification before processing a received USIM toolkit command.

The same issue appears within USIM toolkit applications that are designed in a way to require a user verification. Today this leads to the need to ask the user for entering again for example a PIN. It would be a more user friendly alternative to enable the application to check the status of a user verification that has been performed earlier and re-use this verification to perform the requested activity.

4.5.1.2 User Toolkit Menu

The User Toolkit Menu can be implemented by a toolkit application by using the proactive commands defined in ETSI TS 102 223 [8]. At the time these commands were defined, the MEs had a different way to get the user input and to display the information if it is compared to state-of-the-art MEs (e.g. higher resolution screen, color , touch enabled screen, etc...).

This results in that user toolkit menus used in the MEs do not provide the same user experience as applications running on these devices.

4.5.1.3 Timer

Timing features that may be used by a toolkit applet rely on the timer implementation of the ME. In some cases the timer functionality of the ME may not provide the accuracy that is required by the toolkit application as the precision of the event generated by the ME is not reliable (see ETSI TS 102 223 [8] clause 6.4.21). An internal timer in the UICC together with the capability of the UICC to initiate a proactive session as described in clause 4.5.2.1 would allow for a more reliable solution and enable applications in the UICC to act immediately on timer events.

Another aspect to consider is the certainty of the duration of the timer handled by the ME. An ME may extend or shorten the requested timer period without any possibility for the UICC to identify this. An internal timer in the UCC would provide a more secure source of information for UICC applications.

An internal timer in the UICC would also reduce the amount of commands that are currently required on the interface between UICC and ME to manage timers inside the ME and would therefore provide a more efficient solution in terms of power consumption and execution time.

4.5.2 System applications

4.5.2.1 Proactive commands

In the ME-UICC interface defined in the existing platform, the UICC plays a slave role in the communication with the ME in a way that the UICC cannot initiate by itself the communication with the ME in the case a command from the UICC to the ME is requested to be sent. To enable this case, it is defined in ETSI TS 102 223 [8] the command protocol in the CAT layer that enables the UICC to send the so-called proactive commands to the ME.

This requires the active intervention of the ME in order to give the chance to the UICC to be able to send a proactive command by sending periodically a STATUS command. This creates an additional exchange of commands that could potentially delay the execution of the proactive command by the terminal, thus limiting the extension of new potential features.

It would be beneficial if the new secure element supports interfaces providing remote wake up features e.g. as specified in ETSI TS 102 600 [11].

4.6 Concurrent operation of applications

The existing platform supports multiple applications on different channels, with the limitation of one command at a time. This may result in the interface to the card being blocked by one of these applications, potentially causing disruption in the operation of 3GPP applications.

For instance, some non-telecomunication applications require the execution of cryptographic algorithms that can potentially take a long time, sometimes in the order of tens of seconds. This possibility is supported by the standard, using NULL procedure bytes. The card can send NULL procedure bytes in order to request additional work waiting time and avoid that the transaction timer expires on the terminal.

It is critical and essential for the correct functionality of the terminal and of the telecomunication applications residing on the UICC that the interface between the terminal and the UICC is never blocked for a long time that exceeds a few seconds. Consequences of blocking this interface include, but are not necessarily limited to:

- User cannot originate any voice call or send any text messages due to the fact that the required call control ENVELOPE command cannot be sent to the UICC
- Network authentication cannot be executed and this has some very strict timing requirements
- User cannot access the content on the UICC (phonebook, SMS, ...)
- User cannot navigate the toolkit menu (even if menu is present in the UI of the UE)

5 Possible requirements resulting from existing features

It would be desirable if the new secure platform would support the features listed below:

- storage of large and complex configuration data.
- efficient access to large and complex configuration data in the sense that an ME does not need to read the complete content if only a part of the configuration data needs to be read at a time.
- fast transmission of data in the range of MBytes per second.
- flexible choice of form factor.
- flexible choice of electrical interface.
- flexible choice of protocol with larger payload.
- Provide a mechanism for the secure platform for 3GPP applications to initiate a proactive session with the ME.
- For applications on the secure platform, provide a mean to retrieve the user authentication status.
- Provide a mechanism for rich user interface for applications on the secure platform.
- Provide the capability for the secure platform to manage timers internally.

Depending on the use cases not all of the features listed above are required. A secure platform designed for a specific use case may require to support only a subset of the features listed above. The new secure platform should allow flexibility to create various combinations of features.

6 Possible new features

6.1 Introduction

This clause describes new features that are not specified in 3GPP but may be considered during the definition of a new secure platform.

6.2 Storage of data

6.2.1 The ability to provide the ME with storage space

With such feature the new secure platform could provide a possibility for a device to store specific data, for example sensitive information inside the new secure platform. This would require an efficient mechanism to transfer data in a fast, efficient and secure way. Such a mechanism needs to ensure that only the authorised entities can access the data.

6.2.2 The ability to provide the new secure platform with storage space in the ME

Such a feature would enable the new secure platform to make use of memory available in the ME. This can be data that is encrypted and therefore stored in a secure way or data that is not sensitive. Such a feature could allow new use cases which are currently not possible due to the resource limitations in current UICCs.

6.3 Extensibility of functionality

An update of part of or the whole Secure Platform functionality may be triggered by the need to extend the set of supported features. This includes:

- extension of the supported command set

6.4 Multiple application environment

Multiple applications may be hosted by the Secure Platform and may be active at the same moment in some deployments. Multiple non-telecommunication applications may be communicating at the same moment. Another case is when a network authentication is processed at the same moment as an over-the-air update is performed.

In such a situation, multiple non-telecommunication applications in addition to the Network Access Application may send or receive commands at the same moment in a time critical manner: For instance to perform authentication to their respective services or perform time critical transportation payment. An application cannot afford to wait for other applications to terminate their communications before starting or terminating the application's own transaction.

Consequently, it would be beneficial that

- Communication protocols on the secure platform allow multiple concurrent application sessions.
- The secure platform allows the execution of multiple applications that are time critical.
- The execution of an application does not prevent execution of another application.

Annex A:
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
		C6-160316				First draft	0.1.0
		C6-160396				Revision after first editing session in CT6 #81	0.2.0
		C6-170300				Revision after CT6 #84	1.0.0
		C6-170740				Revision after CT6 #86	2.0.0
2017-12	CT#78	C6-170740					15.0.0
2020-01						5G logo updated in a cover page as agreed in CT#86	15.0.1
2020-09	CT#89e	CP-202130	0001	-	F	Update of spec. reference	15.1.0