ETSI TS 122 112 V4.0.0 (2001-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS); USIM toolkit interpreter; Stage 1 (3GPP TS 22.112 version 4.0.0 Release 4)

Reference

DTS/TSGT-0322112Uv4

Keywords

UMTS

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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 http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://www.etsi.org/ipr).

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.

Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification has been produced by the 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 this TS, 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.

1 Scope

The present document specifies a system to make Mobile Operator services, based on USAT functionality and USIM based security functionality, available to an internet environment. This is achieved by specifying the necessary components and protocols for a secure narrow band channel between the internet application and an USAT Interpreter on the USIM. The actual application could be developed using the application language of choice. Two types of applications interfaces are used as examples, i.e., mark-up language based on WML and Remote Procedure Call (RPC).

The interpreter and the secure narrow band channel form a core platform to enable services like:

- Advanced security functionality, e.g., digital signatures in m-commerce applications
- Value added services based on position and roaming
- Controlled activation and management of other applications, e.g. multimedia and payment type of applications.

The secure narrow band channel is achieved by specifying the following:

- specific application and content related functionalities of the interface between the application system and the USAT Gateway;
- specific functionalities and protocols of the interface between the USAT Gateway and the USAT Interpreter associated with a USIM, achieved by defining a low level command set for interpretation by the USAT Interpreter;
- defined level of functionality available to the application server for the implementation of USIM based services such as PKI, location services, push and broadcast services, event based services, etc..

The present document does not specify any elements of the protocol stack between the application server and the USAT Gateway, the mark-up language definition, and the transport protocols between the USAT Gateway and the USAT Interpreter.

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 TS 03.48: "Security Mechanisms for the SIM application toolkit; Stage 2".

[2] 3GPP TS 02.48: " Security Mechanisms for the SIM application toolkit; Stage 1".

[3] 3GPP TS 31.111: "USIM Application Toolkit (USAT); Physical and logical characteristics".

3 Definitions and abbreviations

3.1 Definitions

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

application protocol: Protocol to convey data between the application system and the USAT Gateway.

end-to-end security: Secure content transfer between the Content System and the USAT Interpreter based on symmetric algorithms and/or asymmetric algorithms.

low level command set: A transport bandwidth and USAT Interpreter implementation efficient coding of the content.

Plug-in: Any other application or functionality resident on the USIM and accessible for the USAT Interpreter (regardless of the language used to implement the plug-in)

USIM: A 3G application on an IC card.

USIM session: link between the USIM and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the USIM

3.2 Abbreviations

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

FFS	For Further Study
GPRS	General Packet Radio Service
HTTP	Hypertext Transfer Protocol
M	Mandatory
ME	Mobile Equipment
O	Optional
PKI	Public Key Infrastructure
SMS	Short Message Service
SSL	Secure Sockets Layer
tbd.	To Be Defined
UCS2	Universal two byte coded Character Set
UE	User Equipment
URL	Uniform Resource Location
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
WML	Wireless Mark-up Language

4 General Requirements

The diagram below describes a system for dynamic content delivery via USAT. The following entities and protocols are defined:

Application System

- This entity is a collection of systems that utilise the USAT Interpreter for services requiring the usage of USIM specific services, e.g., security. The application system may contain keys for secure end-to-end content delivery.

Application to USAT Gateway Protocol (1)

- This protocol is HTTP. A mark-up language is typically used to convey the application, e.g., a WML deck. Where required, SSL may be used to secure this protocol.

USAT Gateway

- This entity converts between the "Application to USAT Gateway Protocol" and the "USAT Gateway to USAT Interpreter Protocol". This system may contain keys for secure transport delivery using GSM 03.48 [1].

USAT Gateway to USAT Interpreter protocol (2)

- This protocol defines a transport bandwidth and USAT Interpreter implementation efficient coding of the content. GSM 03.48 [1] shall be used as the underlying transport protocol.

Access Node / ME

- These entities provide the transparent transport of the USAT Gateway to USAT Interpreter content.

USIM with stored applications

- This entity contains pre-stored low level commands for interpretation by the USAT Interpreter. This is secured by the USIM security mechanisms.
- The pre-stored applications may be updated over the air (tbd.) or directly.

USIM with USAT Interpreter

- This entity converts USAT Gateway to USAT Interpreter protocol to local USIM commands. The local USIM commands could be USAT commands or other commands necessary, e.g., security commands, to execute the application. The USIM with USAT Interpreter may contain keys for both secure end-to-end content delivery and secure transport.

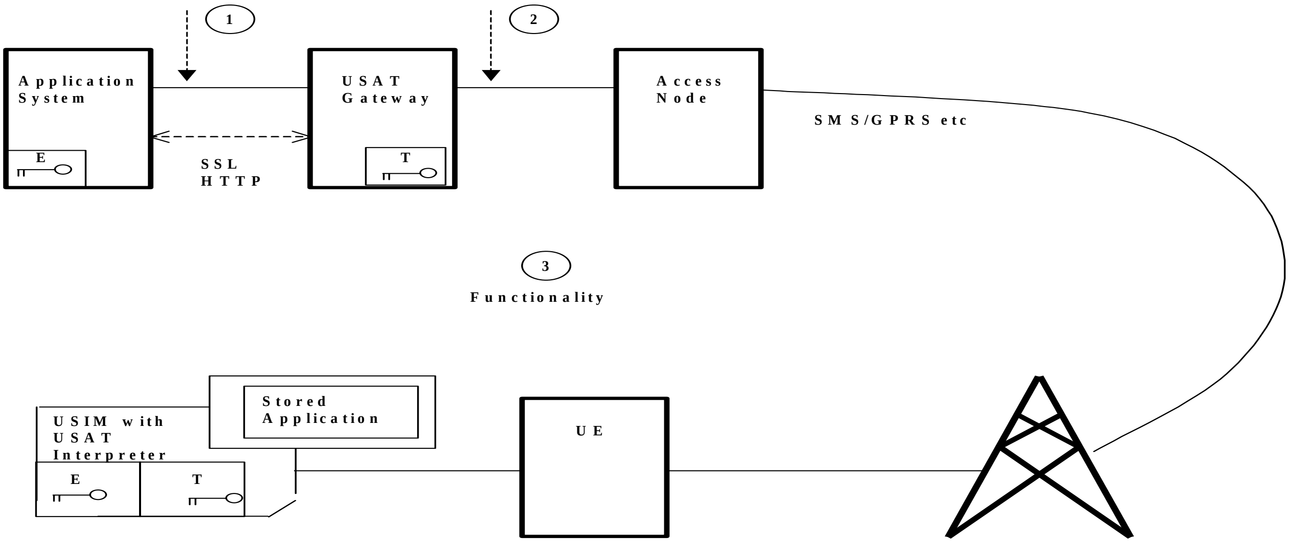

Figure 1: System Components

Functionality (3)

- End-to-end security based on symmetric algorithms, PKI, location services, event driven services, push, broadcast.

5 Component Requirements

5.1 Application System

This entity is a collection of systems that utilise the USAT interpreter for services requiring the usage of USIM specific services, e.g., security. A special case is the provision of dynamic content for delivery via USAT, e.g. web server or an application.

The application system may contain symmetric or asymmetric keys for secure end-to-end application delivery.

The application system shall provide an HTTP interface to the USAT Gateway.

5.2 USAT Gateway

The USAT Gateway converts between the "Application to USAT Gateway Protocol" and the "USAT Gateway to USAT Interpreter Protocol".

The USAT Gateway may contain keys for secure transport delivery using GSM 03.48 [1]. This system shall provide interfaces to the application systems and to the access nodes.

5.2.1 Blocking Mechanisms

The USAT Gateway shall be able to reject application containing forbidden functionality. Forbidden functionality is a set of functionality restricted on a application system basis or on an USIM basis. E.g., a restriction of functionality available could be made based on the level of trust of the application system or on the subscription type of the user.

The blocking mechanism generates an error as defined by the USAT Gateway error handling.

5.2.2 Error handling

When the USAT Gateway rejects user requested content, the subscriber shall be informed by the USAT Gateway.

Samples for possible error reasons are:

- not supported mark-up language tags;
- not supported attributes;
- bad message structure;
- security requirements not fulfilled;
- internal errors;
- rejection by busy USAT Interpreter;
- communication failure;

5.3 Access Node

This entity provides the transparent transport of the USAT Gateway to USAT Interpreter content. This can be SMS or GPRS or any other service available now or in the future, which is able to provide a transparent data channel to the USIM with USAT Interpreter.

5.4 Mobile Equipment

The mobile equipment provides the transparent transport of the USAT Gateway to USAT Interpreter content. For GPRS the ME decodes the IP-packets.

5.5 USIM with USAT Interpreter and stored applications

This entity converts USAT Gateway to USAT Interpreter protocol to local USIM commands. The local USIM commands could be USAT commands or other commands necessary, e.g., security commands, to execute the application. The USAT Interpreter shall use the commands defined in TS 31.111 [2] to communicate with the ME. The USIM with USAT Interpreter may contain keys for both secure end-to-end application delivery and secure transport.

It shall provide memory space for locally stored translated applications.

The USAT Interpreter shall be configurable to allow or deny the execution of specific low level commands.

The USAT Interpreter can be triggered either

- locally from the ME, as a result from a menu selection,
- locally from the ME, as a result from an event,
- by an incoming page as a result from a previous URL request from the USAT Interpreter, or
- by an incoming page initiated by an application system (push).

A caching mechanism may be used by the USAT Interpreter.

The USAT Interpreter shall provide a generic interface to support all USAT commands.

The following table describes the list of additional functionality to be provided by the USAT Interpreter:

Table 1: Additional USAT Interpreter functionality

DESCRIPTION	M/O/FFS
Support mark-up language mediation	
Go (branching to a URL)	M
Variables (referencing, substituting,…)	M
Support of different variable types, including type checking and type conversion	M
Supported types of variables	FFS
Soft-Key support (e.g. Do tags)	M
Minimum Navigation Units: Cards and Decks (or similar for non-WML mark-up languages)	M
Navigation:	
- Go homepage (specific URL)	M
- Go Back	M
This function is depending of the current context and can result in:	
- Restart current Navigation Unit	
- Step back previous Navigation Units	
- Go back (history functionality of visited URLs during the current USIM session)	
- Exit	M
- Help	O
Processing commands	
Unconditional branching (forward and backward)	M
Conditional branching	M
Concatenation of strings	M
String Extraction	M
Environment variables (USIM/USAT/USAT Interpreter platform information available to all services)	M
Variable value sharing between decks/pages (or similar for non-WML mark-up languages) within a session	M
Permanent variable value sharing between sessions and applications	M/O
Execution of locally stored translated content	M
Ciphering / Authentication	
End-to-End security based on symmetric algorithms	O
End-to-End security based on asymmetric algorithm schemes	O
Plug-In	
Execution of an external function	M
UCS2 Support	O
Bookmark storage of the current page on	
- USAT Gateway or	O
- locally at USAT Interpreter by the end user	O
Support for caching	M/O
Session features	O
Session indication	M

6 Protocol requirements

6.1 Application to USAT Gateway protocol

The transmission protocol is HTTP. The application protocol used to convey content is a scripting or mark-up language. An example for an appropriate application protocol would be WML.

SSL is an example to be used to securely move applications between the application system and the USAT Gateway.

6.2 USAT Gateway to USAT Interpreter protocol

This protocol defines a transport bandwidth and USAT Interpreter implementation efficient coding of the application content.

6.2.1 Transport requirements

The protocol shall be specified bearer independent. It shall be based on GSM 03.48 [1], where the USAT Gateway is the sending application and the USAT Interpreter is the receiving application or vice versa.

At least, the following transport mechanisms shall be supported:

- SMS-PP (Single Short Message Point to Point and Concatenated Short Message Point to Point)

Other transport mechanisms are optional.

There shall be support for indicating usage of sessions.

The security mechanisms and recommended combinations of the security mechanisms shall be based on GSM 02.48 [2]. At least one of the listed authentication mechanisms shall be used for this protocol.

6.2.2 Coding requirements

The coding of the content transported within this protocol shall be bandwidth efficient. The coding shall be independent from the transport bearer and from the platform used for the USAT Interpreter.

The coding shall be easily extendable by further commands. It shall easily be limitable to a configurable set of USAT functionality.

6.2.3 Functional requirements

6.2.3.1 USAT command functionality

The USAT Gateway to USAT Interpreter Protocol shall support all current and all future USAT commands defined in TS 31.111 [3].

Some commands may have optimised coding.

6.2.3.2 Non USAT command functionality

The following set of non USAT functionality shall be supported:

Table 2: Non USAT command functionality

DESCRIPTION	M/O/FFS
Support mark-up language mediation	
Go (branching to a URL)	M
Variables (referencing, substituting,…)	M
Soft-Key support (Do tags)	M
Navigation Units, e.g. Cards and Decks	M
Navigation shortcuts, e.g. Go Home, Go Back (history functionality of visited URLs), Exit and Help	M
Processing commands	
Unconditional branching	M
Branching according to user input	M
Concatenation of strings	M
Environment variables (USIM/USAT/USAT Interpreter platform information available to all services)	M
Permanent variables (information related / available to dedicated services)	FFS
Ciphering / Authentication	
End-to-End security based on symmetric algorithms	M
End-to-End security based on asymmetric schemes	M
Plug-In	
Execution of an external function	M
UCS2 Support	M
Bookmark	
- Bookmark storage of the current page on USAT Gateway or	FFS
- locally at USAT Interpreter by the end user	FFS
Support for caching	M
Session features	O
Session indication	M
Interaction with WAP browser on the ME	FFS

6.3 Application System to USAT Interpreter protocol

This protocol is used to make secure services between the application system and the USAT Interpreter possible (e.g. like login of the user into a content server, keep SSL sessions between USAT Gateway and content system alive).

Variable handling can be more effective.

This protocol is FFS.

If this protocol is needed it will have an impact on the USAT Interpreter to USAT Gateway protocol.

6.4 Administration protocol

The administration protocol shall be used independently from the USAT Gateway to USAT Interpreter protocol.

The administration protocol shall define USAT Interpreter specific administrative commands including a separate administration security and leave the storage of data up to the implementation of the USAT Interpreter.

The administration functionality shall be able to:

- download low level command sets independent from the transport layer;
- download dormant low level command sets; tbd.
- add and delete low level command sets;
- handle the generation of menu entries, especially it shall be possible to reference one low level command set by more than one menu item;
- uniquely identify every low level command set

Table 4: Administration

DESCRIPTION	M/FFS
Administration	
Remote File Management according to GSM 03.48 [1]	O
Set Up Menu administration	M
Plug-in administration	M
Download low level command sets independent from the limitations of the transport layer;	M
Download dormant low level command sets; tbd.	M
Add and delete low level command sets;	M
Handle the generation of menu entries, especially it shall be possible to reference one low level command set by more than one menu item;	M
Uniquely identify every low level command set	M

7 Functional requirements of the USAT Interpreter

7.1 End-to-end security

The USAT Interpreter shall provide means for end-to-end security between the Content System and the USAT Interpreter based on symmetric algorithms and/or asymmetric algorithms.

End-to-end security shall include means for:

- Key management / key generation
- Certificate management
- Selection of algorithms and security features
- Integrity of the content
- Integrity of message sequence
- Confidentiality of message contents
- Authentication / Signing of messages
- Authentication of the user
- Mechanisms against replay attacks

All mechanisms may be combined.

7.2 Location services

The USAT Interpreter shall provide means to support Location Services by providing an interface to the Provide Local Information command as defined in TS 31.111 [3] (see chapter 5.5).

The location information shall be provided to the application system in a tbd.

7.3 Event driven services

The USAT Interpreter shall provide means to react on events monitored by the ME or the USIM. The following events shall be supported:

- all events defined in 3GPP TS 31.111 [3].
- USAT initialisation procedure as defined in TS 102 221 [4].
- Timer expiration as defined in 3GPP TS 31.111 [3].

On occurrence of an event the USAT Interpreter shall run locally stored translated applications (USAT Interpreter low level command set).

The USAT Interpreter shall provide means to setup and clear the list of monitored events and modify which locally stored translated applications to run, when the event occurs.

Locally stored translated applications to run, when the event occurs, shall be downloaded by the Administration Protocol as described in chapter 6.4.

7.4 Push

Push messages contain an incoming page addressed to the USAT Interpreter containing low level commands to be executed. Push is initiated by the Application system and not by a user action.

The USAT Interpreter shall support the following two use cases:

- immediate execution of the received Push;
- delayed execution of the received Push.

The USAT Interpreter may reject a Push, when not able to execute or store it.

7.5 Cell Broadcast

A low level command set can be received via cell broadcast messages.

For cell broadcast messages containing low level command sets the USAT Interpreter shall provide:

- means to execute the received low level command set;
- separate security mechanisms;
- separate configuration parameters.

Annex A (informative): Change history

The table below indicates all change requests that have been incorporated into the present document since it was initially approved by 3GPP TSG-T.

Change history								
Date	TSG #	TSG Doc	CR	Rev	Cat	Subject/Comment	Old	New
2001-03	TP-11	TP-010042				Version 2.0.0 was approved at TSG-T #11	2.0.0	4.0.0

History

Document history		
V4.0.0	March 2001	Publication