3GPP TS 31.112 V8.0.0 (2009-02)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module Application Toolkit (USAT) interpreter architecture description (Release 8)

Keywords
USIM, Toolkit, LTE

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 Specification (TS) 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.

1 Scope

The present document defines the stage 2 description for the USAT Interpreter system. As the second stage of a three-level structure, it is derived from the stage 1 service description.

The present document defines the overall architecture for the USAT Interpreter system:

- Role models;
- System architecture;
- Function and information flow.

The stage 3 documents shall conform to the present document.

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 31.111: "USIM Application Toolkit (USAT)".

[2] 3GPP TS 31.113: "USAT Interpreter Byte Codes".

[3] 3GPP TS 31.114: "USAT Interpreter Protocol and Administration".

[4] 3GPP TS 23.048: "Security Mechanisms for the (U)SIM Application Toolkit; Stage2".

3 Definitions and abbreviations

3.1 Definitions

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

Access Node: entity that provides the transparent transport of the USAT Gateway to USAT Interpreter content

Application Provider: entity that defines services using USAT Interpreter functionality

Application System: entity that is a collection of Application Providers that utilise the USAT Interpreter for services requiring the usage of USIM

Gateway: network program that translates from a source language to the USAT Interpreter byte codes

NOTE 1: The gateway resides between the application provider's server that contains pages written in the source language and a USIM containing the USAT Interpreter that will render these pages.

Gateway Selector: entity in the system architecture that decides which gateway shall be used to exchange user data

Master Application Provider: entity that has the capability to act as a proxy between the Service Access Provider and the Application Providers that do not connect directly to the Service Access Provider.

Page: the context of a USAT Interpreter rendering, the scope of USAT Interpreter variables and the unit of transmission between the Gateway and a USIM containing the USAT Interpreter

NOTE 2: Pages exist in source code form expressed in a mark-up language and in compiled form as USAT Interpreter byte codes.

Post mode: data transmission from the USAT Interpreter and the Application Provider triggered by the USAT Interpreter

NOTE 3: The USAT Interpreter does not expect a related reply in this mode.

Pull mode: data exchange between the USAT Interpreter and the Application Provider triggered by the USAT Interpreter

NOTE 4: The USAT Interpreter does expect a related reply in this mode by entering the Wait State.

Push mode: data transmission between the USAT Interpreter and the Application Provider triggered by the Application Provider

NOTE 5: In the Push Mode information is received by the USAT Interpreter without an explicit preceding request as in the Pull Mode.

Security Node: entity that provides security mechanisms according to TS 23.048 [4].

Service: collection of pages that defines an unitary capability of the user equipment from the point of view of the user

NOTE 6: Examples include remote database access, electronic mail, and alerts.

Service Access Provider: entity in the role model that provides connectivity between the 3G operator and the Application System

Wait State: state which is entered by the USAT Interpreter in Pull Mode to wait for a response

3.2 Abbreviations

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

GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio System
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
OSI	Open System Interconnection
RFC	Request For Comments
SMS	Short Message Service
SSL	Secure Socket Layer as defined in a RFC
TAR	Toolkit Application Reference
TS	Technical Specification
UE	User Equipment
URL	Uniform Resource Locators
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module

4 Main concept

4.1 USAT Interpreter system definition

The USAT Interpreter System allows Application Systems to use an USAT Interpreter for services requiring the usage of USAT (refer to TS 31.111 [1]) specific functionality.

4.2 Role model

The role model gives an architectural overview of the requirements for USAT Interpreter systems.

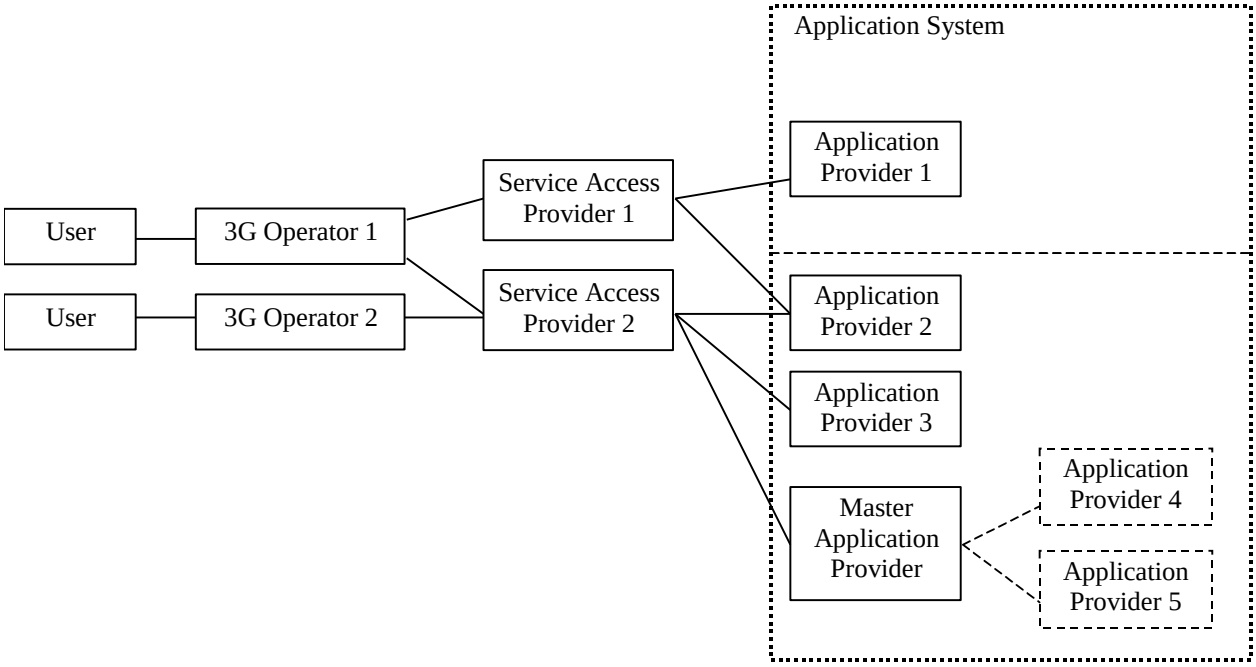


Figure 1: USAT Interpreter role model

The user has the USAT Interpreter installed on his USIM and uses the USAT Interpreter to gain access to applications that reside in the Application System.

The 3G Operator is the entity that provides 3G-network connectivity to the user.

The Service Access Provider is the entity that provides connectivity between the 3G-operator network and the application system. The Service Access Provider can be either the same 3G operator or another party. The Service Access Provider can be shared between several 3G-operators.

The Application System provides the applications that are made available to the user through the system and the USAT Interpreter. The application system can be owned either by the operator or by another party, either completely or partially. It is also possible from an architecture point of view to provide access to the same Application Provider through different operators and Service Access Providers.

The Master Application Provider acts as a proxy between the Service Access Provider and Application Providers that do not connect directly to the Service Access Provider. From the Service Access Provider, the Master Application Provider acts just as a regular Application Provider. The Master Application Provider can have the capability to translate between application languages and protocols.

The role model puts no limitation on the number of different 3G Operators, Service Access Providers or Application Providers.

4.3 USAT Interpreter System Architecture

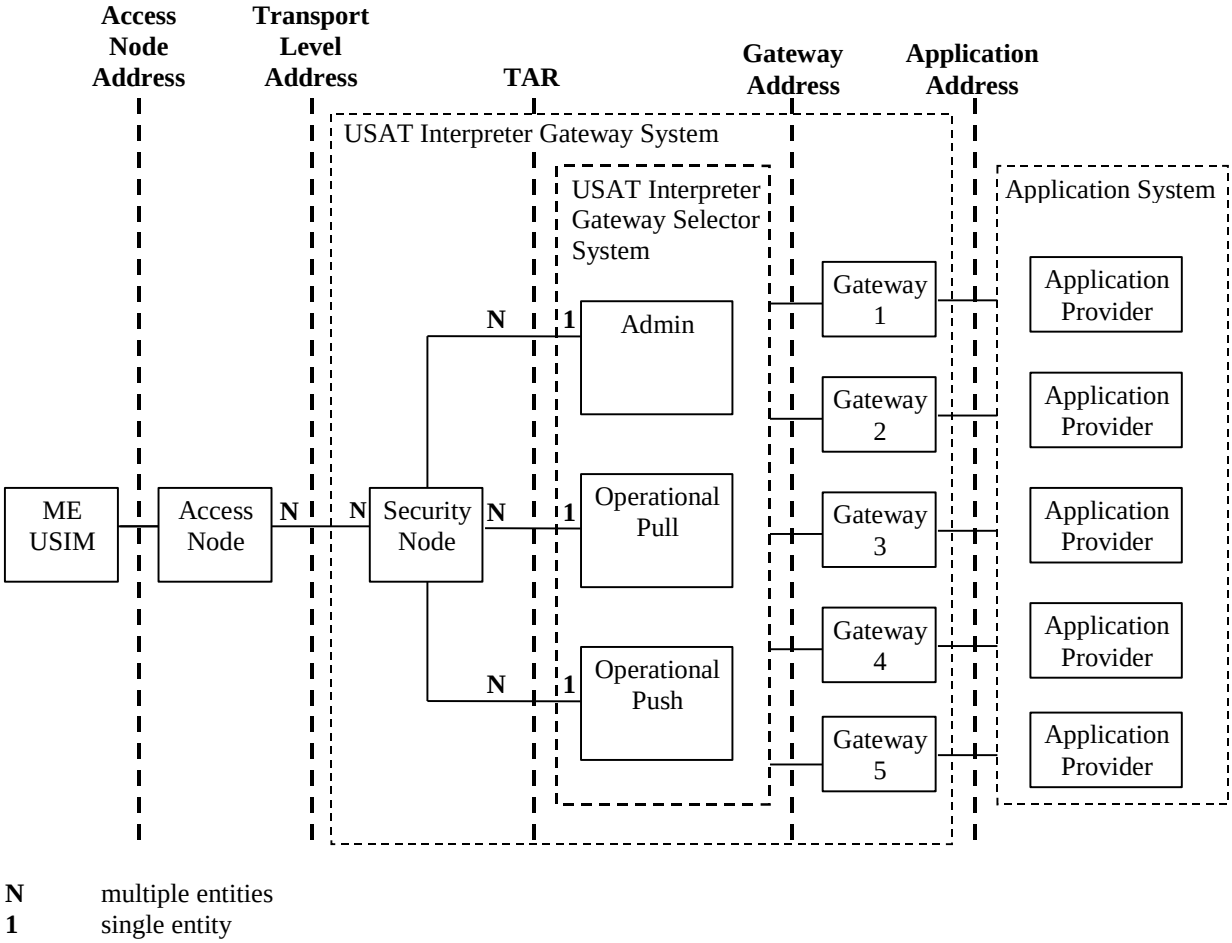


Figure 2: System Architecture

The Access Node is the network entity that provide the transport layer specific connectivity to the Security Node as specified in TS 23.048 [4]. The Access Node can be connected to any number of different Security Nodes.

The bearer type determines the access node. For example in the case where SMS is the bearer, the Access Node would be an SMSC. In GPRS the Access node would be a GGSN. The Access Node is addressed according to the bearer's addressing principle. The user reaches the Access Node using the Service Center Address if the bearer is SMS. If the bearer is IP, the user addresses the Access Node using its IP Address.

The Security Node is the entity that terminates the 23.048 protocol. The Security Node is addressed according to the used bearer. For example in the case where SMS is used as bearer, the Access Node addresses the Security Node using the Destination Address. In the case where the bearer is IP, the IP Port addressing is used to reach the Security Node.

The Gateway Selector is the entity that subscribes to data from the Security Node based on TAR value and is responsible for connecting the data flow into the appropriate Gateway for the application that is addressed.

The Gateway Selector System consists of logically separate Gateway Selectors to handle the different types of access. These are Administrative, Operational Pull and Operational Push Access. The distinction between these is made using separate TAR value ranges. Thus, one TAR value range is reserved for each of these three different access types. The TAR value ranges are specified in TS 31.114 [3].

The Gateway is the entity that has the capability to encode and decode data between the formats used by the application system and the USAT Interpreter byte codes. The Gateway terminates the operational layer of the protocols. One Gateway potentially handles only a limited set of conversions from Application encoding to USAT Interpreter byte codes. There might be Gateways for dedicated purposes that can be addressed using the Gateway Address. Examples can be separate Gateways for banking, different application languages, content types etc.

The Gateway Selector addresses the Gateway using the Gateway Address. The Gateway Address is defined in the Operational Layer, which is described later on in the present document. If no Gateway Address is specified, the Gateway Selector addresses the default Gateway. The Gateway addresses the application using URLs or whatever addressing is implied by the applications that the Gateway handles.

The logical combination of Security Node, Gateway Selector and Gateway is called the USAT Interpreter Gateway System.

The picture shows a generic architecture. The entities depicted above need not be physically separate. It is possible to integrate several of the logical entities into the same physical entity.

The Security Node can be placed either in the operator domain or in the Application Provider domain. This is a deployment choice to be made for the system. The decision on where to put the Security Node will be influenced by security considerations and other aspects.

Whether or not the USAT Interpreter has the capability of addressing only one or several Security Nodes is also a deployment choice to be made by the 3G operator.

The Application System consists of Application Providers. The addressing of these is defined at the application level and beyond the scope of the present document. The entities in the Application need to adhere to the security architecture as specified in clause 5.2 in the present document in order to provide end-to-end security.

4.4 Protocol layers

USAT Interpreter System Architecture is based on the OSI model as described in figure 3. All layers have own functionality and are thus independent of each other.

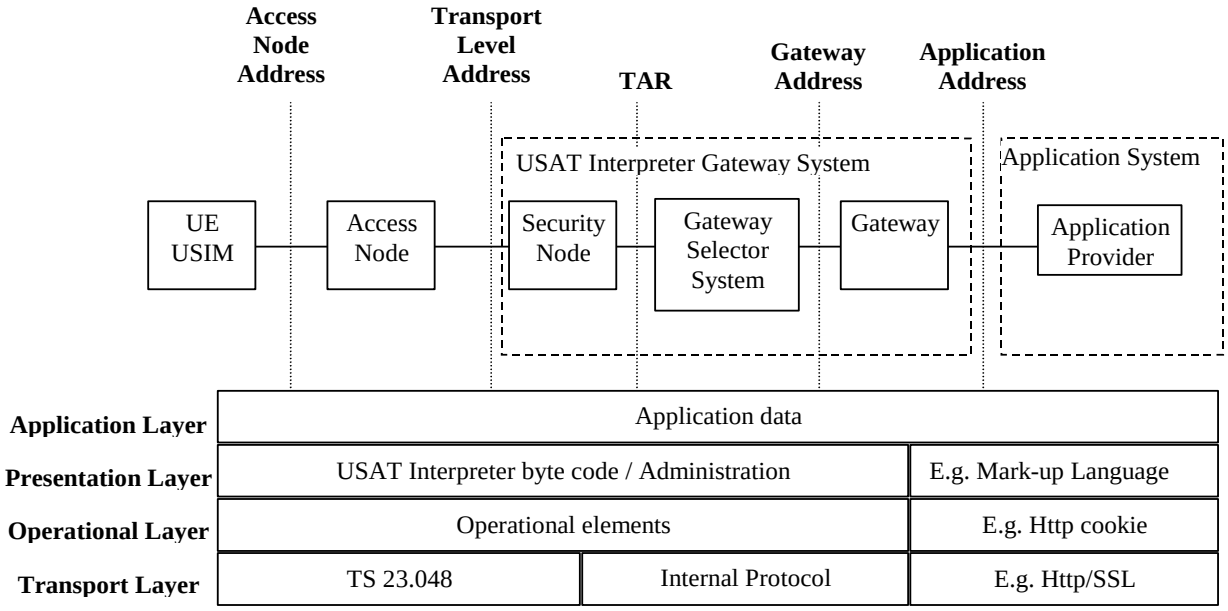


Figure 3: USAT Interpreter Layer protocol layers

4.4.1 Transport layer

The Transport layer between the USAT Interpreter and the Security Node is specified in TS 31.114 [3].

The Transport layer between the Security Node and the Gateway is internal functionality in the USAT Interpreter Gateway System thus it is not specified in the present document.

The transport layer between the Gateway and the Application Provider is beyond the scope of the present document. For example, http can be used.

4.4.2 Operational layer

The operational layer defines the message flow between the USAT Interpreter and the Gateway. The Gateway address is included in the operational layer header.

An operational layer between the Gateway and the Application provider is beyond the scope of the present document. It may include application specific data for state information and other context information. An example could be http cookies in the case where http is used.

The only mode for the operational layer is the transaction-based mode.

The transaction-based mode consists of single request-response pairs between the USAT Interpreter and the Gateway.

The transaction-mode:

- handles two states of each party: idle and waiting-for-response;
- does not define an own set of commands;
- is context free.

Transaction mode between the USAT Interpreter and the Gateway is a mandatory feature.

The transaction-based mode does not provide message context for a sequence of messages. In this mode, if such a context is needed, this has to be provided on the application layer.

4.4.3 Presentation layer

The Presentation layer between the USAT Interpreter and the Gateway consists of the USAT Interpreter byte code and administration as specified in the specifications TS 31.113 [2] and TS 31.114 [3] respectively. The Presentation layer provides way to support end-to-end security, data exchange, user interaction etc.

A Presentation layer between the Gateway and the Application provider is beyond the scope of the present document. It may consist of a mark-up language.

4.4.4 Application layer

The Application layer consists of the data transferred between the USAT Interpreter and the Application Provider. End-to-end security could be supported on the Application layer but relies on the interface provided by the Presentation layer.

The Application is functionality that provides services to the user. Examples can be banking, gambling, trading applications etc. The Application layer may consist of any data defined by the application and is beyond the scope of the present document.

5 Security functionality in the USAT Interpreter System

One of the main requirements of the USAT Interpreter is the security functionality. Transport layer security is offered between different USAT Interpreter System components. The end-to-end security is offered between the USAT Interpreter and the Application provider.

5.1 Transport Layer Security

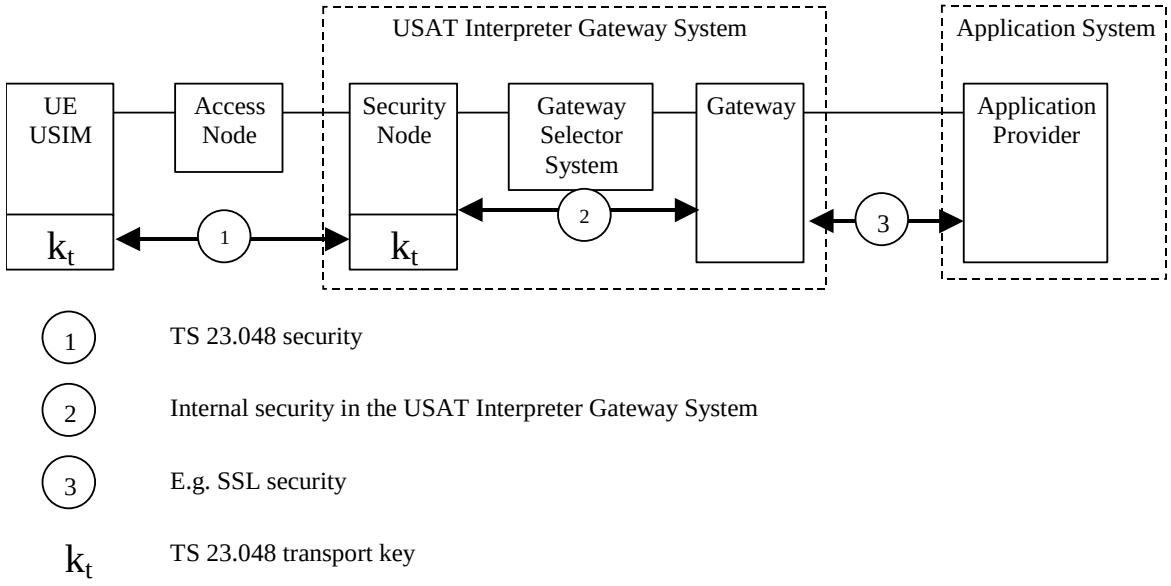


Figure 4 USAT Interpreter Transport Layer Security Model

The transport layer security is provided by three independent point-to-point protocols. On the link between the USAT Interpreter and the Security Node transport security according to TS 31.114 [3] shall be used.

The transport layer security on links number 2 and 3 in the picture are beyond the scope of the present document. On the link between the Security Node and the Gateway, some internal security should be used. On the link between the Gateway and the Application system, some security should be used. For example, SSL may be used on this link.

5.2 End-to-end Security

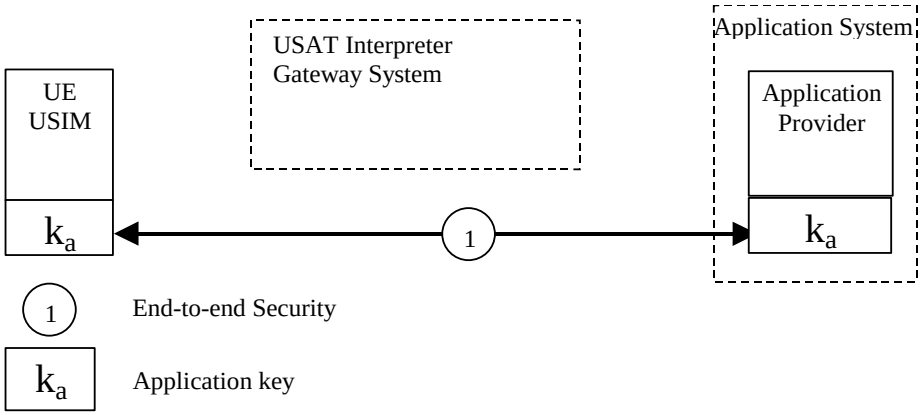


Figure 5: USAT Interpreter End-to-end Security model

End-to-end security is provided between the USAT Interpreter and the Application system (application layer security). End-to-end infrastructures based on both symmetric and asymmetric cipher algorithms can be supported by the USAT Interpreter system.

Byte codes to manage end-to-end security are specified in TS 31.113 [2]. These byte codes shall provide means for:

- Key identification;
- 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.

The Application system shall provide means to manage end-to-end security, however this is beyond the scope of the present document.

5.2.1 Symmetric Security

The symmetric end-to-end security on the application layer is specified in TS 31.113 [2].

5.2.2 Asymmetric Security

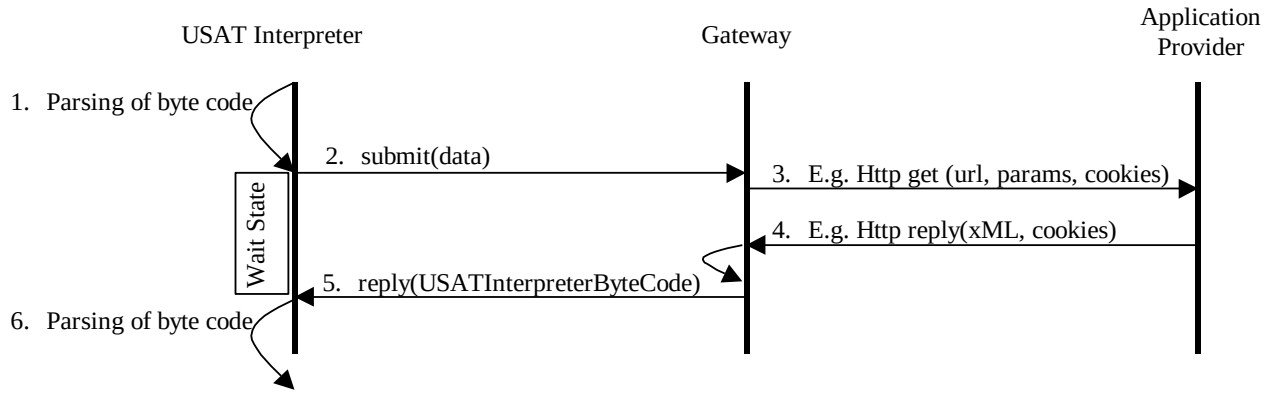
The asymmetric end-to-end security on the application layer is specified in TS 31.113 [2].

6 Modes of Operation

This clause describes possible basic information flows between the USAT Interpreter and the Application Provider. These basic modes of operation may be combined to run a complete service.

6.1 User Triggered Transaction Flow – Pull mode

The following figure gives an example for a data exchange in the pull mode.



1. The USAT Interpreter has been activated and is rendering byte codes.
2. After the USAT Interpreter has rendered a byte code requiring the Pull Mode, the USAT Interpreter shall send information using the transmission protocol (refer to TS 31.114 [3]) to the Gateway and enter Wait State.
3. The Gateway shall interpret the information previously received from the USAT Interpreter and then forward this information to the Application Provider.
4. The Application Provider optionally replies data after the interpretation of the information received from the Gateway. In the given example, where the Http protocol is used, the data reply of the Application Provider is mandatory.
5. The Gateway replies with byte codes for the USAT Interpreter according to TS 31.113 [2] using the transmission protocol (TS 31.114 [3]).
6. If the byte code reply is related to the request the USAT Interpreter renders the received byte codes. In the given example, where the Wait State is still active, the byte code reply of the Gateway is rendered.

Figure 6: USAT Interpreter Pull Flow

Wait State

- After the USAT Interpreter has rendered a byte code requiring the Pull Mode, the USAT Interpreter shall enter the Wait State.
- Pull Mode replies received by the USAT Interpreter not being in the Wait State shall be discarded.
- The user shall be made aware by the USAT Interpreter that the USAT Interpreter is in the Wait State. I.e. a user notification shall be displayed.
- The user notification shall be customisable by administrative means and by the Application Provider.
- The user shall be able to exit the Wait State of the USAT Interpreter. I.e. the user shall be able to cancel a submitted request to the Gateway. This fact does not imply that the Gateway gets a message that the request was cancelled by the user.
- After the user has exited the Wait State of the USAT Interpreter, it shall be possible to continue rendering pages. I.e. the user shall be able to submit e.g. another request.

The following figures show that Pull Mode replies are discarded, if a the Wait State has been cancelled on user request.

The Pull Mode reply is discarded by the USAT Interpreter, if it is received during the rendering of USAT Interpreter byte codes.

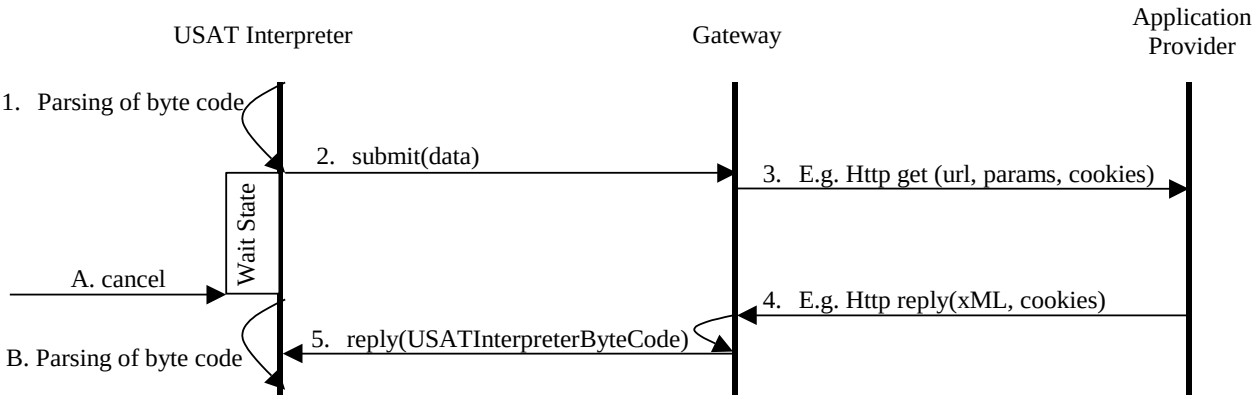


Figure 7: Reply ignored, if received during parsing of byte code

1. The USAT Interpreter has been activated and is rendering byte codes.
2. After the USAT Interpreter has rendered a byte code requiring the Pull Mode, the USAT Interpreter shall send information using the transmission protocol (TS 31.114 [3]) to the Gateway and enter Wait State.

parallel and independent processing:

A. The USAT Interpreter exits the Wait State on user request.	3. The Gateway shall interpret the information previously received from the USAT Interpreter and then forward this information to the Application Provider.
B. Dependent on the user interaction the USAT Interpreter renders byte codes. In the given example, where the user has chosen to render a page, the byte code of the respective page is rendered.	4. The Application Provider optionally replies data after the interpretation of the information received from the Gateway. In the given example, where the Http protocol is used, the data reply of the Application Provider is mandatory.
	5. The Gateway replies with byte codes for the USAT Interpreter according to TS 31.113 [2] using the transmission protocol (TS 31.114 [3]). This reply shall be discarded by the USAT Interpreter, because the related request has been cancelled before by the user.

The response shall be discarded by the USAT Interpreter, if it is received after entering another Wait State.

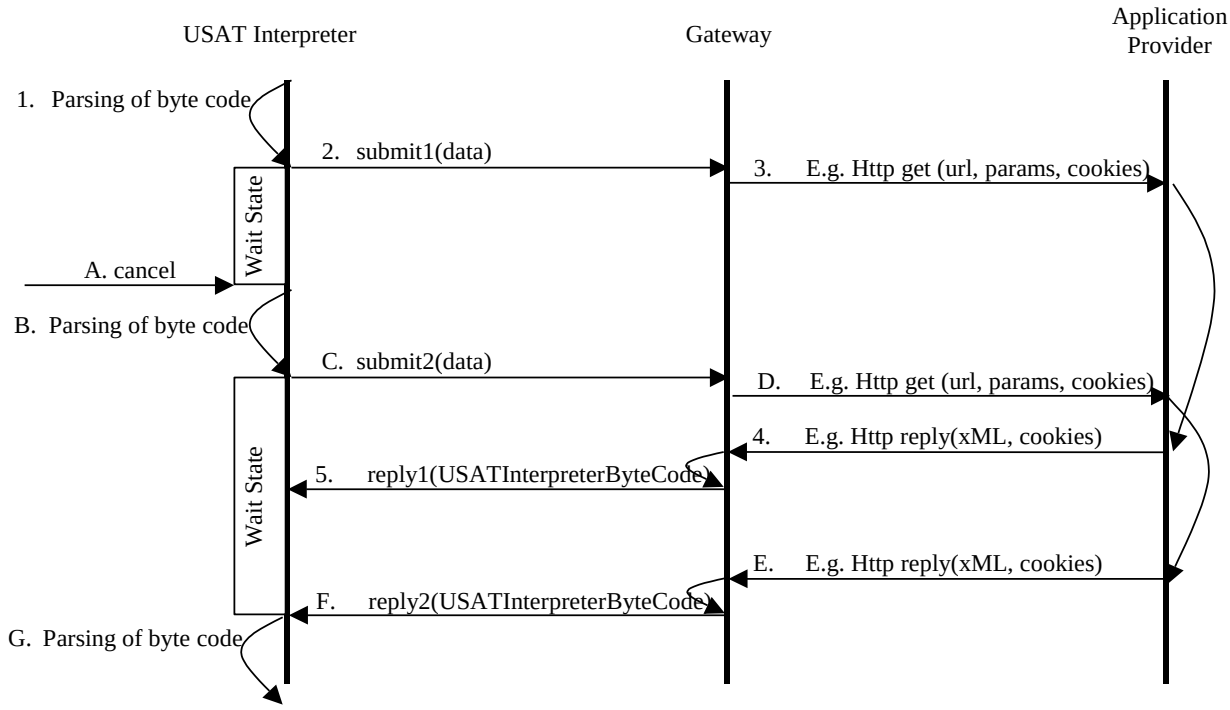


Figure 8: Reply ignored, if received during the wait state of the USAT Interpreter

1. The USAT Interpreter has been activated and is rendering byte codes.

parallel and independent processing:

2. After the USAT Interpreter has rendered a byte code requiring the Pull Mode, the USAT Interpreter shall send information using the transmission protocol (TS 31.114 [3]) to the Gateway and enter Wait State.	A. The USAT Interpreter exits the Wait State on user request. The USAT Interpreter has been in the Wait State before. Depending on the user interaction the USAT Interpreter renders byte codes. In the given example, where the user has chosen to render a page, the byte code of the respective page is rendered.
3. The Gateway shall interpret the information previously received from the USAT Interpreter and then forward this information to the Application Provider.	B. Parsing of byte code
4. The Application Provider optionally replies data after the interpretation of the information received from the Gateway. In the given example, where the Http protocol is used, the data reply of the Application Provider is mandatory.	C. After the USAT Interpreter has rendered a byte code requiring the Pull Mode, the USAT Interpreter shall send information using the transmission protocol (TS 31.114 [3]) to the Gateway and enter Wait State.
5. The Gateway replies with byte codes for the USAT Interpreter according to TS 31.113 [2]using the transmission protocol (TS 31.114 [3]). This reply shall be discarded by the USAT Interpreter, because the related request has been cancelled before by the user.	D. The Gateway shall interpret the information previously received from the USAT Interpreter and then forward this information to the Application Provider.
	E. The Application Provider optionally replies data after the interpretation of the information received from the Gateway. In the given example, where the Http protocol is used, the data reply of the Application Provider is mandatory.
	F. The Gateway replies with byte codes for the USAT Interpreter according to TS 31.113 [2] using the transmission protocol (TS 31.114 [3]).
	G. If the byte code reply is related to the request, the USAT Interpreter renders the received byte codes. In the given example, where the Wait State is still active, the byte code reply of the Gateway is rendered.

6.2 Network Triggered Transaction Flow – Push mode

The following figure gives an example for a data transmission in the Push Mode.

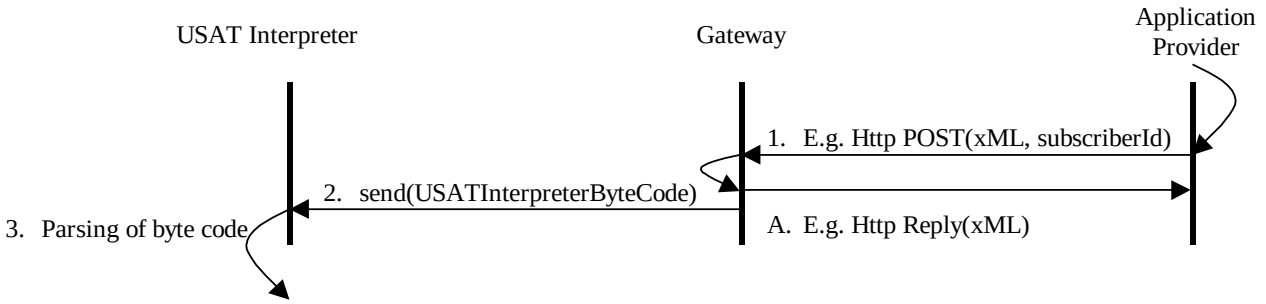


Figure 9: USAT Interpreter Push Flow

1. The Application Provider requests the Gateway to send byte codes to the USAT Interpreter. In the given example, this request uses Http.

parallel and independent processing:

2. The Gateway sends byte codes to the USAT Interpreter using the transmission protocol for Push messages (TS 31.114 [3]).	A. The Gateway sends a reply to the Application Provider, because in the given example Http is used.
3. The USAT Interpreter renders the received byte codes. In the given example, where no blocking conditions are defined, the delivered byte code from the Gateway is rendered.	

The blocking mechanisms for Push Mode and handling of Push messages by the USAT Interpreter and the USAT Interpreter Gateway System are FFS.

6.3 USAT Interpreter triggered transaction flow – Post mode

The following figure gives an example for a data transmission in the Post Mode.

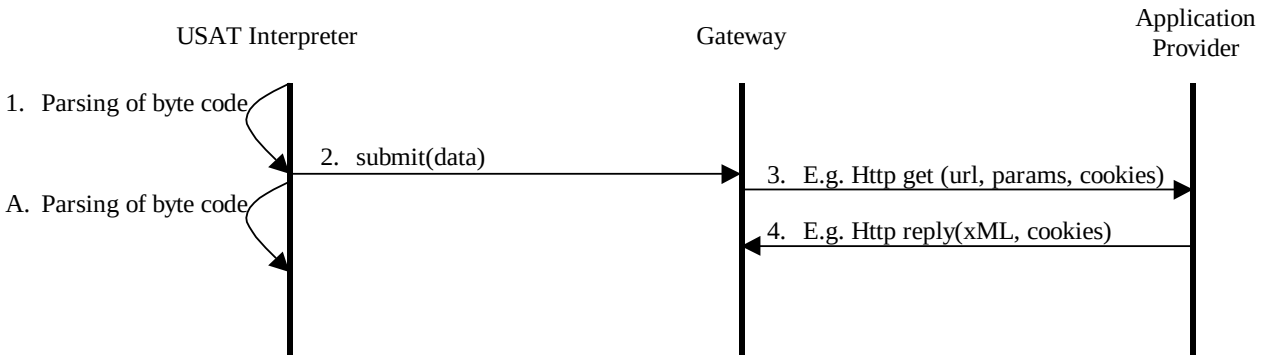


Figure 10: USAT Interpreter Post Flow

1. The USAT Interpreter has been activated and is rendering byte codes.
2. After the USAT Interpreter has rendered a byte code requiring the Post Mode , the USAT Interpreter shall send information using the transmission protocol (TS 31.114 [3]) to the Gateway. The USAT Interpreter will continue rendering byte codes.

parallel and independent processing:

	3. The Gateway shall interpret the information previously received from the USAT Interpreter and then forward this information to the Application Provider.
A. The USAT Interpreter continues to render byte codes in the current page.	4. The Application Provider optionally replies data after the interpretation of the information received from the Gateway. In the given example, where the Http protocol is used, the data reply of the Application Provider is mandatory. The Gateway will not send any related reply to the USAT Interpreter.

6.4 Administrative mode

The following figure gives an example for a data exchange in the administrative mode.

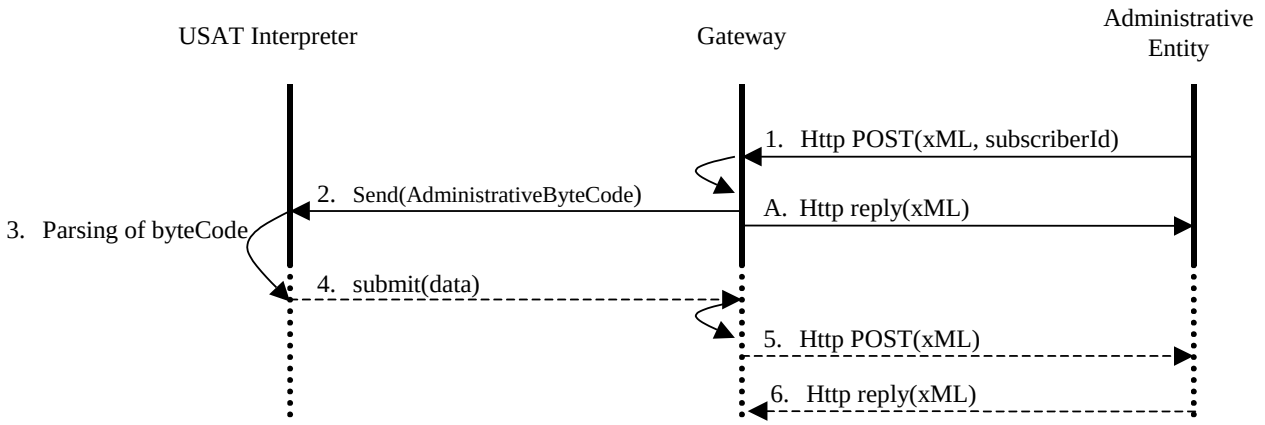


Figure 11: USAT Interpreter Administrative Flow

1. The Administrative Entity requests the Gateway to send administrative byte codes to the USAT Interpreter. In the given example, this request uses Http.

parallel and independent processing:

2. The Gateway sends administrative byte codes to the USAT Interpreter using the transmission protocol for administrative messages (TS 31.114 [3]).	A. The Gateway optionally replies data after the interpretation of the information received from the Administrative Entity. In the given example, where the Http protocol is used, the data reply of the Gateway is mandatory.
3. The USAT Interpreter renders the received administrative byte codes. In the given example, where no blocking conditions are defined, the delivered administrative byte code from the Gateway is rendered.	
4. If the USAT Interpreter encounters a reply request within the administrative byte codes, the USAT Interpreter shall send information using the transmission protocol (TS 31.114 [3]) to the Gateway.	
5. The Gateway shall process the information previously received from the USAT Interpreter and then forward the resulting information to the Administrative Entity.	
6. In the given example, where the Http protocol is used, the Http reply to the Administrative Entity is mandatory.	

The logic of the administrative flow is similar to the Push Mode from the previous clause. The difference is that the USAT Interpreter is addressed through a TAR value range that has been reserved for administrative commands. The behaviour of the administrative mode depends on the state of the USIM Interpreter at reception of the USAT Interpreter byte code.

Annex A (informative): Change History

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	Old	New
2001-09	TP-13	TP-010209				Approved at TSG-T #13	2.0.0	5.0.0
2001-12	TP-14	TP-010245	001		F	Correction of TAR value usage	5.0.0	5.1.0
2002-06	TP-16	TP-020114	002		F	Removal of “session mode"	5.1.0	5.2.0
2004-12	TP-26	-	-		-	Upgrade to Rel-6	5.2.0	6.0.0
2007-06	CT#36	-	-	-	-	Update to Rel-7 version (MCC)	6.0.0	7.0.0
2008-12	CT#42	-	-	-	-	Update to Rel-8 + addition of LTE logo	7.0.0	8.0.0