3GPP TSG-T (Terminals) Meeting #11
Palm Springs, USA, 14 - 16 March, 2001

Tdoc TP-010043

3GPP TS 31.112 V1.0.0 (2001-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Terminals; USAT Interpreter Architecture Description; Stage 2

Keywords
USIM, UICC, Interpreter

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
- Reference models
- Functional flows

The stage 3 documents shall conform to this 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.

[1] SCP TS 102221: UICC-Terminal Interface; Physical and Logical Characteristics

[2] 3G TS 31.102: Characteristics of the USIM Application

[3] SCP TS 102220: Numbering system for telecommunication IC card applications

[4] 3G TS 31.111: USIM Application Toolkit (USAT)

[5] GSM 03.38: Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information

[6] GSM 11.11: Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface

[7] GSM 11.14: Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface

[8] GSM 03.48: Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM Application Toolkit; Stage 2

[9] ISO/IEC 7816-4: Identification Cards - Integrated Circuit Cards(s) with contacts: Part 4: Inter-industry commands for interchange

[10] ISO/IEC 8824: Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1)

[11] ISO/IEC 8825: Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)

3 Definitions and abbreviations

3.1 Definitions

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

Content Provider: Entity that defines services using USIM Interpreter functionality.

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

Gateway: A network program that translates from a source language to the USAT Interpreter byte codes. The gateway sits between the content provider's server that contains pages written in the source language and a USIM containing the USAT Interpreter that will render these pages.

Navigation Unit: A block of a service description that can be referenced (by its anchor) and hence independently activated.

Page: The context of a USAT Interpreter rendering, the scope of USAT Interpreter variables and the unit of transmission between the gateway and a SIM containing the USAT Interpreter. Pages exist in source code form expressed in a mark-up language and in compiled form as USAT Interpreter byte codes.

Service*:* A collection of pages that define a unitary capability of the mobile equipment from the point of view of the user. Examples include remote database access, electronic mail, and alerts.

Service access address:

Bearer Entity: These entities provide the transparent transport of the USAT Gateway to USAT Interpreter content.

Portal:

3.2 Abbreviations

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

AID	Application Identifier
CA	Certification Authority
cHTML	Compact HyperText Mark-up Language
DCS	Data Coding Scheme
HDML	Handheld Device Mark-up Language
HTML	HyperText Mark-up Language
HTTP	HyperText Transfer Protocol
NU	Navigation Unit
OTP	One Time Password
PIX	Proprietary application Identifier extension
STK	SIM Application Toolkit
TLV	Tag Length Value
TTML	Tagged Text Mark-up Language
URL	Universal Resource Locator
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
WBML	Wireless Binary Mark-up Language
WML	Wireless Mark-up Language
XHTML	Extensible Hypertext Mark-up Language
XML	eXtensible Mark-up Language

4 Main concepts

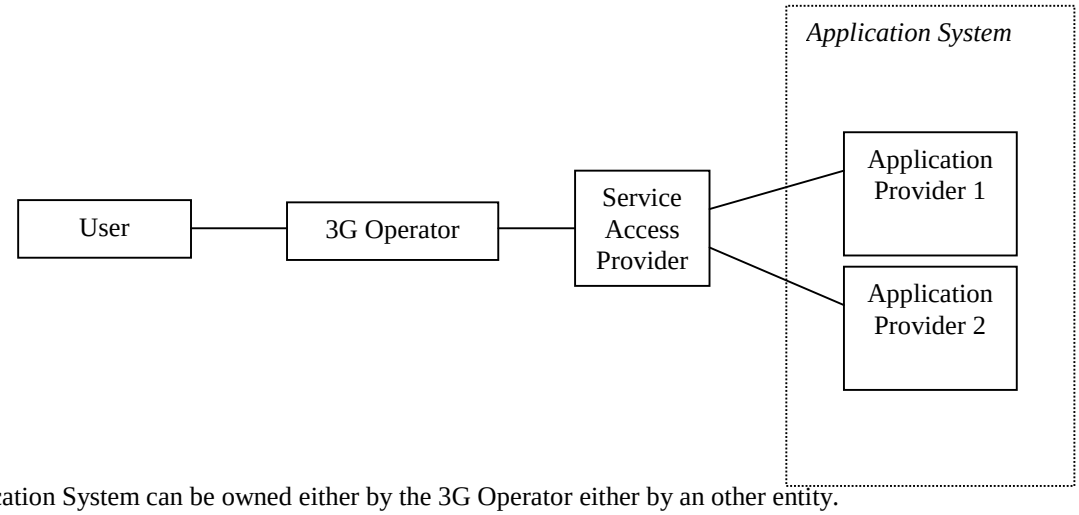
4.1 USAT Interpreter definition

The USAT Interpreter System allows Application Systems to use a USAT Interpreter for services requiring the usage of USIM specific functionality.

4.2 Role models

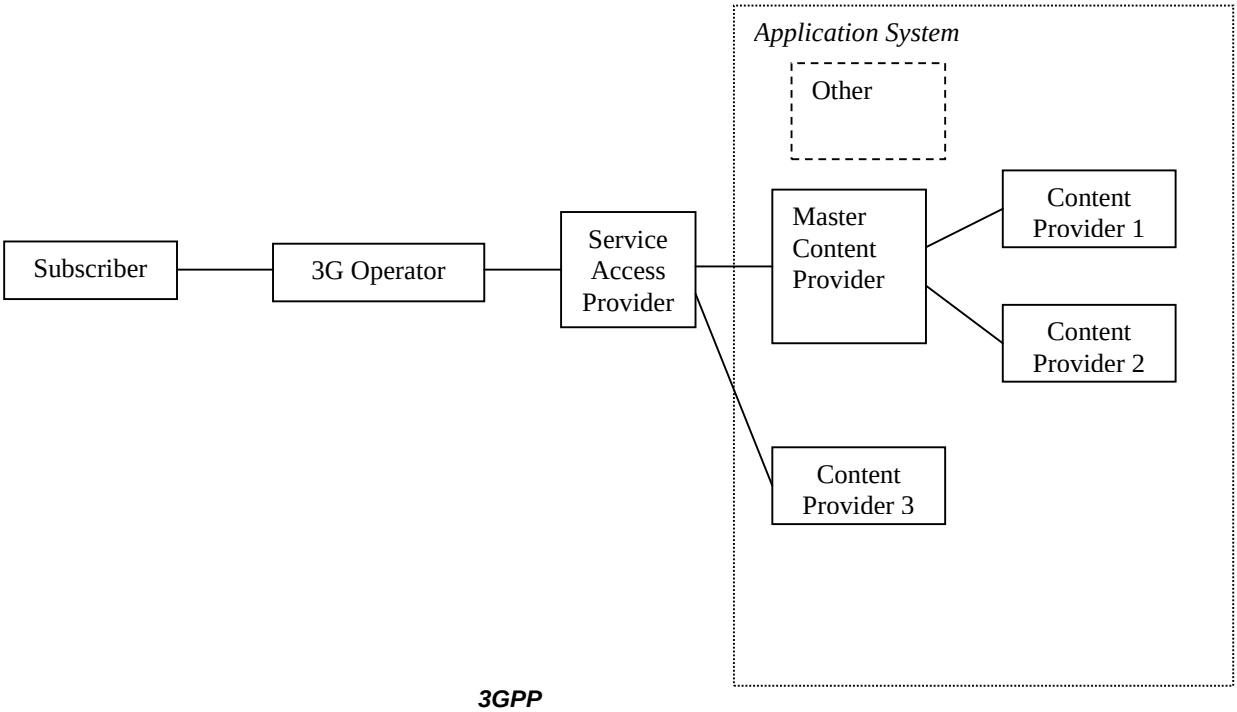
The different role models give an architecture overview of the different requirements for USAT Interpreter systems.

4.3.1 Base Role model



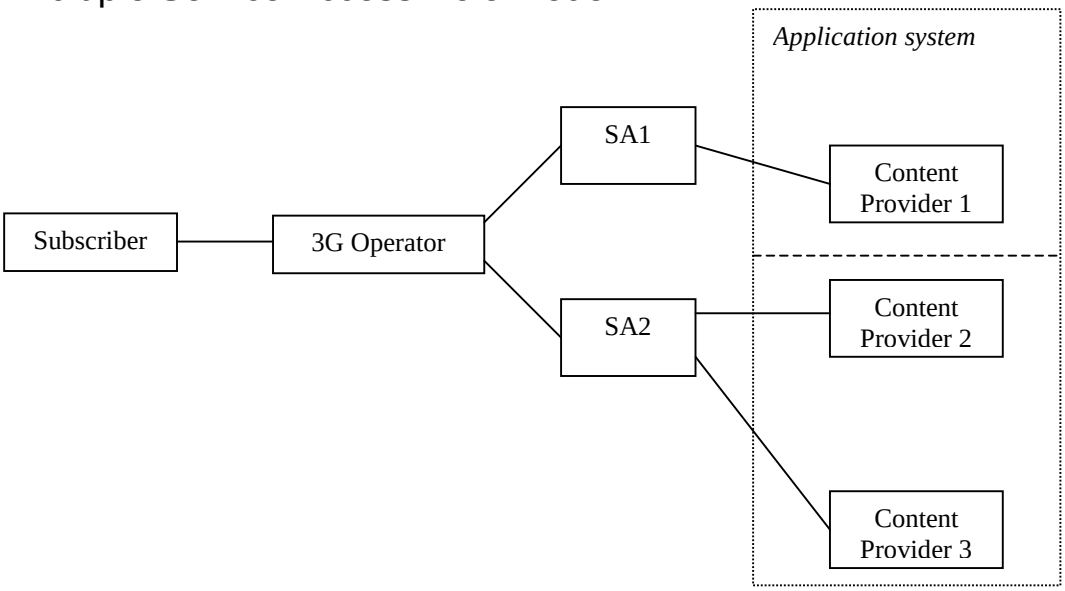
The Application System can be owned either by the 3G Operator either by an other entity.

4.3.2 Master Content Provider Role model



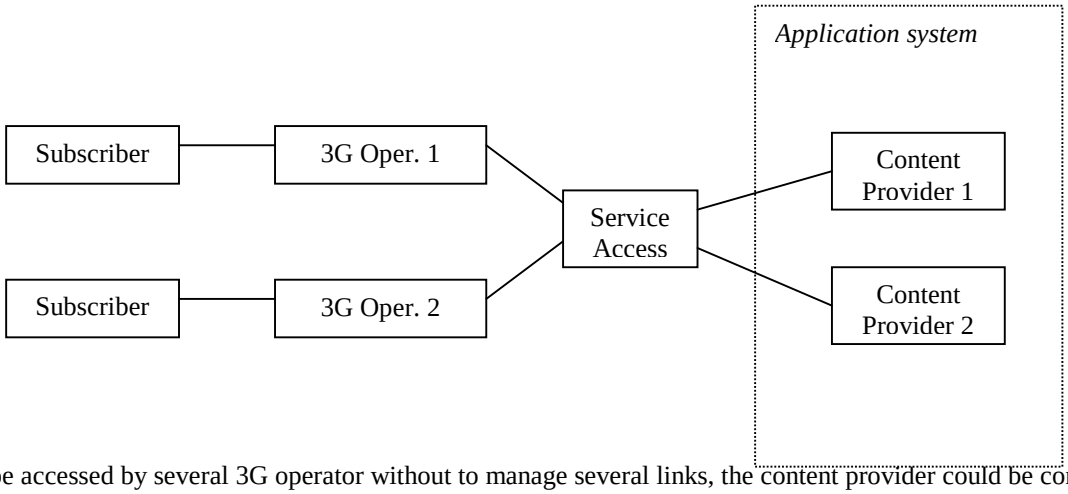
This model describes the case where several content providers use a common interface to be accessed by the USAT Interpreter. This configuration is necessary to federate several content providers using several languages.

4.3.2 Multiple Service Access Role model



In order to be accessed by the 3G subscribers, several Content provider could be federated by a unique Service Access Node which will manage the link with the 3G operator. In this way, the 3G operator could be linked to several SA.

4.3.3 Multiple Operator Role model

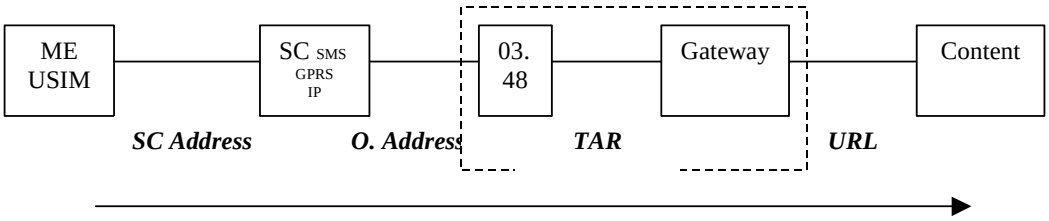


In order to be accessed by several 3G operator without to manage several links, the content provider could be connected to a single SA which will manage the link between the 3G operators.

4.4 USAT Interpreter Reference Model

4.4.1 Base Reference Model

The first reference model refers to the base role model.

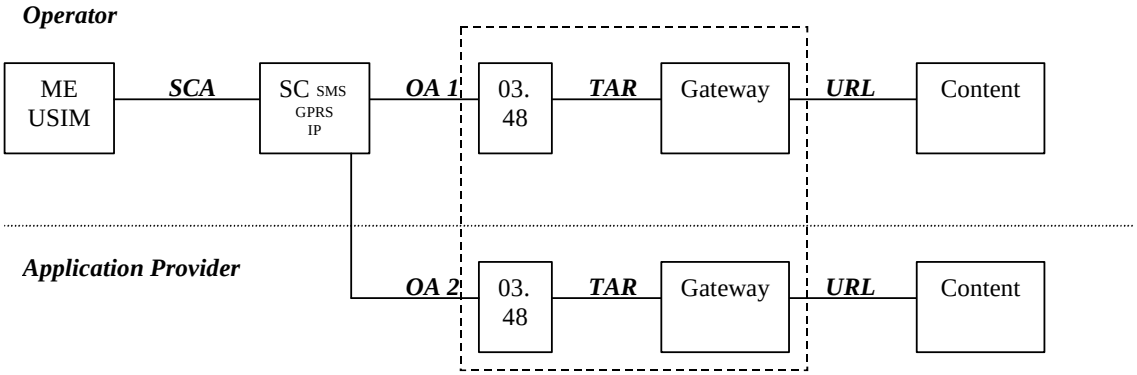


In this model, the USER reaches the SC using the SC address; the SC reaches the 03.48 entity using the Destination Address (Originating address); the 03.48 entity reaches the USAT Interpreter Gateway using the TAR value and between the USAT Gateway and the content provider, the URL is used.

In this scheme, all the layers are completely independent one to the other.

4.4.2 Multiple 03.48 entity Reference Model

In some cases, the content provider want to secure the transport layer between the user and its server. If the used 03.48 entity stays in the Operator field, the transport layer will not be secured between the 03.48 decoding and the SSL encoding. For this reason, the content provider would like to lodge this entity in his secured field. Nevertheless, the operator could have other applications using 03.48. It is then necessary to solve the multi 03.48 entity configuration:



Regarding the Addressing parameters, the multiple 03.48 entity means that either the USAT Interpreter is able to communicate only with one of the several entities either we have to define a mechanism in the URL selection which indicates the OA to be used (The Application Provider has to know the OA the user has to use to reach his service).

This mechanism is described in the Stage3 document.

4.4.3 Multiple Application system Reference Model

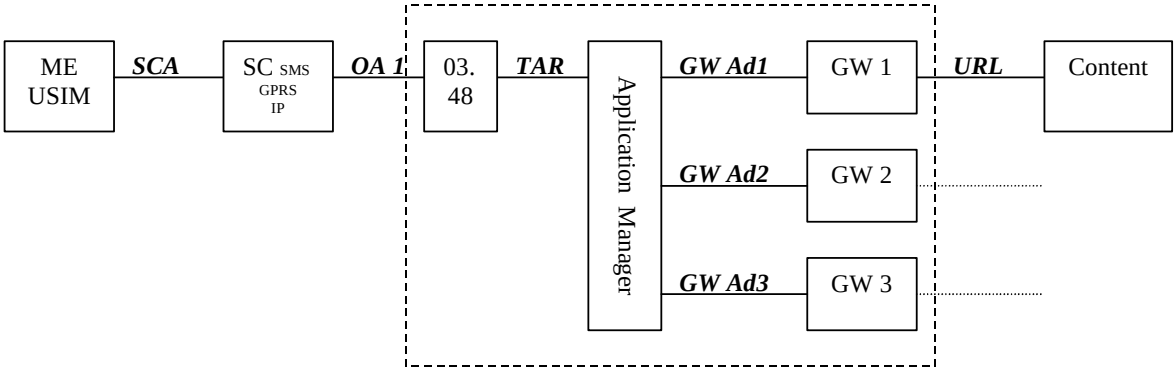
One of the base prerequisite of the USAT Interpreter is to be able to reach any type of service (Mark-up Language oriented, RPC oriented, Fortran…) and where it is (in the operator field or outside).

Using the first reference model, it would be necessary to add a new gateway for each new Application with new language to reach. In this way, the different gateway will be differentiate using the TAR. That means that it will be necessary to reserve a range of TAR for the USAT Interpreter application. And that means also that the application level will be dependent of the secured transport layer. The application will have to know the TAR of the gateway used to convert its language (for each operator accessing this content!).

The second way is to define a new element with a new address in order to guaranty layer independence. This new entity, the application manager, is reachable using a unique TAR. Its role is to create the link between the user and the right gateway.

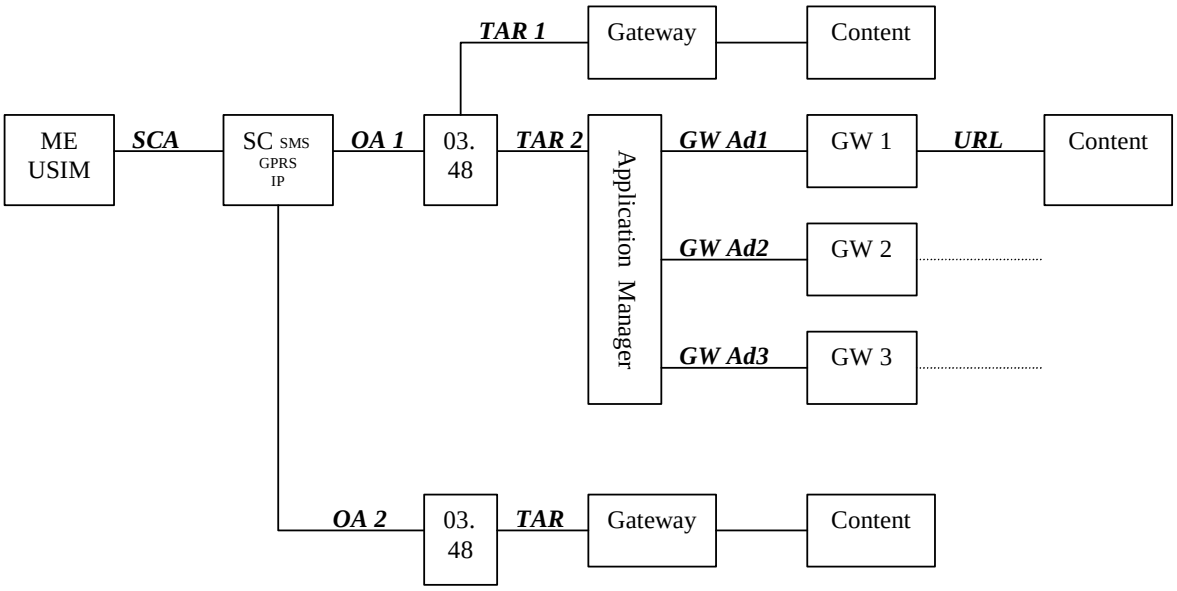
Note: When the term gateway is used, it is to defined the entity which converts high level language into byte-code and not the infra.

On one hand, the application manager is responsible of the routing of the information using the GW Ad and on the other hand, it is responsible of all specific treatment on the message (encoding, persistence….).



The Gateway Address is defined in the Transport Layer (described in a following part of this document). In this scheme, the application is dependent on the Gateway Address and not on the TAR. That means that the Content provider has to know the Gateway Address used to reach its service in order to be able to inform the USAT Interpreter the way to take.

4.4.4 Global Reference Model



The content elements can be located either by the operator either by a distant server.

4.4.5 Layer Representation

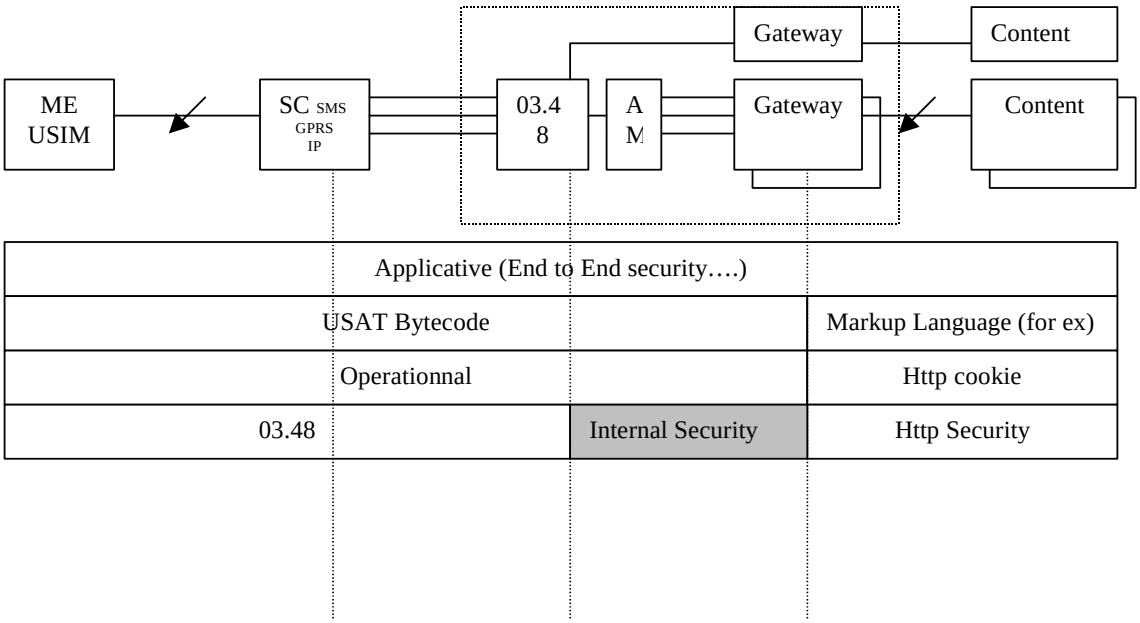


Figure 1: USAT Interpreter Layer presentation

4.5 USAT Interpreter Security

4.5.1 USAT Interpreter Symmetric Security Reference Model

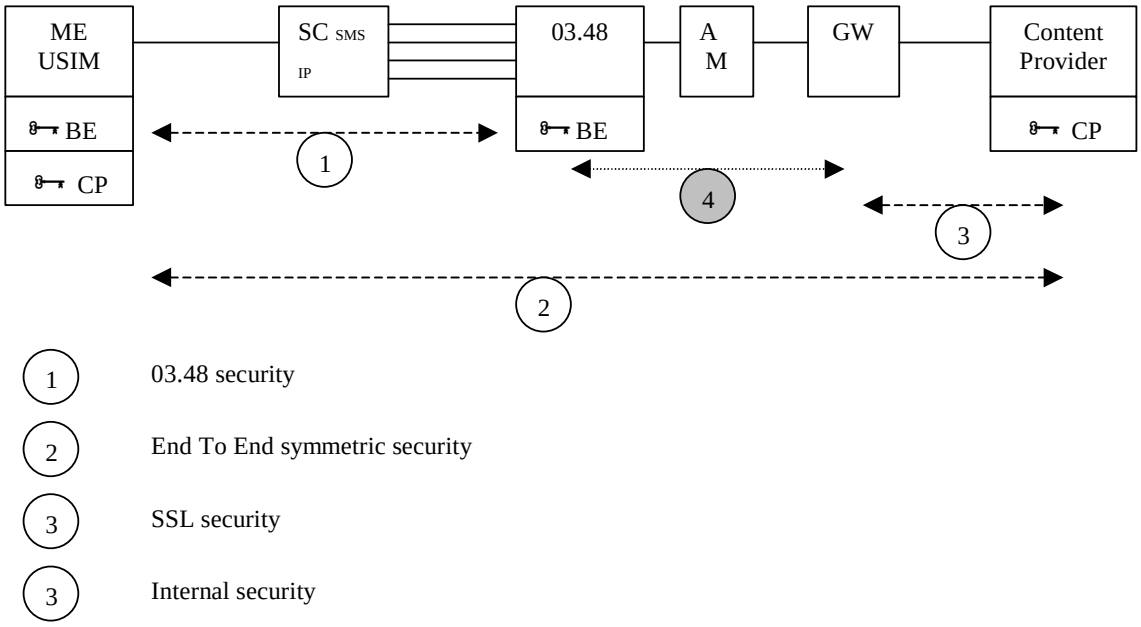


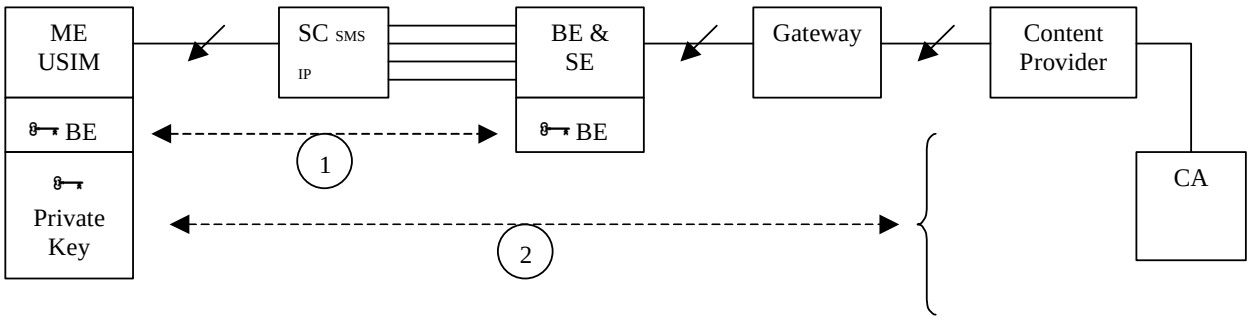
Figure 6: USAT Interpreter Symmetric Security Model

One of the mean requirement of the USAT Interpreter is the Security provided. On the Transport layer, the 03.48 provide the security between the USAT Interpreter and the 03.48 entity. After the gateway, SSL secures the transport layer. Nevertheless, between these two elements no security is provided on the transport layer. One of the solution to work around this issue is to deport the 03.48 entity by the Application System. The other solution is to provide a proprietary secured mechanism.

The End To End security aspects on the applicative layer are standardised in the Stage3 document.

4.5.1.1 Data provisioning for security management

4.5.2 USAT Interpreter Asymmetric Security Reference Model



1 Bearer security

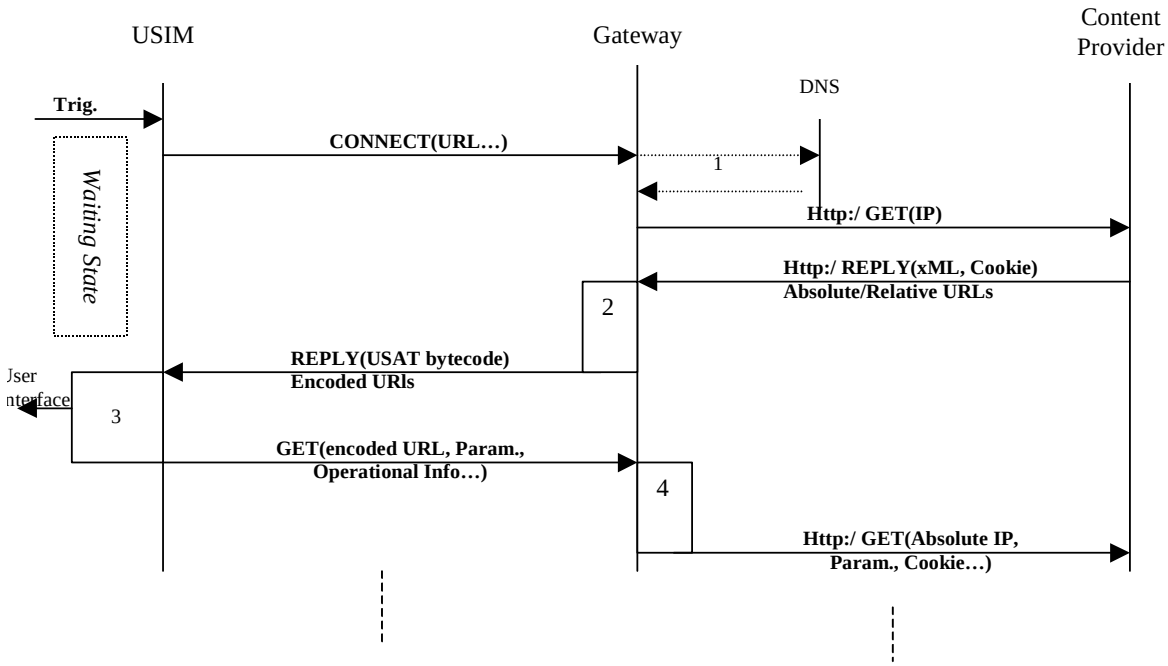
2 End to End asymmetric security

… and transport layer security as described in the previous scheme

Figure 2: USAT Interpreter PK Security model

5 Function and information flows

5.1 Pull mode



1 Request to DNS to get back the IP address

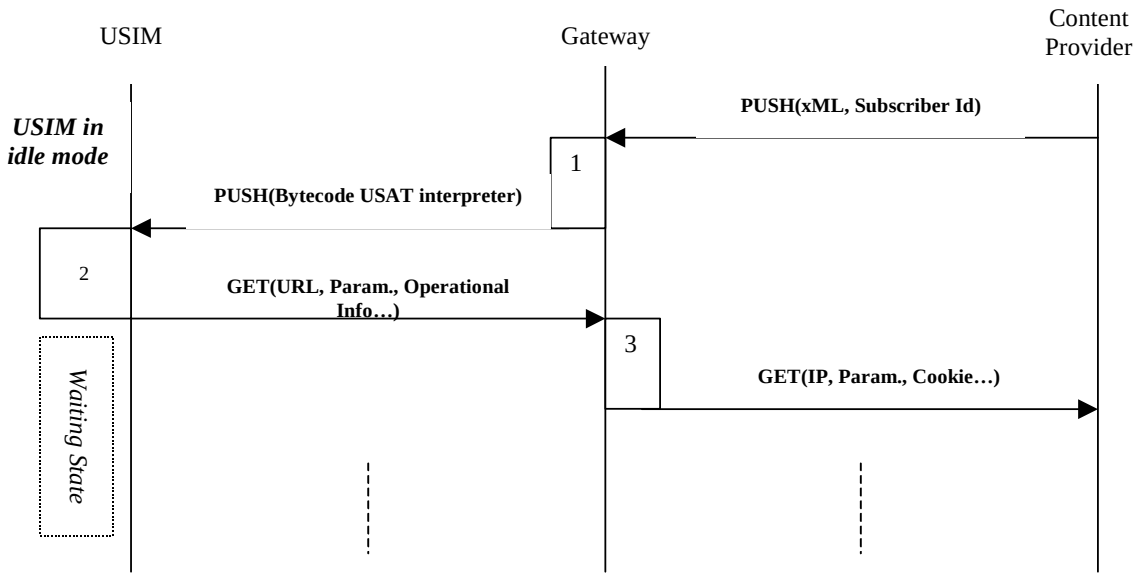
2 Encoding of the Content Provider Reply

3 Parsing of the USAT interpreter bytecode

4 Decoding the USAT interpreter request

Figure 3: USAT Interpreter PULL Flow

5.2 Push mode



1 Encoding of the Content Provider Request

2 Parsing of the USAT interpreter bytecode

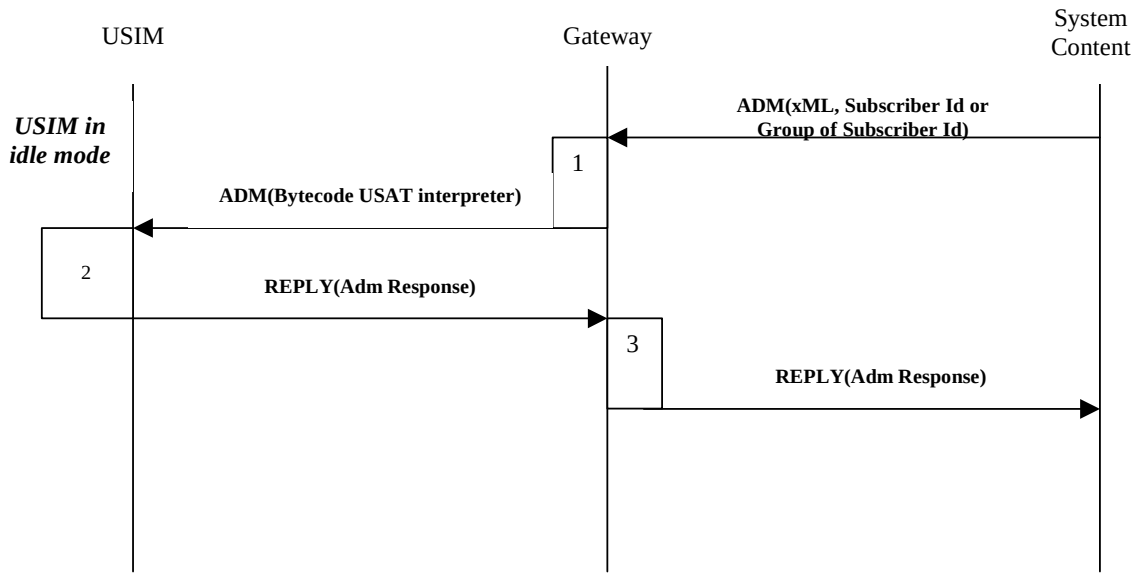
3 Decoding the USAT interpreter request

Figure 4: USAT Interpreter PUSH Flow

The behaviour of the PUSH mode depends on the state of the USIM interpreter at reception of the USAT interpreter byte-code.

5.3 Administrative mode

As described in the stage 1 document, some functionality have to be provide in order to administrate the USIM using the USAT interpreter.



1 Encoding of the System Content Request

2 Parsing of the USAT interpreter bytecode

3 Decoding the USAT interpreter response

Figure 5: USAT Interpreter ADM Flow

The behaviour of the Administrative mode could depend on the state of the USIM interpreter at reception of the USAT interpreter bytecode.

6 USAT Operational Layer

The USAT Operational layer protocol can be used on any connected or non connected media, and guarantees that upper layers are bearer independent by allowing the same functionalities regardless of the media used.

The USAT Operational layer will be used to connect a Client application to a USAT Server (via a SC and an OTA Entity for example) in order to send and receive data.

The USAT Operational layer provides an efficient way to exchange messages and to prevent delayed messages from disrupting an implementation using SMS, but without specific linkage to this bearer.

The USAT Operational layer is located in front of the USAT interpreter bytecode.

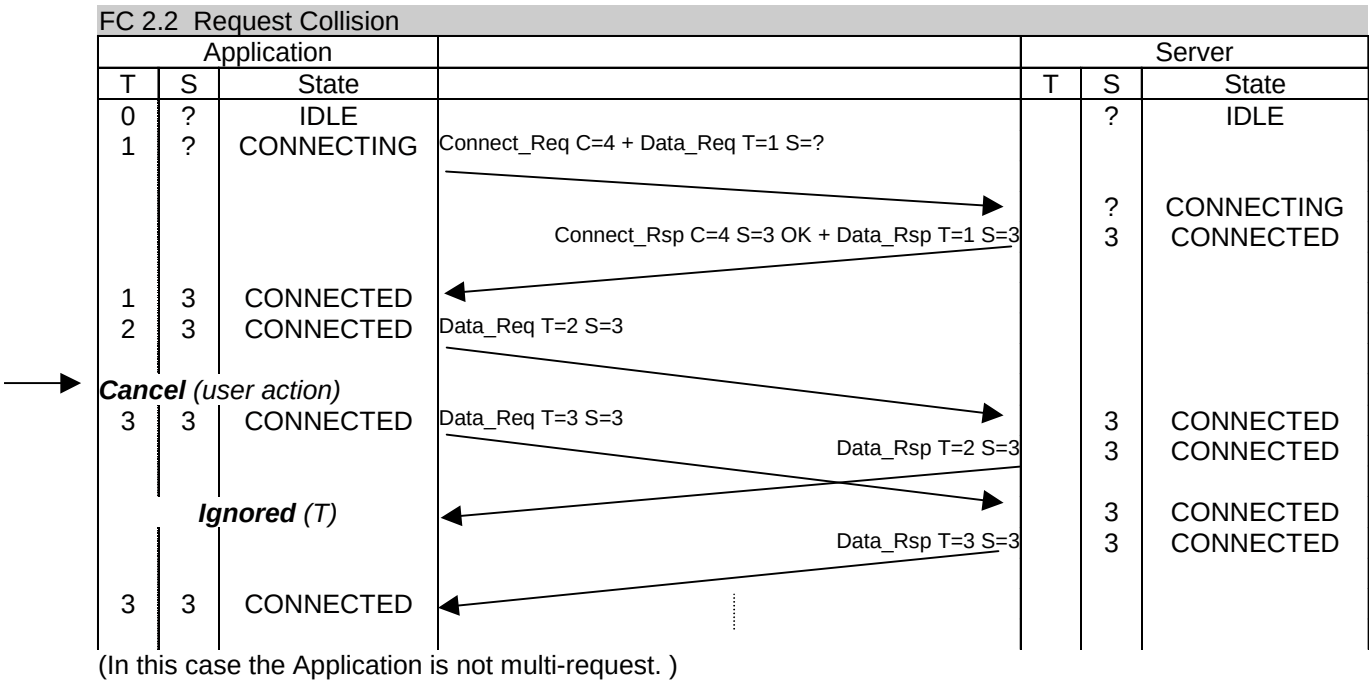
The first byte of this Operational Layer indicates the presence or not of the following information. This byte is mandatory.

Examples:

(T=transaction Id, S=Session Id,C=Connection Id)

FC 2.5 Use of GET_REQ and REPLY_RSP

Application				Server		
T	S	State		T	S	State
0	?	IDLE			?	IDLE
1	?	CONNECTING	Connect_Req C=4 + Get_Req T=1 S=?			
					?	CONNECTING
			Connect_Rsp C=4 S=3 OK + Reply_Rsp T=1 S=3		3	CONNECTED
1	3	CONNECTED				
2	3	CONNECTED	Get_Req T=2 S=3			
					3	CONNECTED
			Reply_Rsp T=2 S=3		3	CONNECTED
2	3	CONNECTED				



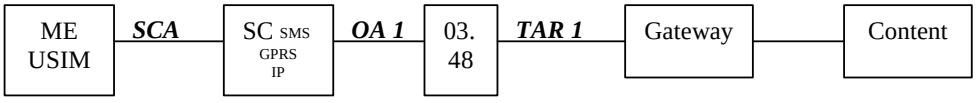
(In this case the Application is not multi-request.)

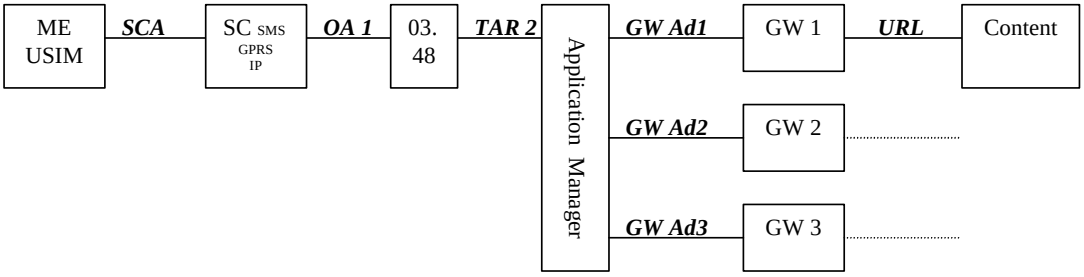
The concept of the USAT Transport layer is independent from the USAT Interpreter byte-code. In this way, this layer could be reused for other 3G application, like administration for example.

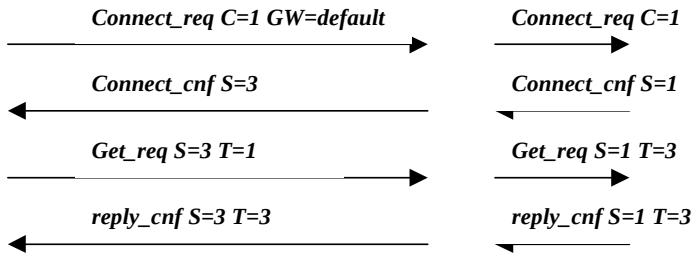
It is designed to allow multiple simultaneous connections and simultaneous requests if supported by the USAT interpreter.

This layer is the placeholder to answer application selection required in 4.4.3.

This layer must be future-proof : a simple topology can easily evolve with a new "session-proxy " node to (for example) dynamically balance load on several GWs. In this case the Interpreter will not select the GW by itself but rely on the system.




ME
USIM
SCA
SC SMS
GPRS
IP
OA 1
03.
48
TAR 2
Application Manager
GW Ad1
GW 1
URL
Content
GW Ad2
GW 2
GW Ad3
GW 3


Connect_req C=1 GW=default
Connect_req C=1
Connect_cnf S=3
Connect_cnf S=1
Get_req S=3 T=1
Get_req S=1 T=3
reply_cnf S=3 T=3
reply_cnf S=1 T=3

History

Document history		
V 0.0.1	February 2001	New version after ad-hoc #25
V 1.0.0	March 2001	Presentation for information to TSG-T #11