3GPP TSG CN Plenary Meeting #25 **NP-040349**
08-10 September 2004, Palm Springs, CA, USA

Source: **CN5 (OSA)**

Title: **All LSs sent from CN5 since TSG CN#24 Meeting**

Agenda item: **6.5.1 (Status report from CN5)**

Document for: **INFORMATION**

Doc	Title	Abstract
N5-040525	Reply LS from CN5 to CN, SA, SA2 on SA2's proposal to transfer OSA stage 2 (23.127) responsibility from SA2 to CN5	Reply to N5-040422. Email approved 23/08/2004
N5-040562	LS to SA1 on removal of Requirements for "User-Application Authentication"	
N5-040564	LS to SA1 on removal of Requirements for "User Data Management (OSA-GUP support)" and "IP session function"	
N5-040619	LS to SA (cc: CN) on OMA and Web Services specifications (3GPP TS 29.199-series).	Email approved 23/08/2004

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) **N5-040525**
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004 *Email approved 23/08/2004*

Title: LS on transferring the OSA stage 2 (23.127) responsibility from SA2 to CN5
Response to: LS (S2-042344/N5-040422) from SA2 on transferring the OSA stage 2 (23.127) responsibility to 3GPP CN5
Release: Release 6
Work Item: OSA3

Source: CN5
To: SA2
Cc: CN, SA

Contact Person:
Name: Chelo ABARCA, Alcatel
Tel. Number: +33 1 30 77 04 69
E-mail Address: Chelo.Abarca@alcatel.fr

Attachments: None

---

1. Overall Description:

CN5 would like to thank SA2 for their LS on transferring the OSA Stage 2 (TS 23.127) responsibility to CN5.

CN5 has considered the proposal from SA2, and has agreed on the following:

1. To take over the responsibility for the OSA stage 2 from Rel-6 onwards (subject to CN endorsement).
2. To submit the final Rel-6 OSA Stage 2 to CN#26 (12/2004), as agreed by CN#24 (06/2004).
3. To request a new TS number for the OSA Stage 2, so that starting from Rel-6 the current TS 23.127, which covers both OSA and VHE in its scope, can be **discontinued**.
4. To bring to CN#25 (09/2004) some updates (CRs) to the current OSA Stage 2 (TS 23.127), so that when contributions are available an alignment can be kept between Stages 1, 2 and 3.
   The latest version of TS 23.127 will be used to create the new, OSA only, TS, for submission to CN#26 for Approval.

2. Actions:

None.

3. Date of Next CN5 Meetings:

TITLE	TYPE	DATES	LOCATION	CTRY
3GPPCN5#29	WG	1 - 5 Nov 2004	Barcelona	ES

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) N5-040564
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

Title: LS on removal of Requirements for "User Data Management (OSA-GUP support)" and for "IP session function" from OSA Stage 1 (22.127)

Response to: n/a

Release: 6

Work Item: OSA3

Source: CN5

To: SA1

Contact Person:
Name: Chelo ABARCA
Tel. Number: +33 1 30 77 04 69
E-mail Address: Chelo.Abarca@alcatel.fr

Attachments:

- N5-040565 (draft Rel-6 CR 22.127-660 for SA1 Approval – "User Data Management (OSA-GUP support)"
- N5-040566 (draft Rel-6 CR 22.127-660 for SA1 Approval - "IP session function")

---

1. Overall Description:

CN5 notes that there were no contributions for the Rel-6 OSA Stage 3 for the following two OSA Stage 1 requirements in TS 22.127:

- "User Data Management (OSA-GUP support)"
- "IP session function".

CN5 has noticed a misalignment between the OSA Stage 1 (TS 22.127-660) and OSA Stage 3.
In the past this has already been a reason to propose deleting some requirements in the OSA Stage 1.

In order to solve this misalignment between the OSA Stage 1 and Stage 3, CN5 believes that the above-mentioned requirements should be deleted by SA1 from TS 22.127.

2. Actions:

To SA1 group:

ACTION 1: CN5 asks SA1, in line with the SA1 agreement reflected in S1-040730 Draft REPORT Version C of SA1#25 Plenary meeting, Montreal, Canada, 28 June - 02 July 2004 (see 6.1 SA -- 24-04 GUP and OSA), to remove the requirement for the "User Data Management (OSA-GUP support)" from Rel-6 TS 22.127.

ACTION 2: CN5 asks SA1 to remove the requirements for the "IP session function" from Rel-6 TS 22.127.

NOTE: CN5 has prepared for SA1 Approval two draft Rel-6 CRs 22.127-660 proposing these removals, which are attached to the present LS (N5-040565 and N5-040566).

3. Date of Next CN5 Meetings:

TITLE	TYPE	DATES	LOCATION	CTRY
3GPPCN5#29	WG	1 - 5 Nov 2004	Barcelona	ES

CR-Form-v7

CHANGE REQUEST

⌘ 22.127 CR CRNum ⌘rev - ⌘ Current version: 6.6.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network X

Title:	⌘	Delete Requirements for "User Data Management (OSA support for GUP)"
Source:	⌘	CN5
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	F
Release:	⌘	*REL-6*

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Missing clear OSA requirements for support of the Generic User Profile (GUP)
Summary of change:	⌘	Delete Requirements for User Data Management (OSA support for GUP)
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)

Clauses affected:	⌘	2 References 7 Requirements for User Data Management 13.3.3 User Profile Management functions

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040564.

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*.

2.1 Normative references

[1] 3GPP TS 22.121: "Universal Mobile Telecommunications System (3G); “The Virtual Home Environment”.

[2] 3GPP TS 22.101: "Service principles".

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

[4] 3GPP TS 23.107: "QoS Concept and Architecture".

[5] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[6] 3GPP TS 29.198: "Open Service Architecture; Application Programming Interface; ~~Part 1~~".

[7] 3GPP TS 22.141: "Presence Service Stage 1".

[8] 3GPP TS 22.228: "IP Multimedia Subsystem (IMS) Stage 1".

[9] 3GPP TS 22.071: "Location Services (LCS) Stage 1".

7 Void~~Requirements for User Data Management~~

~~The User Profile logically is a set of information relevant for a given user. . This set of information might be distributed over various physically separated entities in the network andit is provided by Service Capability Servers and – if permitted – from Value Added Services. In case the Generic User Profile (GUP) is deployed in the network, the User Profile may be provided by both the GUP data and the user profile information that are outside the scope of GUP but provided by SCSs and VAS.~~

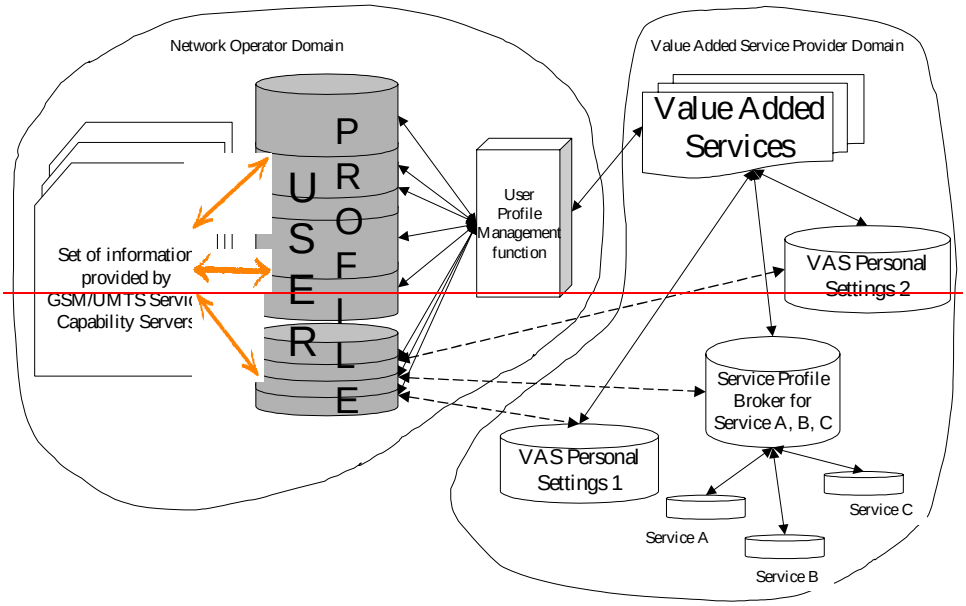
~~Note: The detailed content of the User Profile and the way it is distributed is outside the scope of this specification.~~

~~Subscriber, who subscribe or use services provided by Value Added Service Providers, may customise these VAS according to their needs equally as the subscriber customise her services provided by the network operator. To avoid malicious attacks or conflicting situations, it is needed to allow VAS to access the users User Profile. However VAS shall not be allowed to access the User Profile without permission.~~

~~The OSA Framework functions restrict the applications' access to the User Profile Management functions (section 13.3.3).~~

~~The co-existence of several services and the correct inter-working between them are founded on sufficient information about other services subscribed to.~~

~~The figure below gives a logical overview of the relation between VAS, User Profile Management function and the User Profile itself.~~



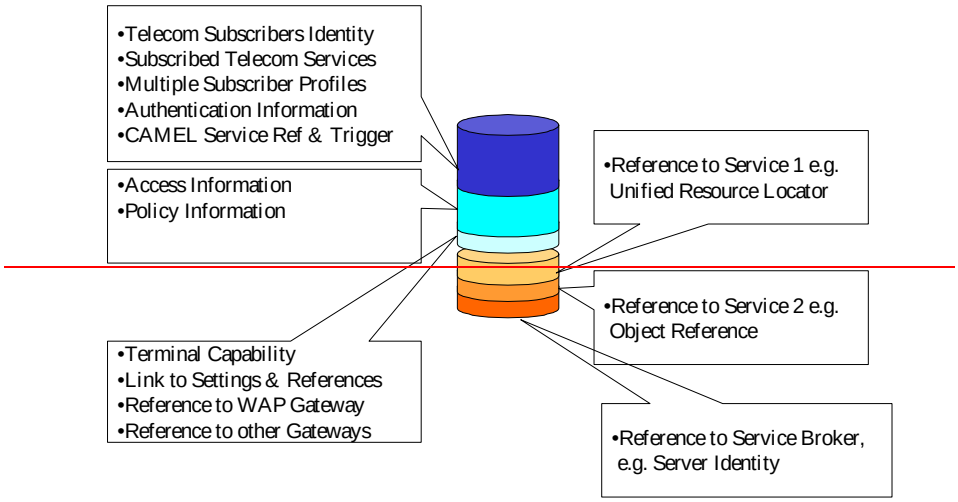
~~Figure 2: Logical overview of relation between User Profile Management function and the User Profile itself~~

~~Note: the dotted line refers to additional Personal Settings. The reference itself shall unambiguously identify the location of the additional personal settings.~~

~~User specific information from the e.g. HLR and/or HSS are equally part of the User Profile as terminal settings and VAS specific preferences. The User Profile in principle is the summary and collection of information with a relevance for the services supported for a given subscriber.~~

~~The figure above shows User and Network Service and VAS specific information, customised by the user. It is assumed that the User Profile consists of several parts. The User Profile elements shall at least be capable to store a reference to additional information stored else where. The User Profile shall act as a root towards all user specific information.~~

~~Even when the content of the User Profile is outside this specification, the following figure shows how a content could look like.~~



~~Figure 3: Example of how a User Profile content could look like~~

~~On the left side of the figure above, typical 3GPP system related information are listed (this is not an exhaustive list).~~

~~The right side depict references to VAS specific information. The representation of references to VAS specific information above, is an example and does not insist to be complete.~~

13.3.3 VoidUser Profile Management functions

The User Profile Management functions enables the (authorised) applications to access the User Profile data, checking before the application's rights related to each separate part of the User Profile. The User Profile data accessed by the application could be independent of specific application but necessary to personalise the application according to the user preferences (an example could be the preferred language of end-user).

Depending on the authorisation, the User Profile Management functions may permit the VAS to read from and/or to add to and/or to modify the User Profile or parts of it. This decision is based on:

- Subscriber identity
- Access information on specific part of the User Profile of the subscriber
- Application identity
- Access type (read, add or modify)

Access information shall contain the user specific access rights per application. These may be given either for individual parts of the User Profile or for a group of data or even all data in the User Profile.

13.3.4 Void

CR-Form-v7

CHANGE REQUEST

⌘ 22.127 CR CRNum ⌘rev - ⌘ Current version: 6.6.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network X

Title:	⌘	Delete Requirements for "IP session function"
Source:	⌘	CN5
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	F
Release:	⌘	REL-6

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	No stage 3 contributions supporting this requirement have been received.
Summary of change:	⌘	Delete Requirements for "IP session function"
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)

Clauses affected:	⌘	13.6 IP session function

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040564.

13.6 VoidIP session function

The IP session function enables applications to access information about IP sessions in progress between a UE and IP networks (i.e., the MSISDN and Session Correlation identifier) using the IP address of the UE. An IP session comprises a flow or a set of flows through a network element during a certain time interval. An IP flow is defined to be a stream of packets that have a set of common properties. The properties include source IP address/port and destination IP address/port, protocol type etc. Flows can be grouped into sessions by specifying wildcards for properties (e.g. the set of flows going to port 80, or the set of flows with target IP address X.X.X.X.)

Applications shall have the ability to :

- Release flows in an IP session:

  This provides the ability for an application to force the termination of an IP session. The application may provide an indication of the reason for release of the IP session.

- Control an IP session:

  This provides the ability for an application to request the modification of the parameters of an IP session both during establishment of the session and while the sessions are in progress. The application may also allow the IP Session to continue with or without the modified information pertaining to the IP Session. This may also include the ability to refuse session establishment, to request modification of Quality of Service parameters, to request modification of the destination IP address (including the IP port) and the modification of volume thresholds (e.g. to allow an application to change the threshold at which a notification is raised).

- Monitor an IP Session:

  This provides the ability for an application to monitor an IP session. The application will specify a particular IP session and event condition. When the condition is met an event is generated and the application shall be informed accompanied with sufficient information. For example, an application could be notified when the data volume threshold of a particular user (defined by source IP address) is exceeded.

- Request flow Information

  This provides the ability for an application to request information about the session of interest. This includes quality of service parameters, target IP address and port, duration of session, and data volume of session

The access to the data, which is typically stored within a network authentication server, is obtained via the OSA gateway (i.e., through this SCF). The IP session information/data shall be released based on specific defined policies between the network operator and the application service provider.

13.7 Multimedia Messaging function

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) N5-040562
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

Title: LS on removal of Requirements for "User-Application Authentication functions" from OSA Stage 1 (22.127)

Response to: n/a

Release: 6

Work Item: OSA3

Source: CN5

To: SA1

Contact Person:
Name: Chelo ABARCA
Tel. Number: +33 1 30 77 04 69
E-mail Address: Chelo.Abarca@alcatel.fr

Attachments: N5-040562 (draft Rel-6 CR 22.127-660 for SA1 Approval)

---

1. Overall Description:

When working on the Stage 3 of OSA Rel-6, CN5 has noticed a misalignment between the OSA Stage 1 (TS 22.127-660) and the work-plan: there is a requirement in the former, "User-Application Authentication functions", that has never been in the latter.

The OSA part of the work-plan lists explicitly all requirements in the stage 1, and CN5 discussions on stage 3 planning have always been based on it.

CN5 notes that no Stage 3 contributions supporting this requirement have been received. This has been a reason in the past to propose deleting some requirements in the OSA Stage 1. CN5 believes that the "User-Application Authentication functions" would have been among the deleted requirements if any company had expressed an interest in including them in the Rel-6 discussions, but this hasn't happened either.

Therefore CN5 believes that the best way to solve this misalignment between the OSA Stage 1 and the work-plan is to delete the "User-Application Authentication functions" from TS 22.127.

2. Actions:

To SA1 group.

ACTION: CN5 asks SA1 to remove the "User-Application Authentication functions" from TS 22.127 for Rel6.

NOTE: CN5 has prepared for SA1 Approval a draft Rel-6 CR 22.127-660 proposing this removal, which is attached to the present LS (N5-040562).

3. Date of Next CN5 Meetings:

TITLE	TYPE	DATES	LOCATION	CTRY
3GPPCN5#29	WG	1 - 5 Nov 2004	Barcelona	ES

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) N5-040563
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **22.127** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **6.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Delete Requirements for "User-Application Authentication functions"
Source:	⌘	CN5
Work item code:	⌘	OSA3
Date:	⌘	12/08/2004
Category:	⌘	**F**
Release:	⌘	*REL-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	No stage 3 contributions supporting this requirement have been received.
Summary of change:	⌘	Delete Requirements for "User-Application Authentication functions"
Consequences if not approved:	⌘	Misalignment between Stage 1 (OSA Requirements in 22.127) and Stage 3 (OSA APIs)
Clauses affected:	⌘	13.1.1.1 Authentication 13.2.5 User-Application Authentication functions

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Draft Rel-6 CR 22.127 sent for SA1 Approval attached to the LS in N5-040562.

13.1.1 Trust and Security Management

The trust and security management feature provides the necessary mechanisms which define the security parameters in which client applications may access the network. This includes the availability of a framework initial access point through which all client applications are authenticated and authorised and the ability to allow the signing of on-line service level agreements between the client applications and the framework.

13.1.1.1 Authentication

Authentication is used to verify the identity of an entity (user, network, and application).

Three types of authentication are distinguished:

- User-Network Authentication:

  Before a user can access her subscribed applications, the user has to be authenticated by the network that provides access to the application. This allows the network to check to what applications the user has subscribed to. User-network authentication *is handled within the network and therefore outside the scope of the OSA ~~present document.~~*

- ~~—~~Application-Network Authentication:

  Before an application can use the capabilities from the network, a service agreement has to be established between the application and the network. Establishment of such a service agreement starts with the mutual authentication between application and network. If a service agreement already exists, modification might be needed or a new agreement might supersede the existing.

- User-Application Authentication:

  Before a user can use an application or perform other activities (e.g. modifying profile data) the application must authenticate the user. When the network already authenticates the user, authentication is not needed anymore. When the network is transparent and the user accesses an application directly, authentication is needed between user and application. This is outside the scope of the OSA.

13.1.1.2 Authorisation

13.2.5 VoidUser-Application Authentication functions

The User-Application Authentication functions provide to applications support for authentication of their users. It also provides an "application-specific user identifier" to be used as a parameter in invocation of other OSA Network functions, when requested by the application.

The User-Application Authentication functions shall authenticate an user upon requests of an application; this requires the application to provide as an input the subscriber's credentials, which enable secure method of authentication (e.g. subscriber's certificates).

The User-Application Authentication functions shall return to the invoking application an "application-specific user identifier" (a true identity or alias) that identifies the authenticated user, when requested by the application. The identifier may be used by the application to recognize a user through several accesses to the application; it may also be used by the application as a parameter in invocation of other OSA network functions (e.g., for User Location function).

The User-Application Authentication functions shall support privacy settings defined by the user.

If the subscriber's privacy settings so require, the "application-specific user identifier", returned by User-Application Authentication function to the invoking application, shall be an alias. Otherwise, the "application-specific user identifier" shall be the true identity of the subscriber (e.g. MSISDN).

When the application invokes OSA Network functions related to subscriber (e.g. Location, Presence), the subscriber's identifier shall be included in the request. An application may request it from the User-Application Authentication function.

When an OSA Network function receives the request from the application and the subscriber's identifier is an alias, the OSA Network Function shall invoke the User-Application Authentication function to translate the alias to the subscriber's true identity (e.g. MSISDN).

13.3 User data related functions

joint-API-group (Parlay, ETSI Project OSA, 3GPP TSG_CN WG5) **N5-040619**
Meeting #28, Piscataway, New Jersey, USA, 09-13 August 2004 *Email approved 23/08/2004*

Title: **LS on OMA and Web Services specifications (3GPP TS 29.199-series)**
Response to: **n/a**
Release: **6**
Work Item: **OSA3**

Source: **CN5**
To: **SA**
Cc: **CN**

Contact Person:
Name: Chelo ABARCA
Tel. Number: +33 1 30 77 04 69
E-mail Address: Chelo.Abarca@alcatel.fr

Attachments: None.

---

1. Overall Description:

CN5 is presenting to the CN#25 plenary the full stage 3 for Parlay X Web Services (TS 29.199-series in NP-040xyz) as per requirements in OSA Stage 1 (TS 22.127).
The Parlay X Web Services are a set of carrier grade, WS-I compliant web services, that allow operator and/or third party applications to be developed on top of an operator's network using Web Services technologies. These specifications have been developed in co-operation with ETSI TISPAN and Parlay, leading to a harmonised web services standard (TS 29.199-series).

CN5 had originally identified this work on web services as part of the overlap between work in 3GPP and work in OMA as reflected in the 3GPP SA#24 document SP-040478. Overlaps may develop into dependencies or even diverging standards, so now that these specifications are ready, CN5 would like to ensure that OMA is aware of the existence of this work and of its relevance to their ongoing activities.

The set of Web Services in TS 29.199-series include:

- Common Data Types
- Third Party Call
- Call Notification
- Call Handling
- Multimedia Conference
- Short Messaging
- Multimedia Messaging
- Terminal Status
- Terminal Location
- Payment
- Account Management
- Address List Management
- Presence

All Web Services are defined using **WSDL based on a style guide** that is already an agreed OMA deliverable.

Mapping to OMA work

The following Web Services may be related to current activities within OMA:

3GPP	OMA
Common Data Types	OMA Mobile Web Services (MWS)
Short Messaging	OMA Messaging Work Group (MWG)
Multimedia Messaging	OMA Messaging Work Group (MWG)
Terminal Status	OMA Messaging Work Group (MWG)
Terminal Location	OMA Location
Payment	OMA Mobile Commerce and Charging (MCC)
Address List Management	OMA Presence and Availability Group (PAG)
Presence	OMA Presence and Availability Group (PAG)

The other services (Call Control related and Account Management) are not yet part of OMA activities. Account Management may come in scope of additional Mobile Commerce and Charging (MCC) work.

CN5 believes that one of the key assets of the OSA APIs is having a single set of APIs for the whole developer community, and based on this principle 3GPP CN5 has worked in co-operation with other organizations – the OSA specifications available today are fully aligned between 3GPP, ETSI and 3GPP2 standards.
CN5 would like to extend this co-operation to the new Web Services specifications in the TS 29.199-series, and ensure that no diverging work is done in OMA.

2. Actions:

To SA group.

ACTION: CN5 asks TSG SA to communicate to OMA the availability of the Parlay X Web Services as 3GPP specifications TS 29.199-series, and propose they be taken into account in ongoing OMA activities as detailed above in order to avoid possible fragmentation or duplication of work which potentially could lead to diverging standards in all the organizations involved in the these activities.

3. Date of Next CN5 Meetings:

TITLE	TYPE	DATES	LOCATION	CTRY
3GPPCN5#29	WG	1 - 5 Nov 2004	Barcelona	ES