3GPP TSG SA WG3 Security — S3#14 **S3-000479**

1-4 August, 2000

Oslo, Norway

1 VHE/ OSA Summary

(Extracts from TS 22.121 Doc 441)

The Open Service Architecture (OSA) defines an architecture that enables operator and third party applications to make use of network functionality through an open standardised interface (the OSA Interface). Network/server centric applications can reside outside the core network and make use of service capability features offered through the OSA interface. Applications may also belong to the network operator domain although running outside the core network.

From the network operator's perspective, it is essential that such an open interface incorporate security features to preserve the integrity of the network and protect the confidentiality and integrity of third party and end user data and applications.

A secure OSA interface is key enabler for the Virtual Home Environment (VHE) concept for personal service environment (PSE) portability across network boundaries and between terminals. For example, users are consistently presented with the same personalised features, User Interface customisation and services in whatever network and whatever terminal (within the capabilities of the terminal and the network), wherever the user may be located.

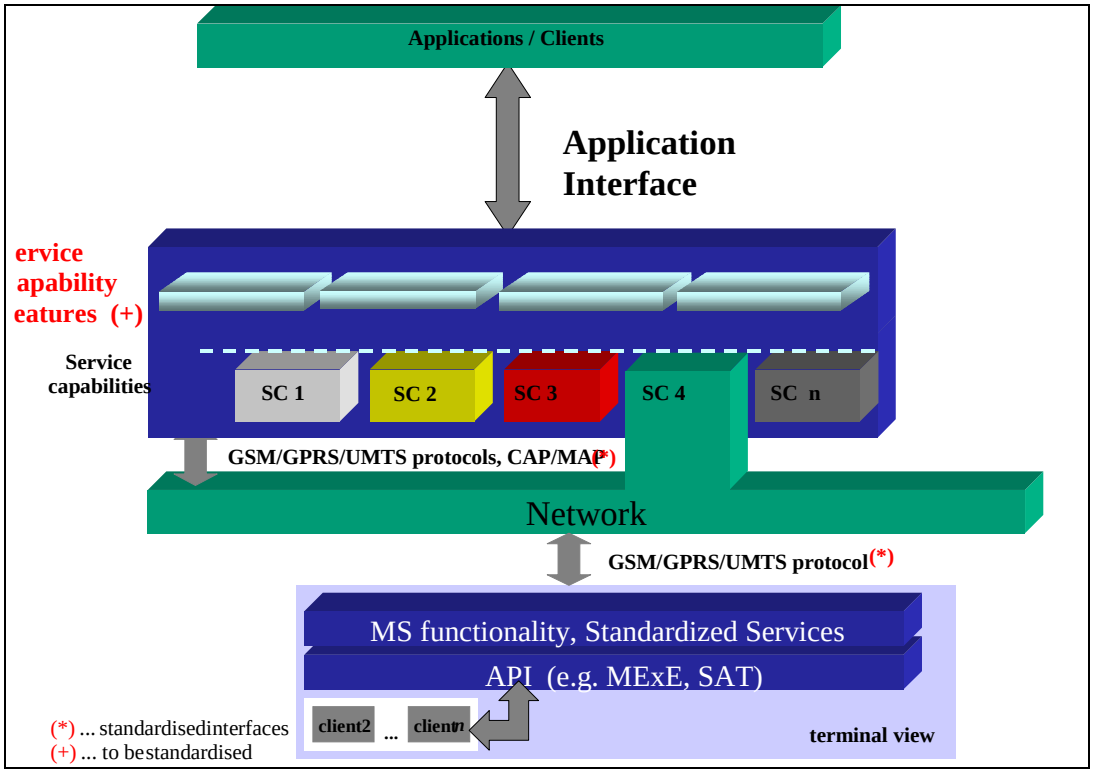

Figure 3: Possible realisation of Framework for Services

2 Call Control Example (Extract from TS 23.127 Doc 442)

7.1.2 Call

The generic call interface provides basic call control methods for applications.

Method	**`routeReq()`** This asynchronous method requests routing of the call to the destination party (specified in the parameter `TargetAddress`).
Direction	Application to network
Parameters	**callSessionID** Specifies the call session ID of the call. **responseRequested** Specifies the set of observed call events that will result in a `routeRes()` being generated. **targetAddress** Specifies the destination party to which the call should be routed. **originatingAddress** Specifies the address of the originating (calling) party. **originalDestinationAddress** Specifies the original destination address of the call. This parameter may be equal to the `originalDestinationAddress` or `Destination Address` as received by the application in the `eventInfo` parameter of the `callEventNotify` method. The latter alternative is conventional when a new `targetAddress` is supplied by the application. **redirectingAddress** Specifies the last address from which the call was redirected. **appInfo** Specifies application-related information pertinent to the call: teleservice information, bearer service information, calling party's category, presentation address, additional calling party address, alerting mechanism, network access type, interworking indicators and generic info for operator specific information. **assignmentID** Specifies the ID assigned to the request. The same ID will be returned in the routeRes or Err. This allows the application to correlate the request and the result.
Returns	-
Errors	**USER_NOT_SUBSCRIBED** Returned if the end-user is not subscribed to the application **APPLICATION_NOT_ACTIVATED** Returned if the end-user has de-activated the application **USER_PRIVACY_VIOLATION** Returned if the requests violates the end-user's privacy setting

3 Current Security Features

The Open Service Architecture consists of three parts:

1) **Applications**, e.g. VPN, conferencing, location based applications.
2) **Service Capability Servers**, providing the applications with service capability features, which are abstractions from underlying network functionality
3) **Framework**, providing applications with basic mechanisms that enable them to make use of the service capabilities in the network. This includes the framework service capability feature (SCF) known as Trust and Security Management (TSM). The TSM Service Capability Features provide:

- **Authentication**: The authentication model of OSA is a peer-to-peer model. The application must authenticate the framework and vice versa. The application must be authenticated before it is allowed to use any other OSA interface. The challenge response protocol actually used is implementation dependent, but assumed to in accordance with CHAP (RFC 1994)

- **Authorisation**: The framework provides access control functions to authorise the access to service capability features or service data for any API operation from a client, with the specified security level, context, domain, etc.

- **Discovery of framework and network service capability features**. After successful authentication, applications can obtain available framework interface classes and use the discovery interface to obtain information on authorised network service capability features. The Discovery interface can be used at any time after successful authentication.

- **Establishment of service agreement**. Before any application can interact with a network service capability feature, a service agreement must be established. A service agreement may consist of an off-line (e.g. by physically passing messages) and an on-line part. The application has to sign (cryptographic) the on-line part of the service agreement before it is allowed to access any network service capability feature.

4 Extracts from R00 work item on VHE doc 438

4.1 IP Multimedia architecture.

The IP multimedia architecture is not considered to make any difference to the service concept provided by VHE. VHE should be transparent to the transport mechanisms. There may be new service capabilities that are realised due to IP architecture and need to be realised in R00 specification. Some VHE service scenarios need to be considered e.g what happens when a CS only user roams into a PS domain what level of VHE should they expect.

4.2 Personal Service Management.

Identifying the handling of user profiles e.g Identify which user is active at any given time in a multiple subscriber profile.
The following are issues for standardisation:

Format
Minimum content
User privacy issues
Application extension of the profile.

- terminal configuration preferences

4.3 Applicability of existing toolkits.

This section will also consider (re) introduction of capabilities that have been removed from R'99. How the existing toolkits can be used to enhance VHE R00 will include the study of:

- **Enhanced Security;**
  The security mechanisms that allows encryption of sensitive user data.

- **Enhanced Session Control;**
  This provides the enhancements of the bearer manipulation and creation of bearers/sessions sessions (in particular negotiation of the QoS).

- **Enhanced UserProfileManagement**

The integration of the Personal Service Environment Management (PSEM) within the Network and Framework SCFs.

- **User Location**
  Further integration of the Location Services within the provisioning of geographical positioning information, taking into account the evolution of the 3G networks associated with this capability.
- **Terminal Capabilities**
  This needs to be studied in collaboration with T and T2. In R99, the mechanism to retrieve the terminal capabilities is only applicable to WAP phones. It is needed to study for R00 a mechanism that is applicable to all types of phones. Security mechanisms for the display of terminal capabilities information have to be studied too.

4.4 Interoperability between toolkits

Are there cases were interoperatability between toolkits becomes an issue? It has been identified by SMG9 that study on interaction between WAP and SAT is important and needed. Some requirements will probably/certainly have to be taken into account by S1. In the list above, it can affect the following points: Enhanced Security, Enhanced Session control, Enhanced UserProfileManagement, User Location.

4.5 Service Continuity

VHE shall be access network independent. Requirement on how this is realised needs to be specified in R00 specification.

The following aspects have to be considered:

- **Provision of Home Services**
  A user roaming to a visited PLMN must be able to use services as provided in the home PLMN.

- **Sevices awareness of roamed-to network capability**
  The home network might need to notify the application or services about a change of the capability of the far end network in order to provide VHE. This is needed for example to ensure that handling of

Incoming Multimedia Calls when roaming in CS network are handled appropriately from the subscriber and operator point of view.

- Independence of Access Technology
  The capability to support different access network should be realised. e.g mobile terminal requiring access to a

  fixed network,
  a bluetooth network,
  a 2G/3G network

Currently to realise this level of support there needs to be a close collaboration with other standardisation groups in this area such as ETSI SPAN group.

5 Extracts from R00 work item on OSA doc 439

This area of study could include identification of enhancements to the OSA interface based on the evolved network capabilities within the Core Networks. Examples of these are:

- Call Control (IP)
  This takes into account the ongoing development of the IP multimedia scenario and addresses the Call Control capabilities based on SIP and/or H.323

- E-Commerce
  This takes into account the capabilities provided by the network to use the capabilities provided by the post processing of the charging capabilities (e.g. E-Pay). It will also involve the enhancements of the security to be provided by the network work and by the application.

Proposed Enhancements for R00

- **User Location**

  Further integration of the Location Services within the provisioning of geographical positioning information, taking into account the evolution of the 3G networks associated with this capability.

- **Terminal Capabilities**

  In R99, the mechanism to retrieve the terminal capabilities is only applicable to WAP phones. It is needed to study for R00 a mechanism that is applicable to all types of phones. Security mechanisms for the display of terminal capabilities information have to be studied too.

- **Enhanced UserProfileManagement**
  The integration of the Personal Service Environment Management (PSEM) within the Network and Framework SCFs.

- **Enhanced Session Control;**

- This provides the enhancements of the bearer manipulation and creation of bearers/sessions sessions (in particular negotiation of the QoS).