3GPP TSG SA WG3 Security — S3#12 **S3-000223**

11-14 April, 2000

Stockholm, Sweden

Source:	**SA WG2**
Title:	**LS on OPEN SERVICE ARCHITECTURE - SECURITY**
Document for:	**Discussion**
Agenda Item:	

3GPP TSG SA2#12 **S2-000557**
Tokyo, Japan, March 6th – 9th, 2000

LIAISON STATEMENT

SOURCE:	**3GPP TSG SA WG2** [1]
TO:	**3GPP TSG SA WG3, TSG CN OSA Adhoc (For Information)**
TITLE:	**OPEN SERVICE ARCHITECTURE - SECURITY**

An S2 – VHE/OSA drafting session has been held on 23-24 February in Stockholm, Sweden. The issue of security within the Open Service Architecture (OSA) has been discussed and agreed.

The agreed text regarding the security (Tdoc S2OSA-000022) has been attached for your information. If S3 has any comments that they would like to express to the attention of CN OSA and S2 experts then an LS would be appreciated.

For your information the following meeting schedule is applicable:

• CN OSA	28-29 February, 1st of March 2000, Antwerp, Belgium
• S2	6-9 March 2000, Tokyo, Japan

Attachment: **S2-000359**

[1] Contact: Alexander Milinski
Tel +49 89 722 29402 Email: Alexander-Milinski@icn.siemens.de

3GPP TSG SA2#12 S2-000359

Tokyo, Japan, March 6th – 9th, 2000

3GPP TSG-SA WG2 VHE/OSA Interim Meeting

February 23 - 24, 2000

Stockholm, Sweden

Title: **Proposed text for a new section on end-user related security (5.3) in 23.127 v.1.2.0**

Agenda Item: 'VHE/OSA'

Source: Ericsson

Document for: Discussion / Decision

INTRODUCTION

Security has been identified as a critical issue to be addressed in order for VHE/OSA to be part of 3GPP release 99. Especially the end-user security needs to be addressed. Therefore, in addition to the framework related sections on security: authentication (6.2) and authorisation (6.3), additional material is introduced here on end-user related security aspects. A new section 5.3 in document 23.127 v 1.3.0 is proposed here. Also, a number of error parameters are introduced to report security violations.

5.3 Handling of end-user related security

Once OSA basic mechanisms have ensured that an application has been authenticated and authorised to use network service capability features, it is important to also handle end-user related security aspects. These aspects consist of the following.

- **End-user authorisation to applications,** limiting the access of end-users to the applications they are subscribed to.
- **Application authorisation to end-users**, limiting the usage of network capabilities by the applications to be authorised (i.e. subscribed) to end-users.
- **End-user's privacy**, allowing the user to set privacy options.

These aspects are addressed in the following subsections~~. Also, a number of error parameters are introduced to handle security violations.~~

5.3.1 End-user authorisation to applications

An end-user is authorised to use an application only when he or she is subscribed to it.

In the case where the end-user has subscribed to the application ~~prior to~~ before the application accesses~~ing~~ the network SCF~~'~~s, then the subscription is part of the Service Level Agreement signed between the HE and the HE-VASP.

After the application has been granted access to network SCF~~'~~s, subscriptions are controlled by the Home Environment. Depending on the identity of an authenticated and authorised end-user, the Home Environment may use any relevant policy to define and possibly restrict the list of services to which a particular end-user can subscribe. At any time, the Home Environment may decide, unilaterally or after agreement with the HE-VASP, to cancel a particular subscription.

Service subscription and activation information need to be shared between the Home Environment and the HE-VASP, so that the HE-VASP knows which end-users are entitled to use its services. Appropriate online and/or offline synchronisation mechanisms (e.g. SLA re-negotiation) can be used between the HE and the HE-VASP, which are not specified in OSA release 99~~parts of this specification~~.

End-to-end interaction between a subscribed end-user and an application may require the usage of appropriate authentication and authorisation mechanisms between the two, which are independent from the ~~VHE/~~OSA API, and therefore not in the scope of OSA standardisation~~subject to standardisation~~.

5.3.2 Application authorisation to end-users

The Home Environment is entitled to provide service capabilities to an application with regard to a specific end-user if the following conditions are met:

1) The end-user is subscribed to the application

2) The end-user has activated the application

3) The usage of this network service capability does not violate the end-users privacy settings (see next section).

~~It is the responsibility of t~~The service capability server ~~to~~ ensures that the above conditions are met whenever an application attempts to use a service capability feature for a given end-user, and to respond to the application accordingly, possibly using relevant error parameters (USER_NOT_SUBSCRIBED, APPLICATION_NOT_ACTIVATED, USER_PRIVACY_VIOLATION). The mechanism used by the SCS to ensure this is internal to the HE (e.g. access to user profile) and is not standardised in OSA release 99~~this specification~~.

5.3.3 End-user's privacy

The Home Environment may permit an end-user to set privacy options. For instance, it may permit the end-user to decide whether his or her location may be provided to 3rd parties, or whether he or she accepts information to be pushed to his or her terminal. Such privacy settings may have an impact on the ability of the network to provide service capability features to applications (e.g. user location, user interaction). Thus, even if an application is authorised to use an SCF and the end-user is subscribed to this application and this application is activated, privacy settings may still prevent the HE from~~to~~ fulfilling an application request.

~~It is the responsibility of t~~The service capability server ~~to~~ ensures that a given application request does not violate an end-users privacy settings or that the application has relevant privileges to override them (e.g. for emergency reasons). The mechanism used by the SCS to ensure this is internal to the HE and is not standardised in OSA release 99~~this specification~~.

(end of text to be inserted)

~~5.3.4~~SECURITY RELATED ERROR PARAMETERS

The following error parameters are introduced with respect to security and/or privacy violations.

- USER_NOT_SUBSCRIBED
- APPLICATION_NOT_ACTIVATED
- USER_PRIVACY_VIOLATION

These error parameters are added for the following SCS's and SCS methods:

Call Control	enableCallNotification()
	routeCallToDestination_Req()

Network User Location	locationReportReq()
	periodicLocationReportingStartReq()
	triggeredLocationReportingStartReq()

User Status	statusReportReq()
	triggeredStatusReportingStartReq()

Generic User Interaction	createUI()