Technical Specification Group Services and System Aspects **_TSGS#8(00)0302_**
Meeting #8, Dusseldorf, Germany, 26-28 June 2000

Work Item Description

OSA Security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

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.

4 Objective

To conduct a threat analysis for the Open Service Architecture and review the security features documented in 3G TS 23.127 for effectiveness in countering those threats and to agree any necessary CR's to S3 and S2 specifications.

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.

The review will also consider “End-user” related security aspects. 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, an end-user is authorised to use an application only when he or she is subscribed to it.
2) The end-user has activated the application
3) The usage of this network service capability does not violate the end-users privacy as 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.

5 Service Aspects

Input from S1 and S2 will be required in order fully understand how the interface will be used by third parties to create new services.

6 MMI-Aspects

Not yet investigated

7 Charging Aspects

none

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X		X	
No					X
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3#14	August 1-4, 2000	Presentation to S3 of Trust and Security Management framework service capability feature (SCF)
S3#15	September 2000	Presentation to S3 of threat and countermeasure analysis
S3#16	November, 2000	Decision if implementation is to be standardised and how much reuse can be made of, 3G AKA as “PrescribedMethod”, Network certificates and security associations etc Approval of any CR’s to S3 and S2 specifications required
	December 2000	Final CR’s to Security Architecture TS 33.102 approved at TSG level
	April 2001	Integration of security architecture Complete CRs
	June 2001	CRs approved at TSG level

New specifications

Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications

Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Possible expanded scope and place of use for existing security features
23.127				Possible CR,s depending on result of threat analysis

11 Work item raporteurs

Colin Blanchard
Network Security Design
MLB1 PP8
BT Advanced Communications Technology Centre
Adastral Park
Ipswich
IP5 5RE
Phone +44 1473 605353
Fax +44 1473 623910
colin.blanchard@bt.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

BT
Ericsson

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)