TSG-SA WG3 (Security) meeting #9 ***TSGS-WG3#9(99)554***

Helsinki, 7-9 December, 1999

From: **S3**

To: **SA, SA2, CN and CN OSA ad-hoc**

Title: **Statement on security issues in VHE/OSA**

TSG SA WG2 thanks TSG CN OSA for their Liaison statement SA2-99F07 relating to security requirements in VHE/OSA. In their LS TSG SA WG2 raises the following issue that relates to network and user security, which is considered part of the open issue on authorization and administration of User Profile highlighted in the developing Stage 2 specification (TS 23.127). SA2 states:

> The proposed OSA API provides to an Application, access to a Service Capability Server (SCSs). The authentication and authorization procedures of this API ensure that only verified applications gain access and that that access is only made available to the use of facilities and operations for which they have are authorized.
>
> However in the current definition, there is a further level of security, which is not being addressed. There is, as yet, no mechanism specified for “authentication and authorization user access to the application and user specific data at the application”. Having authorized an application to use a specific method, there is no control over how that method is used or for which particular data set its use would be valid.

S3 would like to point out that the Home Environment provides services to the user in a managed way, possibly by collaborating with HE-VASPs, but this is transparent to the user. The same service could be provided by more than one HE-VASP and HE-VASP can provide more than one service.

Additionally, but not subject to standardisation, the user may access services directly from Value Added Service Providers. The Home Environment does not manage services obtained directly from VASPs. A mechanism may be provided which allows the user to automate access to those services obtained directly from VASPs and personalise those services. However such a mechanism is outside of the scope of this specification. Here a HE-VASP denotes a Home Environment Value Added Service Provider. This is a VASP that has an agreement with the Home Environment to provide services.'

So S3 has the following final comments on the points mentioned:

1. Secure UA to Application End-to-End authorization is an issue between UA and application and as such transaparent for OSA.
2. Secure User Authorization to the Application via secure access to User Profile Data, (to verify that the User has subscription rights to specific applications) VHE/OSA allows applications to be registered and made available to users. Once the user selects an application (made availble through VHE) it can be assumed by the application that the user has the right to subscribe to the application.
3. The transfer of a Secure User Identity (and possibly signature) to the application, to ensure that the Application can secure access to the Appropriate internal data store at the Application/Application Server. The UMTS network will authenticate a user and a secure user identity is available. Since VHE is a mechanism to provide application to user authenticated in the UMTS network, it can be assumed that the user identity used in the UMTS network can be used as a secure user identity for application as well. So it will be a simple matter of transferring this identity to the application.