MNOs: Secure Your Future in LTE with the Right Choice of UICC Features

LTE has created a mobile environment rich in both opportunities and challenges for mobile network operators (MNOs). At the heart of this environment sits the LTE UICC; an all new, IP-connected multi-application platform. An MNO's utilisation of the LTE UICC will play a huge part in defining how much control it is able to retain over the delivery of, and authentication to, today's LTE mobile services, together with those yet to come.

MNOs which act now to maximise the quality of their end-user's LTE service experience can derive full commercial advantage from LTE and safeguard their competitive standing in the industry. The LTE UICC, or more specifically, the MNOs *choice of LTE UICC features*, holds the key to unlocking this potential.

The right UICC feature choices will:

- Enable MNOs to position the LTE UICC, not the mobile device, as the 'network endpoint', and by doing so, retain control over the services, end-user experience, security and mobility attributes of LTE, together with their associated revenue opportunities.

- Extend its influence outside of conventional mobile boundaries and into the wider online world, through the provision of IP-based identity authentication services.

If MNOs neglect to fully utilise the LTE UICC:

- Over The Top (OTT) players may succeed in positioning the mobile device, not the LTE UICC, as the 'network endpoint' thus reducing MNO control and revenue potential, forcing them to make service concessions that will jeopardise the end-user's LTE service experience and the security of their confidential data.

For LTE, the UICC has undergone a transformation:

No longer is the UICC simply a vehicle for enabling connectivity to wireless networks. Today's LTE UICC offers vast potential for the development of new use-case secure mobile applications and services, including video streaming, mobile payments and identification services. It is IP connected, supports multiple applications and continues to provide an unrivalled environment for secure authentication.

Introducing the SIMalliance LTE UICC Profile:

To help MNOs minimise the risks and maximise the potential of LTE, SIMalliance has published the LTE UICC Profile, a technical document for MNOs that specifies the integrated features required to provide optimal UICC support for LTE network and IMS services deployment.

The use cases in the LTE UICC Profile will be of particular benefit to the marketing teams within MNOs. Technical teams that are responsible for defining the parameters for LTE network utilisation will find

recommendations on a broad variety of critical issues, including the seamless integration of LTE with WiFi networks and femtocell zones; remote Over-The-Air UICC administration using HTTP; and managing user authentication across multiple mobile services using the Generic Bootstrapping Architecture.

The LTE UICC Profile is available for download without charge from:
http://www.simalliance.org/en/resources/recommendations/

About SIMalliance (Security, Identity, Mobility):
SIMalliance is the global, non-profit industry association which simplifies secure element (SE) implementation to drive the creation, deployment and management of secure mobile services. The organisation promotes the essential role of the secure element (SE) in delivering secure mobile applications and services across all devices that can access wireless networks. By identifying and addressing SE-related technical issues, and both clarifying and recommending existing technical standards relevant to SE implementation, the SIMalliance aims to promote an open SE ecosystem to facilitate and accelerate delivery of secure mobile applications globally.

SIMalliance members represent approx 90% of the global SIM card market and work with all global MNOs. As such, the SIMalliance's membership is responsible for delivering the most widely distributed secure application delivery platform in the world (UICC/SIM/USIM).

SIMalliance members are Eastcompeace, Fundamenture, Gemalto, Giesecke & Devrient, Incard, Kona I, Morpho, Oberthur Technologies, VALID, Watchdata and Wuhan Tianyu.

SIMalliance Strategic Partners are Comprion, Linxens and Movenda.

*For more information visit **www.simalliance.org***