

PAMPAS

Pioneering Advanced Mobile Privacy and Security

Soluciones Globales Internet, S.A

Position Paper for Contribution

SGI Soluciones Globales Internet S.A.

Isaac Newton 11
P.T.M. Tres Cantos
28760 Madrid
TEL: 91-806 16 00
Fax: 91-806 16 99

© SGI Soluciones Globales Internet S.A., 2002

Este documento sólo puede ser reproducido en parte o en su totalidad, o archivado, fotocopiado, transmitido de cualquier manera o a través de un medio electrónico o mecánico con permiso previo de SGI Soluciones Globales Internet S.A. Además se debe referenciar si se toma como fuente de información.

POSITION PAPER

From the application point of view several risks do arise while applying Security Mechanism in Mobile Communications. In this Position Paper we shall come along a brief resume of such risks and current Technological Frame in order to better understand how to face and manage actual situation.

Services upon 3G Telephony born under a wide spread of no fully standardized protocols. Even protocols of the same family and relaying under the same technology having a common stem have developed under a no compatible versions depending on the place of the earth these developments took place. Main problem related with this point is the lack of infrastructure needed of these systems to be deployed, so we the case in which a less efficient technology, from the technical point o view, gains a pole position in front of other solutions technically much more better.

We have pointed here that economic cost of implementing the technology is critical, together with the Business Model of such technology. We have not to forget, that wining objective is to offer services and gain deep acceptance of subsequent technology.

If we go some step further in the Security Topics we can highlight the matter of Authentication as one of more interesting challenged to deal with it. Within a cellular network we could identify *machines* with current Protocols and enhanced this identification with IPSec, even so, it remains the topic of identifying the *End User*. The use of Digital Certificates for this matter is tightening to strong discussion currently. Nevertheless, the presence of a mechanism to clearly authenticate the *End User* becomes compulsory.

Another topic, strongly related with Technological Capabilities, is the appliance of flexible enough QoS (*Quality of Service*) contracts and their subsequent SLA (*Services Level Agreement*). So, from technologic the challenges remain open. If successful of 3G services is expected must not be forgotten that this environment witnesses certain lack of objectivity due to Economic Interest and, by its own nature, is a main objective of several Companies, Laboratories Research.

In addition to this, the framework where this technology is deployed is very sensible to Economic Changes, upon this point there is no need of further explication. The will of these lines is having in mind that huge cost in technological deployment is hard to assume nowadays.

Even so, is Security Technology to be applied in 3G Telephony Services mature enough? It is a fact that main security steps will be given when Mobile telephony is able to perform Cryptographic Operations and deal with Certain Storage Capacities to keep sensitive key information together with personal identification information. This is now far to be obtained at a mature and accurate state of the technology together with an appropriate economic cost.

It is a handicap in this election that we are dealing with several information formats and so different branches of toolkits to deal with these different formats, many of them, of difficult integration in prototypes of 3G Mobile Communications.

Soluciones Globales Internet has experienced in the used of Programmatic Toolkits applied to offer 3G Services having the Security of the Final Deployed Solution as one main pillar.

To gain a coherent Security Mechanism, and if not too much, a common meaning of concepts such as Trust and Authentication, if compulsory in order to achieve an European presence in this medium, also in terms of Security. GALILEO was a very important first step that must be continued providing security from a mature point of view; not following not studied enough lines.