

Submission for PAMPAS workshop

by Donald Anderson (donald.anderson@ericsson.com)

As more and more complex and sophisticated systems deliver more and more powerful services there is increasing (potential) advantage to the user in taking up the new services in both a personal and business context.

Particularly in a business context new services can bestow significant competitive advantages for those who take up the new services early, and compel others to adopt new services simply to remain competitive.

Operators benefit from rapid uptake of new services since this translates to rapid return on investment. It is also possible that an operator may rely on a rapid uptake in order to sustain their business plans.

In order to build a secure, high integrity and trustworthy environment suitable to the smooth and confident uptake of new services, operators need to consider a wide range of security and privacy issues and the end users perspective on these issues. Including –

- The operator may need (or be obliged) to control which Certification Authority root keys are stored on the phone (to avoid the user conducting business on the basis of assurances from untrustworthy authorities). The user could perceive this as a restriction, and search out operators with the least restrictions.
- Operator may invest in expensive systems capable of delivering a GPS position faster and with greater availability (assisted GPS) and which resists inappropriate distribution of location information, in this case a mechanism to recoup the cost will be required. The user could perceive this as an attempt to charge for something that should be free.
- If the used service is from an unaffiliated provider there may be no efficient charging agreement or interaction with the mobile network operator. The user may perceive this as charging twice for the same thing – paying the service provider for the service, and the network operator to deliver the service (and the delivery charge could be the more expensive).
- The operator must protect the copyright of service providers (for obvious reasons). Clearly there are some users who will seek out ways to avoid DRM control for both legitimate usage reasons and for illegal purposes. There may also be fears concerning users losing copyright of their own work because of the services used during creation and distribution.
- Tracking and collection of biometrics can be advantageous for development of new services and delivery systems, as well as a source of

revenue in their own right. Clearly these activities can promote adverse reactions from the user.

- On-line attacks on the user or the user's property will inevitably have repercussions for operators and may be expensive to effectively guard against.

In view of these considerations it seems inappropriate to decide technical requirements for encryption, authentication, assignment of bearers etc. without also understanding the services being delivered the mechanisms for delivery of the service as a whole, and the validity of the service from legal, practicality, user perspective and implementation/operational cost.

While it is one of the purposes of technical research to identify what technologies are practical and in what circumstances, it may be possible to prioritize to some extent technologies that have a clear and immediate impact on services that can be offered with contemporary (or near future) network and handset technologies and legal environment.