Optimising Enhanced Mobile Services by Incorporating IN Functionality Into the SIM Card

Nigel Jefferies, Vodafone Ltd[1]

The mobile telecommunications world is undergoing a continuing transformation as an increasing number of services are being offered to a growing number of users by more and more operators. It is essential for the continuing success of this process that the evolving security requirements of users and service providers are properly addressed. It is therefore clear that the requirements on the secure module in the system, the SIM in GSM, are set to increase. In this talk, we will highlight three particular services which a secure module used within a mobile telecommunications systems may support. This work has been prepared as part of the ACTS project ASPeCT[2] " Advanced Security for Personal Communications Systems".

Enhanced Methods of Local User Authentication

In current mobile systems, authentication of the user to the security module is implemented by the use of PINs. Whilst the use of PINs is familiar for the user, it is not perfect. PINs have to remembered, and entered each time the mobile is powered on. In GSM, once a PIN has been entered incorrectly three times, the user must enter a PIN Unblocking Key (PUK) correctly. If this PUK is entered 10 times incorrectly the GSM SIM is unusable forever.

A better system would be an implementation which is more transparent to the legitimate user, but is not weaker than the PIN system. The mobile already has a microphone, so a more natural way for the user to authenticate himself is to use his own voice. Voice biometrics is convenient for the user, low cost and local to the mobile. It is as secure as the PIN system, and can support different security thresholds.

There are three types of vocal user authentication: free speech input; prompted text, and pass phrase. Pass phrase is the more suitable for the mobile environment, but still investigation needs to be made as to the split of functionality and data between the mobile and smart card. The mobile environment brings restrictions on computational resources and storage which makes biometric authentication in the mobile very different from conventional biometric systems.

The ASPeCT project will demonstrate a vocal password based user authentication scheme implemented on a terminal and SIM in December 1997.

Migration of the SIM Towards 3G Systems

Currently, work is under way within ETSI to define a third generation mobile telecommunications system, known as the Universal Mobile Telecommunications System (UMTS), to be introduced in the early years of the 21st century [1].

The main objective of UMTS is to offer a plethora of advanced mobile telecommunication services via a variety of public and private network operators in both outdoor and indoor environments. To allow a cost-effective introduction of UMTS, migration/evolution scenarios have been defined within ETSI, aiming at a smooth introduction of the new services and systems, starting from existing contemporary mobile and fixed telecommunication systems.

---

[1] The Courtyard, 2-4 London Road, Newbury, Berks RG14 1JX. Email: Nigel.Jefferies@vf.vodafone.co.uk

[2] ACTS AC095 ASPeCT is funded by the European Commission and includes the following partners: Vodafone Ltd, Siemens Atea, Giesecke & Devrient GmbH, Lernout & Hauspie, Panafon, Royal Holloway University of London, Siemens AG and Katholieke Universiteit Leuven. Further information (including public deliverables) is available at: http://www.esat.kuleuven.ac.be/cosic/aspect/aspect.html.

The need for enhanced security features in UMTS has led to the definition of specific security objectives [2]. These objectives have been translated into security requirements, resulting in a classification of security features. Mechanisms to realise the UMTS security features are currently under development. Secret key-based mechanisms, as well as public key-based mechanisms have been proposed for UMTS, providing mutual authentication, cipher key agreement for confidentiality, anonymity and non-repudiation. To achieve flexible introduction of new authentication mechanisms and algorithms, a framework for authentication has been developed by ASPeCT and adopted by ETSI , with the ability to migrate smoothly from one mechanism to another.

In order to enable migration from GSM to UMTS, a multi-application card needs to be defined, containing a GSM SIM application and a preliminary UMTS UIM application.

This will be demonstrated and trialled within the ASPeCT project. It will be shown that both the GSM application and the UMTS application can be implemented on one card, and the correct application instigated dependent on the terminal in which the smart card is inserted.

The ASPeCT Payment Scheme

The value-added services of tomorrow will offer endless options to the user. In short, the user will require information on demand to his local terminal. His terminal will therefore require larger processing capabilities, mobile networks will have to support higher bandwidths, and so forth.

To meet the demands of these services, charging will have to be flexible, efficient and secure, and of course electronic. Two forms of electronic payment are credit card based payment, and micropayments. Credit card payment is well known, as are its pitfalls. With respect to value added services, credit card payments may not be applicable as they are not designed for low value payments.

Micropayments have a low processing over head, allow small payments, work both on and off line, and do not need standardisation. The ASPeCT project makes use of a tick payment scheme developed in the RACE project CAFE. The role players in the scheme are the mobile user, the value added service provider (VASP) and the mobile service provider. The user and VASP exchange chargeable information in return for electronic ‘tick’ payments. These payments are collected by the VASP and then presented off-line to the mobile service provider in return for payment. The user is charged by the mobile service provider via the normal monthly billing process.

Conclusions

It is clear that, in the next generation of mobile communications, the SIM card will be required to perform additional functions. These functions are all related to the security of the services provided. ASPeCT has identified the three areas discussed above: local user authentication, a flexible authentication framework and secure charging for value-added services. Indeed, it is hard to escape the conclusion that, although the card can be used to store service profile data, any intelligence will be directed towards enhanced security services. Intelligence related to other functions may be better implemented on the terminal itself.

References

[1] ETSI ETR 050101 Special Mobile Group (SMG): Universal Mobile Telecommunications System (UMTS) objectives and overview. Version 2.1.0.

[2] ETSI ETR 050901 Special Mobile Group (SMG): Security principles for the Universal Mobile Telecommunications System (UMTS). Version 3.0.0.