Special: Applications and Service Platforms for the Mobile User
users need personalised access to their services even if they connect from other network or VHE providers. In such situations, either interworking is necessary between service instances running in the home and visited provider’s domain, or cross-domain access to profile information is required. These scenarios are investigated in the AlbatrOSS project. Again the lack of globally standardised interfaces between services and execution environments prevents the provision of a comprehensive solution.

One possible solution to these kinds of problems is the introduction of service deployment descriptors that describe the requirements and obligations of services towards their users and execution environments. As in well-known component technologies like EJB or CCM, the services as well as the execution environments describe their required and provided interfaces and the appropriate protocols. Thus it is possible to map both descriptions either manually or automatically and to generate bridging components that adapt the technology and protocols between services and execution environments. First steps in this direction have been made in the VHE-UD project.

This adaptation during the deployment time of a service needs only static information. It can be used to satisfy service-level agreements and to guarantee some agreed quality of service during the start-up phase of a service. Much more complex is the task of controlling and justifying the quality of service during the execution time of the service. Components are required that monitor the status of the network and of the services, the end-to-end evaluation of the provided service quality is necessary and an appropriate end-to-end reconfiguration of the service must be enabled. In a fully operational environment, the monitored status information will also be used for logging and accounting purposes.

In current projects, Fraunhofer FOKUS has developed various building blocks for a comprehensive VHE platform together with a series of component-based, adaptive middleware environments. It will be the challenge of future projects to integrate these ideas, experiences, and software modules into a global VHE architecture built around the concept of VHE application servers.

M-commerce API Package for Mobile Phones

by Ioannis G. Askoxylakis, Diomedes D. Kastanis and Apostolos P. Traganitis

M-commerce, the new buzzword in today’s mobile industry, opens new horizons for mobile phones and services. Originally used to place voice calls, today’s mobile phone uses data, multimedia, entertainment, and mobile commerce services, which are expected to overtake voice in revenue generation for operators.

The market for mobile phones, handheld computers and wireless PDAs is increasingly driven by multimedia-based Internet applications. New demands relevant to mobile commerce services include the electronic purchase of tickets, goods, or audio/visual content. The Telecommunications and Networks Laboratory (Netlab) of ICS–FORTH is developing and implementing an M-commerce API package for mobile phones, intended to provide mobile commerce services, achieve widespread usage, and offer unique benefits over and above the alternatives. The design of the corresponding API complies with secure hardware modules already installed on mobile phones (eg SIM cards) and upcoming advanced secure memory modules (SecMMCs).

To achieve this, M-commerce has to be based on secure applications and solutions to gain trustworthiness. SecMMC at ICS–FORTH’s NetLab places strong security at the centre of this project. The challenge is to implement a security scheme that meets the end-user requirements and which, at the same time, is convenient and simple to use. The potential revenue that multimedia and data services can bring to the industry depends on the end-user perception of security and trust, ie, whether the mobile can become a ‘digital wallet’. M-commerce should be viewed in the context of the number of ways that end users will be able to pay for goods and services.

To that end, we are developing secure mobile phone applications, and establishing a framework for secure mobile transactions to support a variety of applications and services. In order to maximise the potential of such services, a number of factors are crucial for success.

Firstly, end users require device ownership: although anyone can pick up the device, only its owner must be allowed to carry out transactions involving personal data. Secondly, end users require secure and reliable networks. Thirdly, all brands and companies supplying services must be able to be trusted. This is true for all components of the value chain, including the financial institution, the retailer, the network oper-
ator and the device manufacturer. Other important factors include allowing end users to record and print transactions, ensuring that services are simple, easy to use, and reasonably priced.

Mobile commerce applications require the existence of a secure module. In our case we consider a variety of security modules, including:

- the broadly used SIM-card module
- the forthcoming Secure Multimedia Card (SecMMC) module
- similar smart memory devices (as specified in the draft standard ‘Mobile Commerce Extension Standard-McEX; Core specification’ by the 5C group).

The SecMMC can be viewed as a classical Multimedia Card with an integrated smart-card kernel, which combines the high security of smart cards with the large memory capabilities of classical Multimedia Cards. Obviously the supported services depend on the security module being used (SIM module or SecMMC). For example, whereas both module types can provide an electronic payment system, memory-demanding multimedia applications can only be supported by the SecMMC.

The SecMMC is being developed by a consortium consisting of Guardarone Solutions AG Germany (project coordinator), Infineon Technologies Flash Ltd Israel, IAIK University of Graz, Technische Universität München, Fraunhofer-Gesellschaft-IGD, FORTH, Infineon Technologies, Flash GmbH&Co KG and Mühlbauer AG.

Our development of the M-commerce API for mobile phones focuses on three basic areas of application:

- mobile payment
- mobile entertainment (or infotainment)
- mobile business.

Mobile Payment applications allow personal payment transactions like e-ticket purchase, local merchant payments, stock trading, and eventually telematic and transportation usage. This type of application can be supported by both SIM and SecMMC modules. Key characteristics of this application are:

- **Anonymity**: during an economic transaction nobody can extract any information concerning the corresponding transaction pair.
- **Off-line operation**: two parties can complete a transaction without the intervention of a third centralised intermediary entity.
- **Transferability**: each entity of the system should have a hybrid role, both as a payer and as a payee.
- **User mobility**: the payment process is independent of the location of the transaction pair.

In addition, Mobile Entertainment applications involve copyrighted content (music, video and eventually navigation content). Consumers want to personalise their mobile phones with ringtones, graphics and picture messages from content providers. Games, downloadable applications, music and video feeds are sure to follow, as secure modules like the SecMMC become available for integration into mobile phones. In some regions of the world this type of system is already in use to a limited degree.

Mobile Business applications securely connect mobile users to both internal company and external public organisations. This type of application is an essential part of comprehensive sales force automation implementation.

All these emerging mobile services involve large volumes of multimedia data and require high levels of security to protect the transmission and storage not only of financial accounts and PIN codes but also of the multimedia data that is downloaded and stored.

Please contact:

Apostolos P. Traganitis
Tel: +30 2810 391724
E-mail: tragani@ics.forth.gr

Ioannis G. Askoxylakis
Tel: +30 2810 391723
E-mail: asko@ics.forth.gr

Diomedes D. Kastanis
Tel: +30 2810 391723
E-mail: diomedes@ics.forth.gr