

# WiTness – Wireless Trust for Mobile Business Position Statement

Thomas Walter, Peter Schoo  
DoCoMo Euro-Labs  
Landsberger Strasse 308-312, D-80687 München  
Tel: +49-89-56824 210/Fax: +49-89-56824-300  
[walter | schoo]@docomolab-euro.com

Jochen Haller, Philip Robinson  
SAP AG, CEC Karlsruhe  
Vincenz-Prießnitz-Str. 1, D-76131 Karlsruhe  
Tel: +49-721-69020  
[jochen.haller | philip.robinson]@sap.com

## Mobile business applications

It is a matter of fact that the on-line community has become larger and more diverse. A typical scenario is a company whose network must support a mobile workforce. The company's service model is based on sales people and consultants travelling to provide on-site customer support and sales. Usually, the consultant uses direct dial-in to the corporate network, which is, incidentally, quite an expensive policy, particularly when we consider an international company without distributed dial-in nodes. Mobile business applications over this dial-in may be represented by the employee accessing the corporate databases, sending and receiving email, time-tracking and travel management, as well as receiving timely information for the next assignment.

## Security requirements in mobile business applications

Running business applications over public networks requires further attention in order to prevent attackers from gaining access to confidential data or otherwise manipulating or forging data. The standard issues to be tackled are: identity verification and authentication, authorization permission, confidentiality and integrity preservation, and nonrepudiation evidence. These must be achieved even when corporate communications are performed across multiple and differently administered domains.

## State-of-the-art in securing business applications

Typically, a security officer has two complementary technologies to protect corporate networks and transmitted data against attacks: firewalls and virtual private networks (VPN). Firewalls can be characterized as a technology providing a set of mechanisms to enforce a security policy on data from and to a corporate network. Since firewalls do not provide privacy and confidentiality, VPNs have to complement firewalls to protect data in transit.

However the above-mentioned approaches are not seamlessly applicable in the assumed business scenario for the following reason:

- Firewalls and VPNs are static and provide little flexibility. One of the classical applications of firewalls is to allow traffic originated from specific foreign IP addresses. Mobility, however, may imply roaming between networks and operators, possibly changing the source address, which because of the static configuration of firewalls, may potentially lead to discontinuity of service connectivity for the mobile user.

Firewalls are suitable to protect a network for a defined set of users, devices and systems. However, if the set is about to change because of some re-organization taking place, re-configuration of the firewall has to be done.

The necessity to protect data in transit has not at all been addressed with the implementation of firewalls. VPNs in addition to firewall-ed corporate networks share the same shortcomings identified above. IPsec as the preferred set of protocols to set up VPNs is suitable to establish a secured subnet-to-subnet connection, but it fails to provide the necessary flexibility to establish

a reliable secured connection for the typical mobile user over a wireless network bearer with *peculiar* properties as, for instance, high latency often encountered with GPRS as bearer.

- Heterogeneity of wireless networks do not allow for a comprehensive and coherent support of security features without looking into the application requirements and support within applications themselves. This holds particularly true, if end-to-end security is required. Firewalls and VPNs are security measures on the network layer and are not application aware.
- Business applications require support to secure business transactions (e.g., nonrepudiation). However, mutual authentication of clients and servers is implemented only to a limited extent, and is mainly based on public key infrastructures. Furthermore, authentication is only done against claimed identities, which are easy to fake on un-trusted client hardware.

## **WiTness – End-to-end security for mobile business applications**

The IST project WiTness (IST-2001-2.1.3) is aiming at providing end-to-end security between mobile business applications without firewalls. In support of this WiTness will develop technologies that allow application providers to define and implement their own security solutions. This will be achieved by providing suitable platforms, flexible services in mobile devices (e.g., smart cards) and suitable interfaces to applications. WiTness focuses on two primary targets for interfacing with applications:

- security-related network services such as secure transport of data between clients and servers, and access to public key infrastructures (PKI); and
- interfaces to security modules, i.e., smart cards (SIMs, USIMs...), which hold security data and partly perform security-related operations.

Security services and interfaces must integrate easily into applications, security services must also be flexible enough to fit the needs of applications (dynamic software configuration and updates come into play here), and different security infrastructures must interoperate to provide protection and integrity of data if sent over heterogeneous networks (wired or wireless -different wireless technologies).

Because of the above mentioned vulnerability of un-trusted client hardware, WiTness looks into the development of smart cards (or applications on SIM cards) that will support authentication, authorization, secure data transfer and, most important for business applications, data integrity and proof of origin. The challenge is that smart cards are limited in resources (CPU, memory), which implies that certain security functions are difficult to be performed. To overcome this drawback, the concept of federation of clients has been coined in WiTness. A federation is to be understood as a collection of client devices that identify and authenticate one another and to the corporate network. The corporate network sees only a single logical client device from which it knows the identity.

In summary, WiTness will provide the highest possible level of mobile security. The technology developed will be:

- generally applicable for all 3G (and wireless network) applications;
- largely backward compatible with 2.5G;
- linked to standardisation and industrial consensus development;
- able to provide a multi-layered architecture, agents-based systems to enable interoperability, inter-working, openness and integration of applications and services across platforms; and
- able to offer applications for e-Commerce, e-Work, transport, health and governments.