Extended Summary

Trusted Integration of Mobile Platforms into Service-oriented Networks

Michael Marhoefer, Siemens AG
Andreas U. Schmidt, Fraunhofer SIT

Keywords: Trusted Computing, mobile device, network-agnostic, service-oriented network.

The medium-term future of mobile services and the service provisioning methods behind them is governed by three major trends.

- Firstly, the access to mobile services, viz., services accessed by users through their mobile devices, is becoming network-agnostic. Driven by the technological trend toward horizontal integration of technologies, users will soon be able to acquire services transparently on a single device via a variety of channels and transport methods such as 2G, 3G, WLAN, Bluetooth, WiMAX, MobileIP, etc. Accordingly, the end users' attention focus will shift away from the network access pricing to that of content and services. Competitors in the sector will need to attract custom by offering attractive applications and content with good price to quality ratio, with only little room left for returns generated by charging for network access and data transport.
- The second important trend is that, in parallel, mobile devices are becoming rather smart appliances which can deliver a good deal more than mere voice communication. Such devices no longer are simple terminals to mobile networks, but they both provide and consume applications, data, and media (handsets with cameras providing the simplest example).
- A third, technological trend is hiding behind the former two, and is, in fact, enabling it. It is the enrichment of mobile devices by trusted computing capabilities, which generally aims to achieve a new level of trust and security for networked devices. The rationale in view of the first two mentioned trends is simple. If a mobile device is trusted, then it is possible to separate the access control for the communication network from the access control for services and content, since the latter can then be enforced end-to-end. This is in sharp contrast to the current operation of mobile network access which is characterized by a rather tight vertical integration from SIM-based authentication up to the service level. Future access control methods will give the choice of authentication method to the service platform operator and the service providers. The SIM/subscriber identity still can be used concurrently or in combination with trusted device-based methods. Thus, we can envisage trusted computing enabling network- and device-agnostic trust relations on the application-level, eventually creating a uniform trusted platform for service provisioning.

From an architectural viewpoint this levers the classical client/server relationship between mobile device and its user on the one hand and the network and the services provided through it on the other hand. Scenarios become possible in which services are exchanged between these two and other business parties. It is an intriguing question how this will affect business models in the mobile domain, in particular if it enables new ones. Two scenarios are highlighted below.

The integration of trust into mobile service provisioning needs to take into account the simple fact that trustworthiness is always an (at least) bilateral matter. This means that a trusted mode of operation and communication needs to be supported, enforced, and maintained within the mobile device, as well as the mobile network – and that both need to operate at the same 'level of trust'. On the side of the mobile device, this trust assurance is essentially a vertical task ranging from application to the hardware level. As for instance the specifications of the Trusted Computing Group specify, application, data, possible middleware, and abstraction layers need to be supported by *a* trusted operating system which provides, together with a trusted hardware platform a secure, tamper-resistant environment for the device's operation. The 'root' for the trustworthiness of the device is provided by a cryptographic coprocessor, e.g. the commonly called Trusted Platform Module (TPM). It holds various public and private keys for, amongst others, memory encryption, secure communication, and to provide secure authentication with a protected device identifier. It also ensures a system's operation in a trusted state by keeping cryptographically secured state registers. In the context of a communication network, the functionality of the devices needs to be complemented by trusted service/content provisioning methods as well as a trust management infrastructure (Figure 1), supplementing the classical authentication methods of mobile networks. The former means basically to base authorization to service access on the trusted computing-specific process of Remote Attestation using the TPM, and content/service delivery on the mentioned secure channels. The latter comprises various new management tasks such as delivering keys and IDs to devices to 'name' them and tie them to the network, but also the enforcement of software updates to maintain a high security level.

Application scenarios for trust-enabled mobile networks and devices exist at all levels of trust from the provisioning of basic functions like network and service access to transactions demanding highest security such as DRM-protected content delivery, establishment of ad hoc contracts and Service Level Agreements, and possibly even (legally binding, qualified) electronic signatures. Two examples shall elucidate the fundamental concepts behind trusted mobile services and outline their benefits.

Example 1:

Imagine a user with a trusted mobile device wants to purchase a soft drink from a likewise trust-enabled vending machine – the point of acceptance (POA). While the user still makes up her mind on her taste preferences, device and POA have already initiated a trusted communication session in a bootstrap approach, e.g., using transport layer encryption to carry out the online attestation using their respective TPMs. Device and POA thus achieve mutual assurance that they are in an unaltered, trustworthy state, and begin to exchange price lists and payment modalities. After the user selects a good and confirms his choice at his device, signed price and payment processing information is transferred to the mobile network's operator (MNO). After verifying the signatures, and optionally informing the good's vendor and a payment service provider, the MNO sends a signed acknowledgement to the mobile device, which is then relayed to the POA, where it is verified and the good is delivered.

The benefits for the vendor that arise in this scenario basically arise from the transitive trust relationship that is mediated between MNO and POA by the mobile device. It entails in particular that no network communication is required during the initiation of a trusted session, that no transaction data needs to be stored in the POA, and that, ultimately, the POA does not need to be equipped with networking capabilities – at least for the sales process. In this way the MNO provides payment services as well as authorization control for the vendor – requiring little more than a TPM and a short-range communication module in the vending machine.

Example 2:

A second, similar but slightly more far-fetched example regards home automation and lets a user and her mobile device become part of the maintenance service of, say, the heating system of her home. Based again on their respective TPMs, heating system and mobile device establish a secure communication channel to exchange maintenance data, or data used for metering. This can be done both at specific user requests or even seamlessly during normal operation of device and heating system, every time the machine-to-machine (M2M) communication module of the device gets in the range of the one in the heating system. In this way, the mobile device can notify user and a maintenance chain about necessary repairs and also support accounting and billing. Here, a trusted computing approach not only ensures the protection of personal data – since heating system and user device 'know' each other – it also enables a simple means of remote maintenance and home automation in non-networked homes by utilizing the mobile network in a clever way.

The two examples described above are meant to give a taste of what may lie ahead in trusted integration of mobile services and represent very self-evident scenarios. More good ideas are certain to emerge pretty soon. The common denominator of all those concepts is the transitivity of trust between mobile devices and other trusted systems, which enables an MNO to provide trusted content and service provisioning beyond the classical boundaries of their networks. They can do that to their own benefit, for instance to enable the transfer of copyright protected content from an MNO's content distribution and digital rights management system to non-mobile devices. Or, they can embrace new commercial relationships in providing third-party services as in particular in the two examples sketched above. This shows that trusted platforms allow for interesting new business models benefiting MNOs, content and service providers, and ultimately also end users.

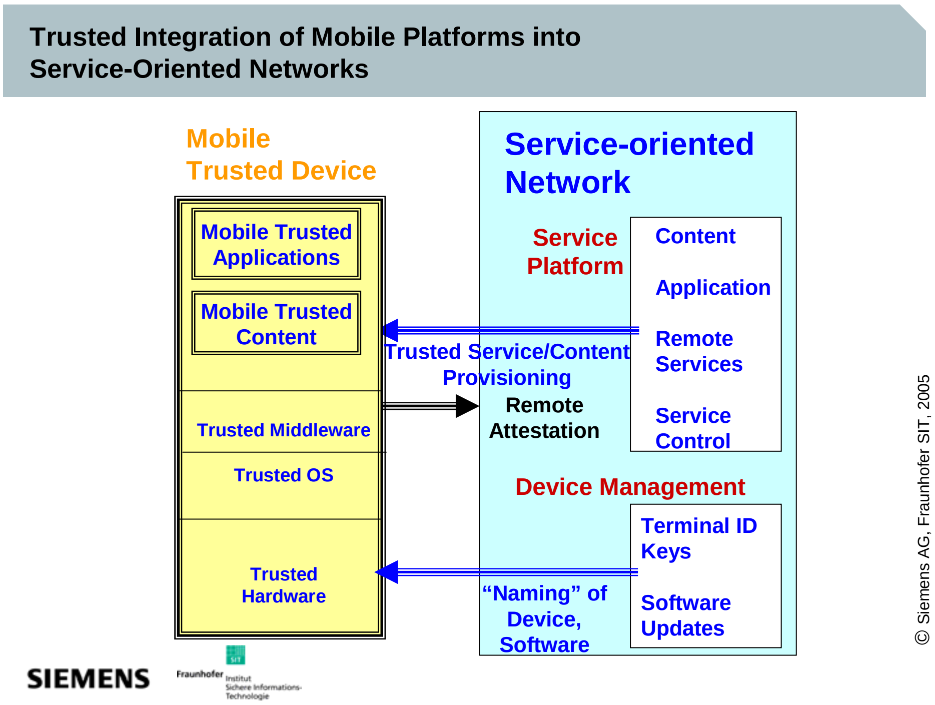

Figure 1:: Trusted Integration of Mobile Platform into Service-Oriented Networks

References

Michiharu Takemoto, Hiroshi Sunaga, Kenichiro Tanaka, Hiroaki Matsumura, Eiji Shinohara: "The Ubiquitous Service-Oriented Network (USON) — An Approach for a Ubiquitous World Based on P2P Technology," *Second International Conference on Peer-to-Peer Computing,* p. 17, 2002. http://doi.ieeecomputersociety.org/10.1109/PTP.2002.1046307

Trusted Computing Group: https://www.trustedcomputinggroup.org/home

Trusted Mobile Platform: http://www.trusted-mobile.org/