Mobile Signature Service Provider

Methics is an independent consulting company located in Finland. Methics has developed PKI and wireless PKI products for application providers, and built unique security and performance testing tools for mobile operators. In consulting the company focuses on system testing and security auditing of system deployments.

Introduction

The increasing need for trusted devices is foreseeable. The need for secure authentication and safe digital signature based proof of consent is becoming imminent, eCommerce being the major driving force. Despite of the availability of required technology, no sound infrastructure for digital signatures is available today, neither on Internet nor wireless mobile networks. The position is open and is to be filled in.

The role of digital signature infrastructure provider has been suggested for the mobile operators. In this model, the mobile operators would enable their subscribers to digitally sign application provider transactions; mobile phones would grow into personal trusted devices. The operators would become *Mobile Signature Service Providers (MSSP)* and providing digital signatures for the application providers would become a new service in the operators' service offering.

European Telecommunications Standards Institute (ETSI) has defined concisely MSSP as *"a person or entity enabling the generation of Mobile Signatures by Signers and the use of Mobile Signatures by Application Providers."* [2] Figure 1 illustrates the MSSP concept further.

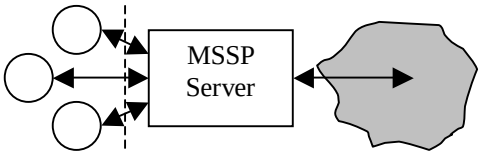

Figure 1 – Mobile Signature Service Provider consists of a MSSP server and subscribers. The MSSP server is the gateway for application providers (represented by the circles) to request digital signatures from the MSSP's subscribers (the dark cloud). The dashed line separates the application provider and MSSP domains.

The GSM mobile operators of today have the largest deployed network infrastructure supporting secure end user authentication and communication. Clearly, the mobile operators have a significant asset in their hands. The interesting question that remains to be answered is how this valuable asset could be used to build and operate an infrastructure that enables the aforementioned security services.

Starting a MSSP service requires solutions for five main issues: 1) which standard private key storage technology is used [PKI enhanced Subscriber Identity Module (SIM), Wireless Identity Module (WIM) or combined SIM and WIM (SWIM)]? 2) How subscriber registration is implemented? 3) Which MSSP implementation strategy is used? 4) What is the MSSP business model? 5) How is trusted transaction roaming between mobile operators implemented?

This paper introduces the requirements for MSSP functionality and the available strategies for the mobile operators to implement the MSSP functionality.

MSSP Requirements

From the mobile operator's point of view the role of MSSP composes a new mobile service, which combines classic value added mobile user services and Internet application provider services. It's ultimately this specific service nature that defines the requirements for a MSSP and its implementation. In general, the requirements the new service sets can be divided into three categories: 1) subscriber management, 2) charging and billing, and 3) transaction requirements. In the following more detailed requirements of each category are discussed.

In practice, digital signing requires that the end user possesses a special identity module. This practical requirement renders the actual logistics requirements for MSSP. First, the identity module; namely a PKI enhanced SIM, WIM, or SWIM must be delivered to a subscriber. Second, a reliable registration of the security credentials on PKI SIM/WIM/SWIM and the identity of the signer (subscriber) must be done. Then MSSP is able to publish these bindings, called digital certificates. From application provider's point of view it's essential that in the ongoing technical battle between PKI enhanced

SIM/WIM/SWIM, the mobile operator remains neutral. The MSSP implementation must support all three technologies.

The transaction flow discussed next illustrates the diversity of key functional and non-functional requirements MSSP has to meet.

From MSSP point of view a transaction begins when an application provider contacts the MSSP. MSSP provides its services across organization borders over public network. Thus, it's required that the security of the interface is well-taken care of to prevent unauthorized use of MSSP. Clearly, well-defined processes to manage the application providers are required.

As the transaction processing continues, it's essential for MSSP that a comprehensive audit trail is generated; the audit trail enables the generation of charging information to be fed further into the billing system. MSSP billing is more content charging than traditional telecom charging as MSSPs can establish variety of new value-added Internet services which charge, based on the application itself, and not based on the connectivity.

The application provider sees the MSSP transaction as a sub-transaction of its own transaction which an end user has initiated. As application providers integrates these transactions, the transactions become highly dependent on the MSSP. In fact, the Quality of Service (QoS) of MSSP limits the QoS of the application providers. Availability and performance matters of the MSSP's application provider interface should be solved by using well-established Internet techniques. Figure 2 shows the relationship of these two types of transactions.

When the number of application providers increases, proprietary and different MSSP interfaces become an unnecessary burden for the application providers to cope with. Such interfaces will delay considerably the application providers' service integration and overall acceptance of a new type of service. Ideally, all MSSPs implement a common service interface that binds the digital signature transaction of MSSP to the application provider's transaction. Clearly, the MSSP service interface must be standardized.

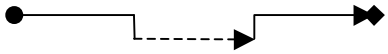

Figure 2 – The relationship of a user initiated application provider transaction (the upper solid arrow) and a MSSP transaction (the lower dashed arrow) initiated by the application provider. The vertical lines mark communication occurring between the application provider and MSSP. The dark circle and rectangle start and end the application provider's transaction.

Implementation strategies

Today the GSM mobile operators have different technologies available to become a MSSP. Next, these approaches are discussed in the light of requirements introduced above. The focus shall remain strictly in the MSSP server which is the actual system providing the application provider interface.

Open Mobile Alliance's (OMA) Wireless Application Protocol (WAP) has defined a standard interface for WAP pages to access the digital signature functionalities of WIM and SWIM [4]. Similarly, ETSI has defined an interface to access GSM mobile phone's SIM in a secure manner (so called OTA interface [1]).

Figure 3 illustrates the essential difference between these two technologies. It is the communication path from the MSSP server to the trusted device (mobile phone) and its credentials on PKI enhanced SIM (or WIM/SWIM). However, it must be emphasized that it's irrelevant for MSSP which the actual transport to the PKI SIM/SIM/WIM/SWIM is.[1] MSSP only requires standard formatting of digital signatures (PKCS #7) which all aforementioned identity modules do support.

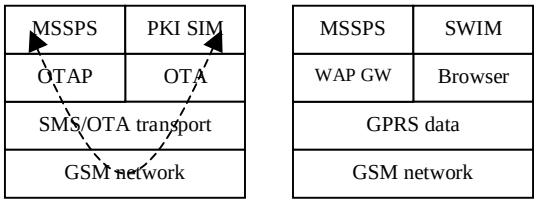

Figure 3 – The protocol stacks for both WAP (on right) and OTA (on left) based digital signature transactions. The dashed arrow shows how the information flows in the stacks from the MSSP server (MSSPS) to the digital signature capable SIM/WIM/SWIM and vice versa. (OTAP = Over-The-Air SIM management platform)

[1] In practice, OTA platforms are capable of providing a WAP look-alike interface to the PKI SIM.

For a GSM mobile operator (without strong commitment to WAP) enabling digital signature transport means introduction of a service interface (MSSP server) and upgrading of the existing SIMs to support PKI. These actions are sufficient to enable transmission of digital signatures between application providers and the operator's subscribers. On the other hand, to accomplish the same, a WAP operator introduces WIM/SWIM cards and a MSSP service interface for its application providers. In both cases the existing network infrastructure requires no further modifications or enhancements as such. All interfaces involved have already been standardized (the MSSP service interface for the application providers being the latest [3]). To conclude, the required new components are technology (WAP, OTA, SIM, WIM and SWIM) independent and based on standards.

As discussed above, the user identities must be bound to their WIM/SWIM/SIMs. An infrastructure for the binding process must be established. The process may reuse an existing Certification Authority (CA) infrastructure, if such is available, however. The actual binding entity is called Registration Authority (RA). The binding process requires verification of user's identity, and thus customer service locations, users become subscribers at, are natural locations for RA points. Figure 4 below depicts the binding process.

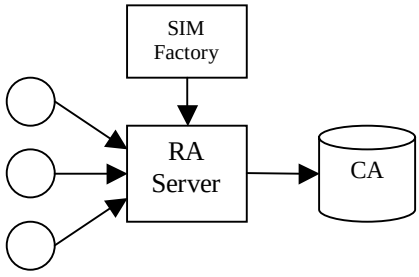

Figure 4 – SIM shops (circles) become RA points (clients) that verify user identities thus binding a PKI SIM/WIM/SWIM and identity. Once the identity is verified certificate enrollment is triggered resulting to the publishing of a digital certificate into CA.

The two technologies have both heavy optimizations in place to minimize the data transfers occurring during digital signature transactions. The signatures SIM/WIM/SWIMs generate and send require a special transformation in order to be usable for application providers.[2] Transformation process requires subscriber specific information, namely the digital certificate. Thus, MSSP server must have access to the CA storing the digital certificates. MSSP server requires no other subscriber information and thus MSSP server requires no active subscriber provisioning, it simply relies on the information CA already has. As a result, the MSSP server has no direct connection to the binding process and RA; instead, the CA is the interconnecting element.

Unlike the subscribers application providers do require provisioning into MSSP server. MSSP provides a *non-free* digital signature *service* for them. MSSP server must have access control mechanisms in place to prevent unauthorized usage of its service.

Charging and billing is straight-forward from MSSP server point of view. It has the necessary information available about the charged transactions: it has information about the involved parties (subscriber and application provider), time, and the type of transaction. The question is merely integrating the MSSP server to the billing system of the mobile operator, i.e. in practice generating proper Charging Detail Records (CDRs) for the billing system.

Conclusions

Implementing the MSSP functionality and fulfilling the MSSP requirements is straight-forward – even though there are two different digital signature transmission technologies to choose from. From MSSP point of view the differences are minimal. Moreover, it is possible to choose an implementation strategy that builds the required functionalities on top of existing network components. This maximizes the usage of the investments as the existing components are leveraged more efficiently.

The required MSSP components and interfaces have lately become standard. Clearly, this important milestone that has been achieved opens new possibilities for both application providers and mobile operators. Instead of solution providers, standard component providers may be used. The field is now open for all players.

[2] SIM/WIM/SWIM generated signatures are in WAP signedContent format which differs from the standard Internet PKCS #7 signedData format.

To summarize, the key problem of becoming a Mobile Signature Service Provider is not the MSSP implementation itself. Instead, the real hurdles to tackle are the challenges related to the business model, the certification process of subscribers, and transaction roaming.

References

[1] *TS 101 181 v8.8.0 Technical Specification; Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2*, ETSI, 1.12.2001.

[2] *TR 102 203 v1.1.1 Technical Report; Mobile Commerce (M-COMM): Mobile Signatures; Business and Functional Requirements*, ETSI, 3.6.2003.

[3] *TS 102 204 v1.1.4 Technical Specification; Mobile Commerce (M-COMM): Mobile Signature Service; Web Service Interface*, ETSI, 28.8.2003.

[4] *WMLScript Crypto Library*, WAP Forum, 2001.6.21.