



Digital Signatures pave the way for Mobile Banking and Commerce

Strong authentication and integrity are necessary security features when parties communicate using a mobile network. The security measurements enforced on the users must provide the state-of-art technology and at the same time be as easy to use as bank cards in ATMs. Public Key Infrastructure (PKI) is a mature and well established technology to enable a secure channel between users and service providers.

The Challenge

The digital age has brought with it new threats like identity theft and man-in-middle attacks. These are increasing together with the growing usage of electronic transactions. To prevent the fear of these threats from hindering the use of convenient remote services security techniques must be in place that give both the service providers and the end users the peace of mind required.

Combining ease of use for the end user and high security is a difficult task. However, this task must be achieved; otherwise the services will not be used.

For a successful deployment a security solution must work on all handsets and for multiple use cases. For a bank or merchant it must be possible to reach their customers independent of the mobile operator their customer is currently using.

The Solution

SmartLicentio is a Mobile Signature Service Platform (MSSP). It provides mobile signature service functionality for applications and operators to establish a standards based and secure channel between end users and business applications.

SmartLicentio is based on the latest Java technology and system design. It consists of three server modules.

- MSSP Server handles messaging and validation,
- MSSP Management takes care of service management
- MSSP Reporting provides auditing and reporting data for billing.

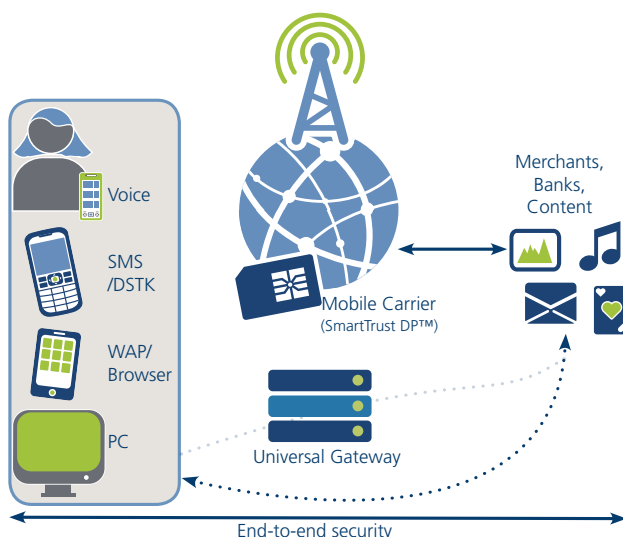
Benefits

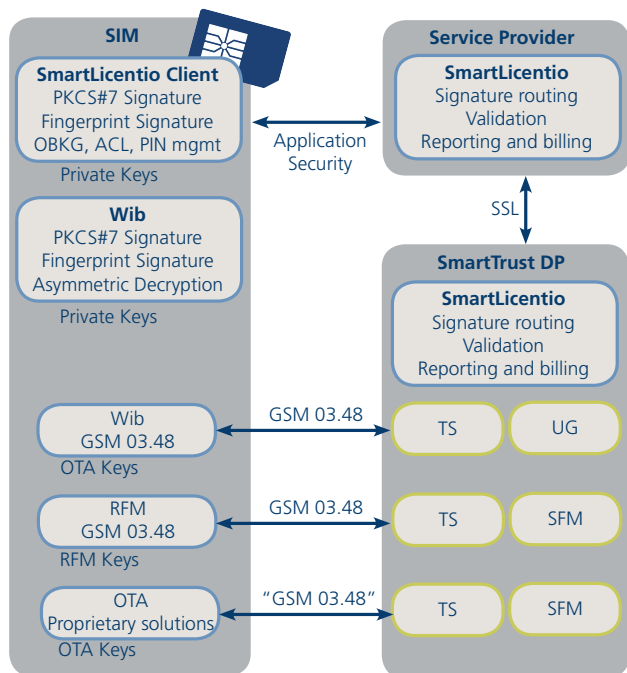
SmartLicentio provides a scalable, high availability messaging and validation platform for signature services. Additionally, multiple MSSP roles (Routing, Acquiring and Home MSSP) can be managed separately. Each server can be managed independently allowing message routing to be handled based on business needs.

The mobile operator has a unique combination of assets;

- Tamper-resistant Smart Card - the SIM
- The mobile network - a secure, trusted and well managed environment
- Trusted brand
- SIM Personalization routines
- SIM and PIN mailer distribution
- Point of Sale with skilled personnel
- Supporting systems

All these make the mobile operator well positioned to take the role as an identity provider and security enabler. SmartLicentio is the tool that helps mobile operators leverage their unique assets to enable mobile electronic transactions.





Features

Mobile Signature Messaging

- SmartLicentio routes MSS signature requests from applications to end users. End users can sign the requests by using their mobile phones with WPKI SIM cards. It handles MSS roaming, signed message validation and routing back to the application provider.

Web Services for Application Providers

- SmartLicentio provides a SOAP interface for application connectivity. Java (1.5 or 1.6), JAAS and Perl APIs are included for application integration.

Application Provider Management

- It includes a browser-based user interface for managing application provider lifecycles.

Mobile User Profile Management

- SmartLicentio provides a Java API interface for provisioning Mobile User profile information.
- In addition it supports Mobile User profile management with a browser-based user interface.

Billing and Reporting

- SmartLicentio's logging management extracts technical transaction data to a business transaction storage database. This provides an integration point to fraud control systems, document management and billing systems.

The Future

Mobile commerce and banking is predicted to grow as the number of subscribers continues to grow and new technologies are introduced. For instance, Near Field Communication (NFC) enables applications for device proximity payments and ticketing. The SIM will be a Secure Element (SE) and carrier of the mobile electronic identity (e-ID) with the means to digitally sign whatever data that needs to be protected, for example the payment for an event ticket to be downloaded Over The Air (OTA) to the SIM.

Other security aware services like logging in to a secure web site or VPN will benefit from the e-ID and the handset/SIM as the security token. The need for a convenient way to authenticate users is increasing as the number of e-services grows. The SIM as the portable security device that always is within convenient reach is being used more often and makes the use of user IDs and passwords obsolete.

SmartLicentio

SmartLicentio is a Java based signature, routing and verification server software running on Sun Solaris and Linux. It has a high transaction throughput enabling security aware services for strong authentication and digital signatures for integrity protection and non-repudiation. It works with SmartLicentio Client™ as well as SmartTrust Wib™. It supports built-in and external audit logging services. The system monitoring is based on SNMP.

The key components of SmartLicentio are:

Routing

Flexible rule-based SOAP routing. Routing can be based on message elements or external routing services like number portability.

Security

Supports independent SSL connections for integrated services. Validation is based on FIPS 140 certified validation module. SSL certificates and certificate revocation lists can be operated without any service breaks

Standards

Signature Verification as per RFC 3280 and PKCS #10, MSS compatibility according to ETSI TS 102 204 and 102 207.

Related SmartTrust Products and Services

SmartLicentio Client™

A standalone Java based SIM security client using the encryption keys for signature creation.

SmartTrust Broker™

Performs RAM operations on Security Domains according to the GlobalPlatform standards including Supplementary Security Domain creation, loading and personalizing applications as well as allocating keys.

SmartTrust endeavors to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission. The development of SmartTrust products and services is continuous and published information may not be up to date. It is important to check the current position with SmartTrust. This document is not part of a contract or license save insofar as may be expressly agreed. SmartTrust is a trademark of SmartTrust AB. All other trademarks are the property of their respective owners. SmartTrust is a part of the Giesecke & Devrient Group.

© SmartTrust January 2010. All rights reserved.

For more information about SmartTrust, please visit us at www.smarttrust.com