White Paper

(Wireless) Enterprise PC Security

Author: Sten Lannerstrom, SmartTrust

Document number: MPM02:0015

Revision: A

(Abstract)

From a security perspective the traditional handset could become a “personal trusted device” (PTD) as its internal structure already carries a smart card capable of storing private credentials and encryption keys.

With a Wireless Enterprise PC Security concept, the mobile handset is not just a phone, but also the world’s most commonplace smart card reader. The SmartTrust security solution allows any compliant PC application to utilize the SIM’s security mechanisms. This makes it possible to use a handset as a secure device, e.g. for the signing of e-mails and strong client authentication during remote access among other security related tasks.

The Wireless Enterprise PC Security concept allows Mobile Operators to offer a complete mobile security service for enterprises. The service offering from the mobile operator side could typically be based on bulk of messages- or per transaction oriented charging.

For readers requesting a more in-depth coverage of solutions from SmartTrust we suggest visiting our web site at http://www.smarttrust.com/ where you can find information about solutions for managing and securing mobile services, topics like Roaming Management, Infotainment and Wireless Security.

Revision: A, September 12, 2002

Next revision not later than: *March 12, 2003*

Document Number: MPM 02:0015

About SmartTrust

Through our offerings we allow organizations within the mobile ecosystem to deliver mobile e-services that inspire confidence and convenience in the sharing and trading of online information, products and services

By supporting multiple generations of networks and mobile devices, SmartTrust is able to offer the best end-user reach possible to more than 75 mobile operator customers and 150 corporate customers.

More information about SmartTrust is available at http://www.smarttrust.com.

FINLAND

Sonera SmartTrust Oy
P.O. Box 425,
FIN-00051 SONERA
Elimäenkatu 17-19, Helsinki
FINLAND
E-mail: info@smarttrust.com
Tel: +358 (0) 2040 63031
Fax: +358 (0) 2040 6213

SWEDEN

Sonera SmartTrust AB
Årstaängsvägen 21 B,
Box 47154
SE-100 74 Stockholm
SWEDEN
E-mail: info@smarttrust.com
Tel: +46 8 685 93 00
Fax: +46 8 685 65 30

UNITED KINGDOM

SmartTrust Ltd.
112 St Leonards Road,
Windsor Berkshire,
SL4 3DG
UNITED KINGDOM
E-mail: info@smarttrust.com
Tel: +44 1753 620 262
Fax: + 44 1753 842 773

BENELUX

SmartTrust
Rue du Baukion, 28
B-1370 Jodoigne-Souveraine
BELGIUM
E-mail: info@smarttrust.com
Mobile +32 (0) 477 70 70 09
Tel +32 (0) 10 88 09 25
Fax +32 (0) 10 88 09 26

GERMANY

SmartTrust GmbH
Firkenweg 7
D-85774 Unterföhring
GERMANY
E-mail:info@smarttrust.com
Tel: +49 89 85 635 0
Fax: +49 89 85 635 111

ITALY

Sonera SmartTrust
Via Torino 2
20123 Milano
ITALY

E-mail: info@smarttrust.com
Tel: +39 02 725 46 221
Fax: +39 02 725 46 400

SPAIN

SmartTrust Spain
Paseo de la Castellana 93-4º
28046 Madrid
Spain
E-mail: info@smarttrust.com
Tel: +34 91 418 5013
Fax: +34 91 555 9957

AUSTRALIA

Sonera SmartTrust Pty Ltd.
Level 31, Aurora place
88 Phillip Street
Sydney NSW 2000
Australia

E-mail: info@smarttrust.com
Tel: +61 2 8211 0488
Fax: +61 2 8211 0555

CHINA

Suite 1413, Tower B, COFCO Plaza
No.8, Jianguomennei Dajie
Beijing, China (100005)
Email: info@smarttrust.com
Tel: +86 10 6525 3523
Fax: +86 10 6525 2671

HONG KONG

Sonera SmartTrust Limited
Unit 902
CyberPort 2
100 CyberPort Road
Pokfulam, Hong Kong
E-mail: info@smarttrust.com
Tel: +852 3121 6888
Fax: +852 2918 9108

INDIA

Room 212, Paharpur Business Centre
Nehru Place Greens, New Delhi - 110019 India
Switchboard: +91 11647 4701
Fax: +91 11620 7556

E-mail: info@smarttrust.com
Tel: +91 1145 11678

MALAYSIA

Sonera SmartTrust Sdn Bhd
Level 40 Tower 2
Petronas Twin Towers, KLCC
50088 Kuala Lumpur
Malaysia
Fax: +603 2168 4654

SINGAPORE

SmartTrust Pte Ltd.
8 Temasek Boulevard
Level 44 Suntec Tower Three, Singapore 038988

E-mail: info@smarttrust.com
Main Tel: +65 6866 3788
Tel: +65 6866 3786
Tel: +65 6866 3789
Fax: +65 6866 3787

UNITED STATES of AMERICA

Sonera SmartTrust US, inc
5800 Granite Parkway, Suite 300
Plano
TX 75024 USA
E-mail: Info@SmartTrust.com
Tel: +1 972 731 2685
Fax: +1 972 731 2695

LATIN AMERICA

SmartTrust Latin America
R. Oscar Freire, 379 Conj. 121g
Sao Paulo SP 01426-001
Brasil
E-mail: info@Smarttrust.com
Tel: 5511 9983 2079
Tel: 5511 9628 7815
Fax: 5511 3064 3042

Document number: MPM02:0015
Revision: A

Contents

Document number: MPM02:0015
Revision: A

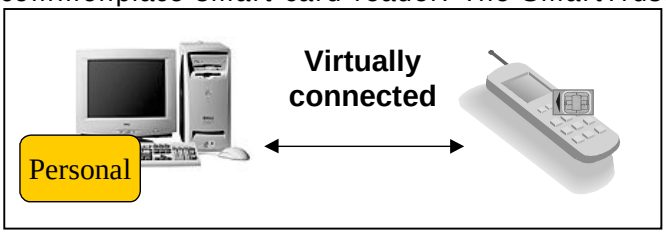
Introduction

Many analysts predict, and figures already show, that ARPU[1] based on pure voice airtime will decrease over the coming years. New messaging data services can and will balance the reduction in voice revenue, if properly exploited. Using messaging services has already become an everyday event by many young users. However, most of them have a very limited spending capacity. Attracting the average business user has been a tougher challenge although they represent a much more promising market segment.

Data services are promising to be the way to attract this financially stronger segment. With data comes a challenge and opportunity for mobile operators. New wireless services, such as security services, can be offered. Security is closely linked with cost and smart card usage has often been desired but forsaken due to the cost of implementation. However, the SIM card inside a traditional GSM phone can also be used as a security token providing mechanisms for digital signatures, authentication and encryption.

Security services are becoming a standard part of many applications in the PC environment. Secure e-mail is perhaps the most obvious but there are several other applications that are security enabled without yet having caught the users' attention. By having a solution that can combine mobile services in general with the top class security mechanisms that modern SIM cards can supply, it is possible for mobile operators to target entire enterprises with an attractive service offering. The list of application areas for an enterprise that benefits from security can be long; secure web access for intra- and extranet, VPN, e-mail and other office applications.

With the Enterprise PC Security concept using SmartTrust Personal on the client side, the mobile handset is not just a phone, but also the world's most commonplace smart card reader. The SmartTrust security solution allows any compliant PC application to utilize the SIM's security mechanisms. This makes it possible to use a handset as a secure device, e.g. for the signing of e-mails and strong client authentication during remote access among other security related tasks.



Offering Public Key Infrastructure (PKI) for an enterprise is within reach for today's mobile operators. The solution from SmartTrust is ready to be used with any modern SIM enabled device supporting GSM 2+, which essentially covers all handsets made the last three years. The mobile operator can take the Certification Authority (CA) role, should this be a strategic business decision, but an existing Trusted Third Party (TTP) can equally well host this role.

[1] Average Revenue Per User

Security Background

Security Services

Protocols for data communications were initially based on static identities and the devices were stationary. There were several competing concepts but eventually IP won and has since evolved to be dynamic, mobile and even wireless.

Security concerns has been an issue ever since man started to communicate (and this happened slightly prior to the invention of IP… ;-). Most commonly people think of confidentiality when security is mentioned, but security services can generally address the following four areas; confidentiality, integrity, authentication and non-repudiation.

Cryptography has long been able to solve most security concerns but lacked proper management and control of the encryption keys, which became a cumbersome task to administrate. The invention of asymmetric encryption and PKI in the late 70's and the possibility to store encryption keys in tamperproof smart cards resulted in a viable, but expensive, way to overcome management issues. Smart cards with capabilities to handle asymmetric encryption had initially less memory than desired and were far to expensive for a large scale deployment. Additional drawbacks were the necessity of additional hardware, the smart card reader, and the lack of hardware standardization. Smart card based solutions are still fairly expensive and the hardware problem remains although standardization efforts have made a huge impact, especially on software implementations, and this reducing cost.

The invention of HTTP back in the early 90's gave PC based browser tools with graphical easy-to-use user-interfaces. As a result of this the growth of PCs being connected to the Internet was enormous. Security issues were addressed practically from day one but were not easy to resolve in a user friendly and secure way. Private keys, necessary for asymmetric encryption used in e.g. SSL (HTTPS), could easily be stored in files but tamperproof storage such as in smart cards still required the additional reader hardware and the business model for providing them remained an unsolved query.

Mobile Networks

Alongside and with a similar growth as the Internet came mobile networks, and especially GSM. In recent years there has been an overwhelming growth of mobile handsets, once dedicated only for voice services but they are now becoming very advanced devices, hosting considerable processing power.

In mobile networks based on GSM, GPRS and 3G there is a Subscriber Identity Module (SIM) present in the form of an Integrated Circuit Chip (ICC) card. In essence the SIM card is a smart card imbedded in the mobile equipment. The plastic size of the SIM card is usually in the smaller (ID-00) "plug-in" format rather than "full-size" (ID-1), typical credit card size.

Nevertheless, the SIM is a smart card and can be equipped with a fully functional ICC capable of processing.

A new landscape of opportunity

Traditional handsets are now becoming mobile devices capable of providing local application support. One step in this direction was the invention of SIM Application Toolkit (SAT) and another was support for the asymmetric RSA process within a standard SIM card.

Restricting factors for PKI usage in the past has typically been lack of legislation for digital signatures, export restrictions on strong encryption and the availability of established Public Key Infrastructures (PKI).

Now the landscape is different. Laws exist giving digital signatures equal standing to traditional signatures. Encryption export restrictions have essentially been lifted and several Trusted Third Parties (TTP) can now offer Certification Authority (CA) services for PKI. The remaining issue, having mass-market tamperproof security tokens out in a business environment, can now be accomplished by using the SIM, inside a (GSM/GPRS/3G) mobile handset as the security token.

Personal Trusted Device

From a security perspective the traditional handset could become a “personal trusted device” (PTD) as its internal structure already carries a smart card capable of storing private credentials and encryption keys. Likewise “smarter” devices such as PDAs with GSM/GPRS/3G support can equally make use of security features, such as digital signatures, becoming available through the SIM.

A personal trusted device can be defined as something you always have with you – a device that offers so much value in so many environments that you never leave home without it. With the correct infrastructure in place a mobile phone could quickly gain acceptance as a personal trusted device, enabling the user to make secure transactions in a multi-channel environment. Such a development would, in turn, see the traditional mobile operator evolve into a ‘Trusted Operator’.

The Delivery Platform, developed by SmartTrust, is unique in its ability to support the full range of services required for managing SIM cards and mobile devices. The Enterprise PC Security concept described here is just one out of many application scenarios available with the Delivery Platform.

Enterprise PC Security

What it is…

The Enterprise PC Security concept is especially suited for the enterprise market, as it allows the mobile handset to act as a locally connected smart card in the everyday office environment. Applications executing in a workstation can utilize the SIM card within the mobile device as a security token carrying private keys.

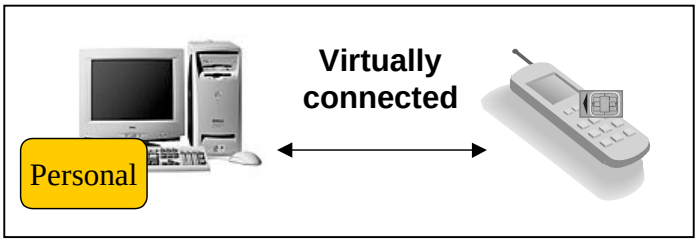
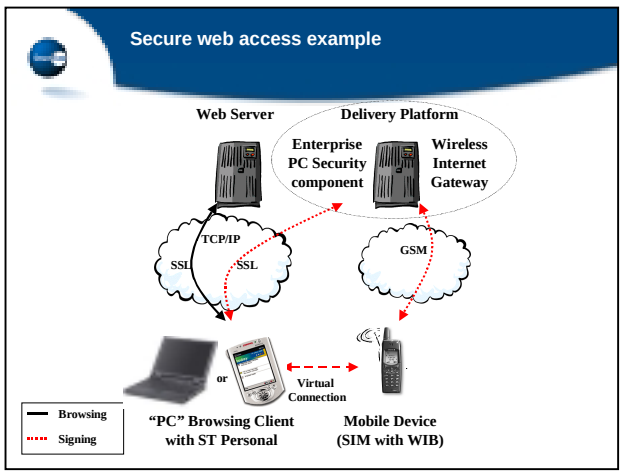


Figure 1. Virtually connected mobile device

The mobile handset becomes a virtual part of the workstation hardware. This enables the application to support encryption, authentication and digital signatures.

Smart cards are commonly considered to offer the highest level of security but the logistics and costs of wired smart card readers has been a prohibitive factor. One way to alleviate this, while still having the high level of security with smart cards, is to use a PKI-enabled SIM card as the key storage device, and the mobile equipment (ME) as the smart card reader.



When an application requests a security service, e.g. a digital signature or decryption of data, the request is directed from the application through the Delivery Platform, where both the Enterprise PC Security component and the Wireless Internet Gateway resides (figure 2), and furthermore towards an ordinary SIM enabled mobile phone.

Figure 2. Secure Web Access Example

The secure web access example above shows how SmartTrust Personal redirects the signature request through the Delivery Platform towards the mobile device. From the perspective of the PC client the mobile device become a virtually connected piece of hardware. This scenario can be used with practically any kind of application where security mechanisms are required locally such as with secure e-mail and VPN usage.

Document number: MPM02:0015
Revision: A

A major advantage is that the server side does not need to know anything about how the security device, actually handling the signature request, is connected. From the server side this is transparent and it is up to the client to ensure a proper link with its security token, i.e. the mobile device in this case.

Another advantage, compared to using a file-based solution where the security token is just a file in the PC, is the issue of trust between the client and the security token. Having the security token within the mobile device, typically the users phone, the user is in a physical possession of something easy to carry and protect. If the device is lost the PIN, different from opening the device, protects from unauthorized operations of the security mechanisms. It is additionally possible to revoke the certificate linked with the keys inside the security token.

Application areas

Secure intranet and extranet

The most successful usage area based on PKI today is securing web access through SSL or TLS with standard Internet browsers. The web server involved has a set of private keys and an issued certificate from a Certification Authority (CA) and the typical browser client in a PC has a set of trusted CAs in its internal store. The client can then authenticate the web server as a part of the standard communication protocol. The user can configure to what degree the authentication process should be visible.

Being able to authenticate the content provider, i.e. the web server through its certificate, is beneficial for the user at the client side from several aspects; the user “knows” whom the remote party is, the communication session becomes confidential and data sent in both directions is integrity protected. The user should be comfortable trusting that the connection is established with the expected provider and that all data is secured during transport over the Internet.

However, the most common approach with secure web access is based on anonymous clients, i.e. the web server is not requesting strong client authentication. The Enterprise PC Security concept allows for strong PC client authentication based on using private keys residing in the SIM within the mobile handset. It will operate as if the mobile handset was a locally connected reader with smart card inserted. An enterprise can benefit from this having their intranet and extranet solutions secured using strong client authentication. SmartTrust Personal on the PC client side works with most standard browsers such as Microsoft Explorer and Netscape Communicator.

VPN access control

Virtual Private Networks (VPN) are becoming increasingly popular, allowing employees to access the LAN remotely with the same access rights as if they were locally attached to the network. Once being authenticated and access is

granted, the user has access to the LAN as anyone else being physically on-site.

VPN solutions are often based on a password approach, sometimes even with static passwords. The use of static passwords is not very secure and systems or applications protected only by such passwords are quite often vulnerable to attacks. Static password systems are additionally of little value on a mass-scale, as they require a great deal of back-office administration. Passwords can be stolen or copied and are surprisingly often written down on paper and even attached to a computer monitor. Access is granted as long as a correct password is entered. An entity controlling certain information has no way of telling who is actually on the other side unless strong authentication based on digital certificates is used.

VPN solutions based on PKI and digital signatures provide for a much more controlled environment through the use of strong authentication. Any solution package with VPN clients based on standards (Microsoft Crypto API and PKCS #11) can be used with SmartTrust personal in the Enterprise PC Security concept. It then becomes possible to utilize the SIM in the mobile handset as the security token required for strong authentication. Having strong client authentication with the use of certificate information for access authorization provides for a VPN solution capable of being highly secure, flexible to use and easy to maintain.

Secure e-mail

Secure e-mail has probably been the most discussed application area on the Internet. As e-mail solutions have been around for quite a while there are a vide variety of e-mail clients, the more modern ones more coherent to open security standards than the older ones. E-mail, not being secured, has been around for over three decades now and issues around the lack of security is a burden for anyone responsible for enterprise information security.

With the Enterprise PC Security concept it is possible to utilize secure e-mail by having the SIM within the mobile device as the security token for execution of digital signatures and message decryption.

Whenever the user desires, e-mails can be digitally signed. All the user needs to do is to acknowledge that the signature should take place, by entering the correct PIN for the signature key on the handset.

Receiving encrypted e-mails work according to a similar principle as when signing. When the encrypted e-mail is selected for reading, the wrapped key is decrypted within the handset and securely returned to the e-mail client for actual message decryption. *Almost every modern secure e-mail system use the principle of having the "message" part encrypted by a volatile symmetric key and then having the symmetric key transformed (wrapped) by an asymmetric process.* Sending encrypted messages does not involve any operations within the handset as this process only operates on the public key

of the receiving parties. The public key is a part of the recipient's digital certificate.

E-mail clients supporting Microsoft Crypto API and PKCS#11 are supported by SmartTrust Personal and work seamlessly in the Enterprise PC Security concept. Two widely used e-mail clients that may serve as examples are Microsoft Outlook, based on MS Crypto API, and Netscape Messenger based on PKCS#11.

Using signatures in the traditional office environment

In a Microsoft XP environment Microsoft Word is prepared for the signing of documents, and so is Microsoft Excel as well. Tools for making electronic forms to be used in a web environment have had this signing capability for several years although seldom being used to their maximum potential.

Other applications offering security services

Because SmartTrust Personal implements the PKCS#11 standard and includes a Microsoft Cryptographic Service Provider (CSP), it can be integrated seamlessly with a number of third party products. Any application supporting Microsoft CAPI or PKCS#11 security standard interfaces allow the use of the SIM, inside the mobile device, as a virtually connected security token. With the Enterprise PC Security concept from SmartTrust, available at the mobile operator side, and SmartTrust Personal installed on a workstation PC client, the mobile handset act as a virtually connected smart card reader to a workstation PC.

Business Benefits

Mobile Operator perspective

The Enterprise PC Security concept allows Mobile Operators to offer a complete mobile security service for enterprises. The service offering from the mobile operator side could typically be based on bulk of messages- or per transaction oriented charging. In combination with other, non-security related, capabilities within the Delivery Platform a Mobile Operator can provide an offering for an enterprise that could include:

- Voice services for an entire enterprise
  - Indirect subject as a result of a complete offering
- The mobile device available as a security token for all employees
  - Direct subject from Enterprise PC Security
  - Enabling a variety of applications mentioned above
- Special roaming management for the enterprise where applicable
  - Direct subject from OTA capabilities within DP
- Premier message distribution through dedicated servers

- Direct subject from WIG/DP SMSC configuration

- Trusted Archive of Secure Transactions
  - Direct subject from using Security Services Portal within TOS
  - A high level interface for handling secure e-commerce transactions
- An tailored menu structure on every handset dedicated for the enterprise
  - Direct subject from WDM within DP

Enterprise perspective

From an enterprise perspective the Enterprise PC Security concept incorporate the following benefits:

- One supplier of mobile services should provide better control of the total wireless cost
  - Reduction on the overall cost compared to ad-hoc based subscriptions
  - Less costly cross-country network selection through dedicated roaming
- One supplier of mobile services should provide for better performance
  - Having dedicated message routing services at the operator side should give capability of premier response times
- Usage of mobile phones for internal calls as if they were fixed phones
  - Call set up on the mobile device can be accomplished from using a PC application if desired
- Less expensive – no separate security tokens
  - High-end security solution at a lower cost as compared to a separate deployment of security tokens
- Future proof investment as the security concept is based on existing standards
  - The SIM browser concept is included in the 3G specifications
  - Cryptographic support based on open standards
  - Public Key Infrastructure support based on open standards
- Better security – PKI with tamperproof security tokens

Enterprise PC Security System Description

General

The Enterprise PC Security concept consists of two parts, a client and a server part. The client part consists of SmartTrust Personal, extended to allow the use of a SIM Card in a cellular phone as a key storage device. The SIM Card must contain a Wireless Internet Browser (WIB) with a plug-in for making RSA signatures, as well as the necessary private key.

The Enterprise PC Security server component acts as a front-end to the Wireless Internet Gateway (WIG) and offers the clients the required services. The Mobile Operator or the Enterprise can host this server component. The business model directed and typically controlled by the Mobile Operator determines the actual location of the server part.

Figure 3 below shows how Personal communicates with the SIM Card through a Server component, connected to a SmartTrust Delivery Platform-WIG, which is able to communicate with the mobile phone through the use of SM. The Enterprise PC Security server component acts as a front-end to the WIG and offers the clients the required services. SSL is used to protect the transmission between the client PC and the Enterprise PC Security server component.

For more information about the WIG and WIB concept, contact SmartTrust.

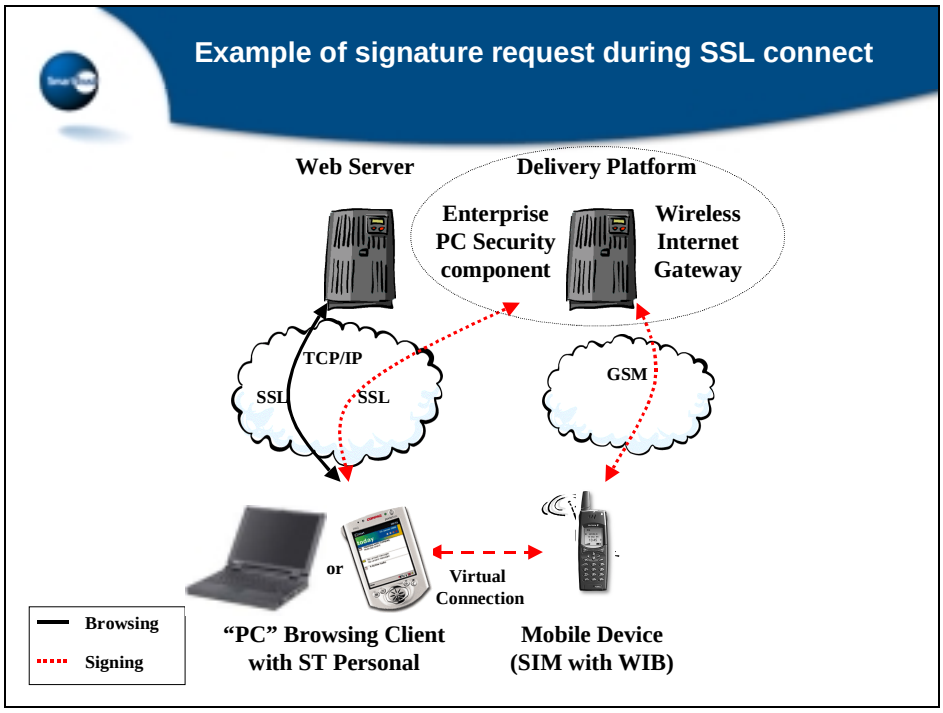


Figure 3 Communication flow while requesting a signature

Accessing the SIM as a security token

Accessing the SIM as a security token can be done in essentially two ways, through a virtual connection or through direct physical access. Furthermore the SIM needs to contain the Wireless Internet Browser (WIB) and (3) specific plug-ins. The required plug-ins are:

- P7 - Signed Text, for text signatures and WAP compliant output
- FP – Fingerprint, for signing binary content, and
- AD - Asymmetric Decrypt, for unwrapping symmetric keys (decrypting)

Virtual Connection

A virtual connection implies that the mobile device is accessed over-the-air and this can be accomplished through using a Delivery Platform WIG push concept. The security client needs to resolve the link between the PC-device and the device handling the push request towards the mobile device. The client establishes a virtual link with the mobile device, like if it was connected through a long cable. *This is the implementation of the trial version.*

Direct Physical Access

A direct physical access with the SIM can be especially desired when the mobile device is an integrated part of a computing device, such as a PDA or a laptop with an integrated phone. The security token within the SIM could then be accessed and used without even having mobile network coverage available. *This is not implemented in the trial version.*

Client Side

Establishing the virtual connection

SmartTrust Personal delivers end-user security in the client environment. Handling the SIM as a security token is just one function, it also handles “soft” file based keys as well as traditional smart cards and readers. To be able to use the SIM Card as a security token in SmartTrust Personal, the user first has to add it in the Administration Utility as shown in Figure 4.

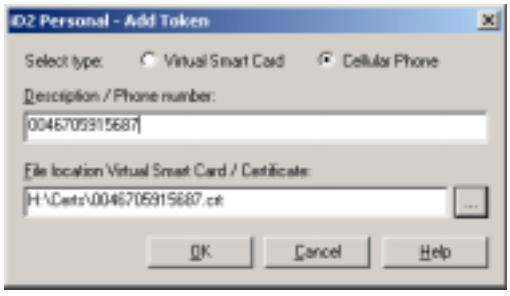


Figure 4 Adding a SIM Card token

To confirm that the user owns the SIM Card, the Enterprise PC Security server component sends an acceptance request to the mobile device in question. The user's certificate is downloaded from the server component upon if the user accepts to create a virtual connection.

A convenient configuration setting makes it possible to re-established the virtual connection after a workstation restart without further user intervention.

User Dialog

Digital signatures carried out through mobile devices have "traditionally" (if tradition is really the correct word) referred to signing clear text readable to the user. When it comes to digital mechanisms using, the Enterprise PC Security concept, it is a matter of handling binary data, be it the RSA transformation of data for an SSL negotiation during handshake or unwrapping a symmetric key in an encrypted S/MIME mail content.

Hence, a "traditional" mobile signature is typically visible to the end user as something readable but the typical content in the Enterprise PC Security concept is just a hash of a binary blob. A binary blob is however not very readable to the human eye and it is therefore necessary to convert the binary data into something representing it, a hexadecimal text representation of the hash. The user is therefore presented with a dialog box when it is time for a security mechanism to be executed. This may sound complicated but is not as seen below in Figure 5. The hexadecimal presentation is performed in order to guide the user and to maintain the security.

In a sign dialog, when for example signing a large document, the hash of the data about to be signed is shown on the computing device, so that the user may compare this to the fingerprint shown on his cellular phone. The user can thereby be ensured that the data has not been tampered with during the transmission.

Figure 5 shows how a signature request will look like on the client PC and what the handset will display.

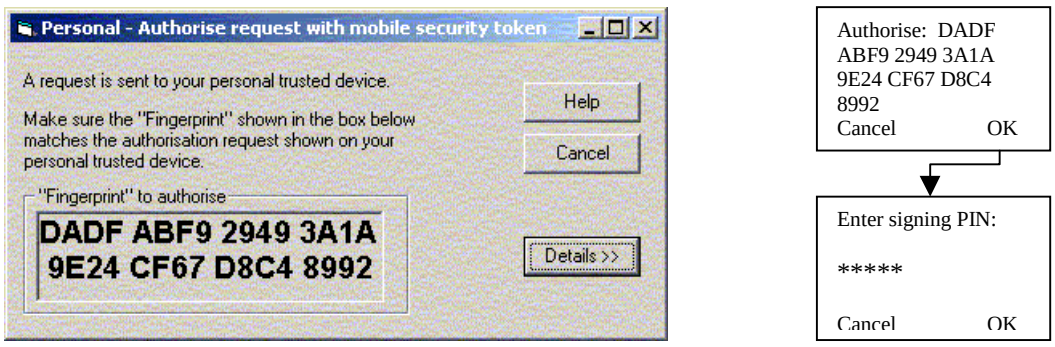


Figure 5 Fingerprint of hash shown by the client and handset

More low-level technical descriptions of how Personal handle support for Microsoft Crypto API and PKCS#11 can be found within the technical documentation for SmartTrust Personal.

Server Component

The Server component acts as a front end to the WIG inside the Delivery Platform, and offers together with SmartTrust Personal the service of making digital signatures using an RSA enabled WIB in a SIM Card.

To make signatures, the user first has to login to the server component, which is described above. The Server stores the session ID and its associated mobile device number. The user need not to remember the session ID as SmartTrust Personal handles this automatically after logging in. By doing this only a specific computer showing a link with the mobile device is allowed to request cryptographic operation, i.e. digital signatures and decryption, from the specified SIM Card. This procedure prevents malicious users from sending signature requests to other person's, hoping they will sign something they do not want to sign, by mistake.

The server component can be configured on an enterprise wide level to keep sessions indefinable or to request a new login if the service has not been used by a specific workstation for a lengthy period.

The Enterprise PC Security server component has the possibility to audit the login, and to make this information available, e.g. for billing purposes.

Server vs. Client initiated service request

The wireless security solution from SmartTrust has supported server application initiated service requests for several years. The Enterprise PC Security concept takes this one step further by making it possible to initiate a security service request from a client workstation.

The major difference, apart from the convenience of being served with a flexible security token, is the possibility of being able to perform a security operation as if it was an actual part of the client workstation. This makes it possible to handle strong authentication of the client workstation, an essential issue in several applications, like for instance secure web and VPN.

Additional Services and Products

Trusted Operator Services

The Trusted Operator Services (TOS) module is a set of products and components logically packaged under a common name providing the core services necessary for a wide range of applications delivering secure e-commerce solutions. TOS is an add-on to the Delivery Platform and brings the ability of providing added value for applications residing on the content provider or enterprise side.

The Enterprise PC Security concept, described in this document, is a part of the Trusted Operator Services (TOS) module.

The Trusted Operator Services module can be complemented with additional SmartTrust products:

- SmartTrust Security Center – installed at the content provider/enterprise

  For providing end-to-end confidentiality, and signature/certificate verification functionality for content providers when accessing mobile devices remotely

- SmartTrust Personal – installed on client PC workstation

  A product necessary for creating local client accesses with the security token within the SIM in the Enterprise PC Security concept (this document).

- SmartTrust Certificate Manager – installed at CA, TTP or Mobile Operator

  For complete certificate management including issuing-, carried out remotely over-the-air through the Certificate Portal or in batch, and revocation of certificates.

For further information on Trusted Operator Services or the Delivery Platform please contact SmartTrust, or visit our web site for more information at: http://www.smarttrust.com/

Certificate Management

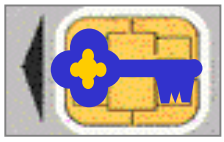
A digital certificate could be described as a digital signature proving your public key actually belongs to you. Hence, a digital certificate is an electronic

piece of information, like a document, telling about the bind between a public key and the entity (an individual or a machine) being the owner of the key in question. The party issuing the certificate, i.e. signing the information and vouching for the ownership of the public key, needs to be someone trustworthy, and is usually called a Certification Authority (CA). The Certification Authority role can be taken by the mobile operator should this be a strategic business decision, but can equally be hosted by an existing TTP or enterprise should this be preferred.

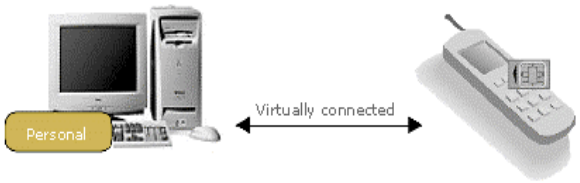
Managing certificates is necessary for providing the Enterprise PC Security concept and supplying a PKI for an enterprise is within reach for today's mobile operators. SmartTrust has developed a product named SmartTrust Certificate Manager dedicated for this purpose. For further information on Certificate Manager please contact SmartTrust, or visit our web site for more information at: http://www.smarttrust.com/

Summary

From a security perspective the traditional handset could become a “personal trusted device” (PTD) as its internal structure already carries a smart card capable of storing private credentials and encryption keys.



With the Enterprise PC Security concept using SmartTrust Personal on the client side, the mobile handset is not just a phone, but also the world’s most commonplace smart card reader. The SmartTrust security solution allows any compliant PC application to utilize the SIM’s security mechanisms. This makes it possible to use a handset as a secure device, e.g. for the signing of e-mails and strong client authentication during remote access among other security related tasks.



Having mass-market tamperproof security tokens out in a business environment can now be accomplished by using the mobile handset, as the security token. Likewise “smarter” devices such as PDAs with wireless support can equally make use of security features, such as digital signatures, becoming available through the SIM

The Wireless Enterprise PC Security concept allows Mobile Operators to offer a complete mobile security service for enterprises. The service offering from the mobile operator side could typically be based on bulk of messages- or per transaction oriented charging.

From an enterprise perspective the Wireless Enterprise PC Security concept incorporate the following benefits:

- One supplier of mobile services should provide better control of the total wireless cost
- One supplier of mobile services should provide for better transaction performance
- Usage of mobile phones for internal calls as if they were fixed phones
- Better security, less expensive, high-end, security solution – PKI with tamperproof security tokens without having separate smart card readers
- Future proof investment as the security concept is based on existing standards

Glossary

API	Application Programming Interface
ARPU	Average Revenue Per User
CA	Certification Authority
CSP	SmartTrust Delivery Platform
DP	Enhanced Datarates for Global Evolution
GPRS	General Packet Radio Services
GSM	Global System for Mobile communications
HTTP(S)	Hypertext Transfer Protocol (over Secure Socket Layer)
ICC	Integrated Circuit Chip
IP	Internet Protocol
LAN	Local Area Network
ME	Mobile Equipment
OTA	Over-the-Air
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKCS	Public-Key Cryptography Standards
PTD	Personal Trusted Device
RSA	Asymmetric process, named after its inventors Rivest, Shamir and Adleman
SAT	SIM Application Toolkit
SIM	Subscriber Identity Module
SMS-C	Short Message Service Center
SSL	Secure Socket Layer
TLS	Transaction Layer Security
TOS	Trusted Operator Services
TTP	Trusted Third Party
VPN	Virtual Private Network
WIB	Wireless Internet Browser
WIG	SmartTrust Wireless Internet Gateway

Document number: MPM02:0015
Revision: A