



Mobile PKI Security

Potential, Challenges and Prospects

The mobile phone is everywhere and available to almost everyone. So is mobile PKI (Public Key Infrastructure) security: every mobile phone and every other device that works with a SIM card supports mobile PKI.

THIS PAPER HIGHLIGHTS THE POTENTIAL of the mobile phone for authentication and digital signatures, discusses the challenges and explains methods for the establishment and use of a mobile PKI.

A mobile PKI solution enables secure mobile commerce applications, whereby transactions can take place directly via a mobile phone – anytime, anyplace and with any service. Another scenario sees the mobile phone as a secure device for authentication and digital signing for transactions conducted via a PC.

Mobile PKI is universally available

A few isolated mobile PKI solutions are already available on the market ^{1,2}. These are designed to work exclusively with Blackberry devices or with a specific mobile OS, in which case an SD card is required. These solutions are only adaptable in a business environment with a system administrator who oversees the entire rollout process for the necessary software, keys and certificates.

The mobile PKI discussed in this paper is far more generally applicable and concerns all mobile phones for private and business use, regardless of brand or manufacturer, and is adaptable to all kinds of applications. The challenge is the development of a trust framework for the secure distribution of private keys and the storage of certificates suited to various handsets, operators, and distribution networks.

Mobile society

Today, more people own and use a mobile phone than a personal computer. Mobile penetration in Europe is way above 100%. Smart phones have become more common and sales are on the increase. A report ³

sees smart phones outnumbering PCs by 2011. Every mobile phone is much more than just a telephone and their use for electronic commerce is predestined.

Demand is potential

A mobile phone is a device with many functions and a display large enough for user interaction. Smart phones are small computers, which can run several applications and have Internet access. Mobile devices seem to have become indispensable for most people, and not only in the business world where mission-critical applications have to be accessible in real-time, always and everywhere.

People have also become mobile themselves, but still want to stay connected. They want their digital environment to be the same on the move as it is at home or at work. Applications that customers are used to have to be accessible independent of time and place. The good news is that the mobile phone can be used not only to gather information, but also for secure transactions.

A few examples of services on the move are: remote access to email, calendar info, shared files and other business applications, eBanking, stock trading, eTicketing, eCommerce, logistics, gambling and entertainment. The more sensitive the information that can be accessed, the more the demand arises for security; security that ensures the confidentiality of communication, the genuineness of information and the authentication to use services.

Utilizing the mobile phone

The mobile phone can be used for both authentication and digital signing. In order to use these functions,





the end user needs a verified digital identity. The private key for verification can be stored on the mobile phone's SIM card.

Every mobile and smart phone works with a SIM card. SIM cards are smart cards and as such can be used for identification, authentication and data storage. They contain tamper-resistant properties and can transfer data not only to central administration systems, but virtually anywhere via the SMS interface. So every mobile phone meets all PKI requirements right from the start. A mobile phone just needs to become part of the mobile PKI. This means that a private key must be sent to and stored on the mobile phone while a digital certificate is stored on the operator's directory server. The digital certificate holds the end user's public key. The private and public keys stay linked and can be used for authentication and digital signing.

The question is, how can the end user obtain the private key to be stored on his or her mobile phone? The challenge lies in the enrolment process for trusted key distribution.

Enrolment process

The enrolment process, as you will see in our example, involves the operator, a trust centre or the operator's own CA, the point of sale (PoS) and, of course, the end user in need of a digital identity. The trust centre can be operated by the network operator, but this is not

the only possibility. In some cases it may be favorable to use an operator-independent mobile PKI solution. Another company – a content provider, for instance – could offer this service and build up a mobile PKI with an external trust centre, or even the trust centers themselves could offer such a service.

Registration Service Registration Service login authenticated by certificate

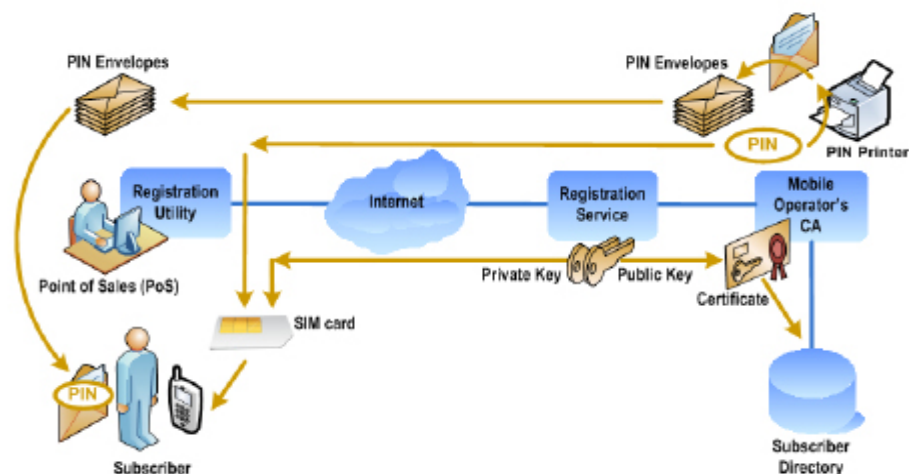
The enrolment process is initiated by the mobile network operator. The operator service for mobile certificate enrolment is available at the operator's PoS. Authorization to use the operator's enrolment service is based on the PoS's possession of a valid certificate issued by the operator's trust centre service (CA). These authentication certificates will be issued in advance in the form of software tokens to all PoS units that offer the registration service to their customers.

PIN management

The operator's CA will generate random PINs in advance and print them. An envelope protects the PIN from unauthorized reading. A batch of envelopes will be pre-printed and distributed to the PoS together with a software token as part of the setup procedure. The PIN envelopes will be held in stock at the PoS and have limited validity for security reasons. All have a unique label on the outside. The PIN is associated with the label on the PIN envelope and the CA registers these.

Enrolment Scenario

The picture on the right shows an example scenario for the trustworthy enrolment of PKI credentials for a mobile phone subscriber.





Subscriber application for certificate

End users who intend to use their mobile phones as a device for authentication and digital signing need to visit a certified PoS partner for the enrolment procedure. Face-to-face authentication with a passport or similar authentication method will be the first step of the registration process to check whether the person is the person he/she claims to be.

The staff at the PoS will have to log on with the software token they were given by the operator's CA. Security is guaranteed by strong, challenge-response authentication. A web-based registration utility (RU) provides the graphical user interface (GUI) for registration. The PoS employee randomly selects a PIN envelope from stock and enters the identity data of the applicant and the label of the envelope in the RU. Next, the RU generates an asymmetric key pair and requests a certificate from the CA. The envelope label details are included in the request to the CA. The CA generates the certificate with all identity data included.

Proof of possession of the private key

Along with the certificate, the CA will return the PIN associated with the label on the PIN envelope to the PoS. Note, however, that this PIN will never be visible to the PoS employee. The PoS employee will connect the SIM card to the RU via an appropriate card terminal. The RU will then write the generated private key to the SIM card and set the PIN. The PIN protects the private key from unauthorized use.

The SIM card and the selected PIN envelope will be handed over to the end user to complete the enrolment process. The user now possesses the private key, which is protected by the PIN inside the PIN envelope. It can

be assumed that the subscriber in possession of the envelope is the only person who knows the PIN that controls the private key.

Finally, the RU will confirm enrolment to the CA, which publishes the certificate in an LDAP repository. Being in possession of a digital identity, the user can now use the mobile phone in a secure way for services and transactions that require authentication or a digital signature.

Mobile PKI for direct use via mobile phone

Secure transactions can be performed directly via the mobile phone itself as follows: using an application on the mobile phone, the subscriber connects to the requested service over the mobile network. The server will connect to a validation server to authenticate the user. A challenge-response protocol will be run between the validation server and the mobile phone: the server will send a random challenge number in a special SMS to the phone, which will activate the SIM card's signature function. The subscriber will be asked to enter the PIN and the phone then signs the challenge number using the private key. The signature and the subscriber's certificate will be returned to the validation server for verification. The verification includes checking the revocation status (valid or revoked) with the operator CA over Online Certificate Status Protocol (OCSP). If validation succeeds, the validation server will send confirmation to the service, which in turn will grant access to the subscriber.

Commitment signatures can be handled in a similar way, where the challenge is replaced by the data to be signed. The validation server may be operated by the mobile network operator or the service provider.

Mobile PKI enables secure smart phone applications

The figure on the right shows the validation scenario for mobile PKI-based authentication triggered by a smart phone application.

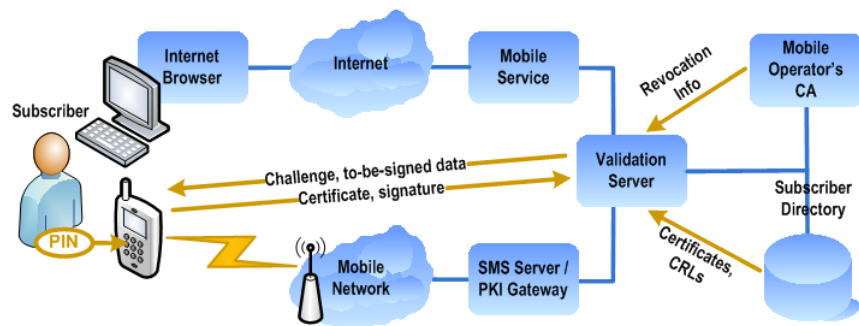




WHITE PAPER

Mobile phone as secure signature creation device

The figure on the right shows the verification scenario for digital signatures that can be used for various applications on any PC.



Mobile PKI security for transactions on a PC

A mobile phone can also be used as a secure signature creation device for authentication and digital signing for transactions performed on a PC.

The user connects from the PC to a service provider's application. The application will display a message on the PC requesting the user to perform authentication using his or her mobile device. Challenge-response authentication is then performed between the validation server and the phone. After successful validation, the user's identity is passed to the application and the user can enter the service.

Commitment signatures can also be created in a similar way: the user submits the to-be-signed data over the PC to the application, which creates an abbreviated version of the data (a digest) and passes it to the validation server. The validation server interacts with the mobile phone to create the signature. It sends a special SMS to the phone, and the phone displays the digest and requests the PIN needed to sign the digest.

Finally, the signature is returned to and verified by the validation server. The validation server sends the signature back to the application for archiving.

Mobility and independence

The mobile PKI gives users more mobility and independence, while service providers benefit from secure user identification and instant transaction commitments. Secure transactions can now be made on any PC at Internet cafés or business centers, or even without a PC. Considering the growing market for mobile and smart phones, and the rapidly increasing number of useful mobile and Internet applications, we expect Mobile PKI to become a relevant and economically justifiable service.

References

- 1) www.corisecio.com
- 2) www.peak-solution.de/
- 3) www.gartner.com/technology/about.jsp - newsroom

NEXUS products ready for mobile PKI security

Nexus Certificate Manager

Nexus Certificate Manager is a well proven high security platform for issuing digital identities (certificates). It can be used to issue soft tokens to the PoS as well as subscriber certificates for mobile phone SIM cards.

Nexus Certificate Manager comes with a Secure Printer suited to the production of PIN envelopes.

Nexus Personal Security Client

Nexus Personal is PKI middleware that provides computer applications with access to the security functions of smart cards, SIM cards and software tokens. It also contains the online Registration Utility used for the enrolment service at the PoS.

PortWise Validation Server

PortWise Validation Server is called whenever a certificate or a digital signature needs to be validated. It performs the complex validation procedure for the entire certification path and includes revocation status checking of the certificates.

Nexus OCSP Responder

Nexus delivers certificate revocation status information to relying parties according to the standard Online Certificate Status Protocol. It determines a certificate's status using the revocation lists (CRLs) or OCSP services of the mobile operator's CA.

Nexus

www.nexusafe.com
contact@nexusafe.com



Identifying and Authenticating
the Connected World