

## Use the mobile phone as a secure channel with Wireless PKI

By Sverker Arvidson (sverker.arvidson@bankid.com)

### Lessons from the WAP-era

In 1999, there was a WAP-hype in Europe and the US. The trend was strongest in the Nordic countries. Sweden and Finland was at that time the centre of mobile development through Ericsson and Nokia. WAP was to offer Internet even on mobiles. The prospects were huge. Plans to develop mobile applications were made.

If a start-up had WAP and Internet in there business plans, the value would raise. Even in the banking sector many also were carried away and decided to develop applications for mobile banking. Several banks launched WAP-services.

The applications for mobile banking were never a success. In spite of extensive marketing only some thousand customers connected and regularly used the mobile services. There are several concurring explanations:

- The mobile phones (the terminals) were immature and unstable. The display was small which meant that the presentations were indistinct and not very pedagogical,
- It was hard to set the parameters for the mobiles. The settings of parameters were a manual process where a number of values should be fed in the mobile unit to enable it to work as a WAP-terminal. The instructions were written by technicians and thus nearly impossible to understand for the common user. Already here, many customers gave up. Today, the parameters are transferred via SMS and the setting is no longer a problem.
- GPRS (technique for mobile data communication with higher speed) was not yet introduced. You were forced to use the normal GSM-communication. The changing of pictures were very slow. And the meter ticked also when the customer only looked at the contents, i.e. the transactions. This was rather expensive for a private person.
- The WAP-standard (1999) did not include security. This meant that the application for mobile banking was limited. The banks could not decide with enough security who the customer was. It was of course possible to use PIN/TAN sheets or smart card calculators. This was not an acceptable solution - you cannot execute the transactions with the mobile in one hand and a security device in the other. One solution was to introduce a fixed pin-code with an unsatisfactory security level. With these necessary limitations, the customer could only transfer money between their own accounts. You could get updated rate of exchange but transactions were too risky.

Summing the above, you could understand why the introduction of applications for mobile banking in 1999 not was a success. The result was that in some communities, the word WAP was seen as equal with abusive language.

### Secure re-start

The idea of using your mobile on the Internet was never the less still attractive. In year 2000, people from Nokia, TeliaSonera and Handelsbanken took the first steps trough several discussions on possible ways of future development in this area.

The starting-point for the discussions was to add more advanced security solutions to the mobile application Handelsbanken already used. During this period the standardisation of

WAP had gone forward and resulted in a specification of how a PKI-based security solution should be designed (WAP PKI or WPKI). Since the Internet bank Handelsbanken had established already used PKI as method of security, a WPKI-based mobile services should be possible to be integrated without further extensive amount of work. The limitations of the services possible to offer in the existing mobile solution could be eliminated.

Mobile services based on WAP had, however, got a very bad reputation on the market and the parties considered it impossible to plan for further development of the applications that Handelsbanken offered.

That led to that we shifted focus from realising a service in the short timeframe to build a solid base for future mobile security services. The first step was to give the mobile phone the right characteristic, making it possible to use the phone as a trusted device connected to the Internet. The technology to be used was WPKI. The critical point in a PKI-solution is how to protect the private key. We considered a solution where the private key should permanently be saved on the SIM-card. This solution would be equal to the so called hard key solution on smart cards. When this technique is built-in in your mobile, you could identify yourself on the Internet as well as sign transactions. Comparing the security solutions based on calculators, the mobile phone has a number of advantages:

- Almost all adults in Sweden have a mobile phone, it can be considered a personal equipment.
- You carry the mobile phone almost at all times, you wish to be reached on the phone. If the mobile should have a security solution, this is always available when you need it. A calculator is probably at home if you need to execute a transaction unexpectedly.
- You get full PKI-functionality with your mobile phone, both for identification and signing.

Following scenario was discussed between the three parties:

*"You are a customer in an Internet bank using WPKI as security solution. When you log-on to the Internet from your PC, you get an offer to log-on from your mobile phone. You click on that alternative and some seconds later you get a signal in your phone. At the display you get a message to give your password (the WPKI-password you have already chosen). Doing this, the cryptographic process is started and the private key is used. The central internet bank application can now decide that you are the one you say you are and you get the possibility to use the services you have on your PC. You can transfer money from one account to another using your PC and then click "Sign". The procedure is repeated, you get a signal from your mobile phone and in the display you can see the transferring you registered on your PC. You give your password again and by doing this you sign your transaction".*

This scenario was considered to be so interesting that a proof of concept was carried through. TeliaSonera produced a SIM-card including a private key. A simulation of an Internet bank was built. Using a standard version of a PC and a mobile with a special PKI based SIM-card successful tests were carried out. The simulated Internet bank handled two separate channels synchronously, one secure channel to the mobile phone and a channel for information over the Internet to the PC.

An important conclusion in WPKI-connection is that the channel to the mobile phone always should be a secure channel. The channel for information could be connected to a PC, but also to a digital TV or the mobile itself. This means that if you need a large picture (a form for tax declaration for instance) you can use a combination of PC and the mobile phone. If you only transfer money between two bank accounts, both security and the transaction could be

performed from the same mobile phone. The lack of security described in the beginning of this article is now solved when WPKI is used.

### **Security is a question for the society**

Another important solution drawn during the discussion is that WPKI is a decision on infrastructure. A bank cannot accept that the services offered are restricted only to customers with a subscription at one specific operator or a user of a special mobile phone can access the new services. In conjunction a operator or mobile device supplier cannot develop this infrastructure for one single bank.

Since the banks already have developed a common security solution that resulted in the concept BankID (e-signature), a company jointly owned by the Swedish banks. It was natural to plan for further development in the already existing company. To the concept "BankID", an additional method of security should be added. One key success factor was to get several operators and the leading actors in the telecom industry engaged in building the new infrastructure. The degree of interest from these parties was so extensive that we could decide on a joint venture.

The joint venture started in February 2004, aiming to produce specifications on how to build a WPKI-infrastructure. The interface between the system of the mobile operator and a certificate authority should be specified as well as the specification for construction of new SIM-cards. A demonstrator should also be developed to use all functions decided upon. In this project TeliaSonera Sweden, Vodafone Sweden, Tele2, Ericsson, the banks behind BankID and their company was represented, together with specialists from Teleca. The project closed in December 2004 and it resulted in specifications covering all functions and a working demonstrator.

### **Use our work**

The parties found it important to make the specifications public. They could hopefully be the foundation for standardisation and the publishing could refrain someone from taking out a patent on the result of parts of it. The specifications were published in March 2005 together with other material at [www.wпки.net](http://www.wпки.net). An organisation was founded "WPKI-association" and it should manage and develop the specification. Another aim for the organisation is to inform about the concept and work for future standardisation. We welcome new members from government and enterprise in addition to the members from the founding organisations. This is a unique project, not only the specifications and the demonstrator, but also because of the cooperation between banks and operators. This was not possible some six or seven years ago.

Those who wish to develop WPKI within their own concepts are welcome to do so, but preferably using our specifications. Within BankID there are ongoing projects studying how to implement WPKI in this concept. An important factor is that moderate economical terms and conditions are agreed upon between the banks and the operators.