

# Secure and Mobile Digital Signatures for Internet Banking

**Taking an entirely new approach to digital signatures, Cryptomathic has developed a solution, which is highly secure, user-friendly, and fully mobile. The solution supports qualified certificates if required and provides optimal protection of the user's signature key as required by European legislation. This addresses issues of major importance for future Net banking.**

The political and technological development poses two major challenges for tomorrow's Net banking applications:

- The use of digital signatures and management of certificates is an issue now covered by law in most European countries. By July 2001 all member states should comply with the European Commission directive on digital signatures from 1999.
- In a banking system based on digital signatures, security is highly dependent on proper storage and use of the signature key. The increasing popularity of always-on Internet connections again questions the security of traditional solutions, which store the key on the user's hard disk.

## **Certificates**

The first issue – digital signatures – is first and foremost a political one. Many Net banking solutions already use digital signatures, and the European legislation does not cover Net banking as such. However, the standards set by the EC directive are expected to affect requirements for future applications of digital signatures in general.

In particular, one must assume that future Net banking solutions are based on – or at least capable of handling – qualified certificates issued in accordance with national laws complying with the EC directive.

## **Protection of Signature Keys**

The second issue – key protection – touches a vulnerable point of traditional digital signature solutions: From a security perspective one must prefer to keep the signature key in hardware, e.g. on a smart card. But usability considerations have promoted software-based solutions, and today these are by far the most widespread. (In a software-based solution the key is stored on the user's hard disk and read into memory whenever a signature needs to be generated. This, in fact, would not suffice for qualified certificates.)

Thus, the traditional solution is a compromise between security and usability, and in reality it ties the user's access to the Net banking application to one specific PC. Mobility, though, ought to be one of the major advantages of Net banking over traditional home banking.

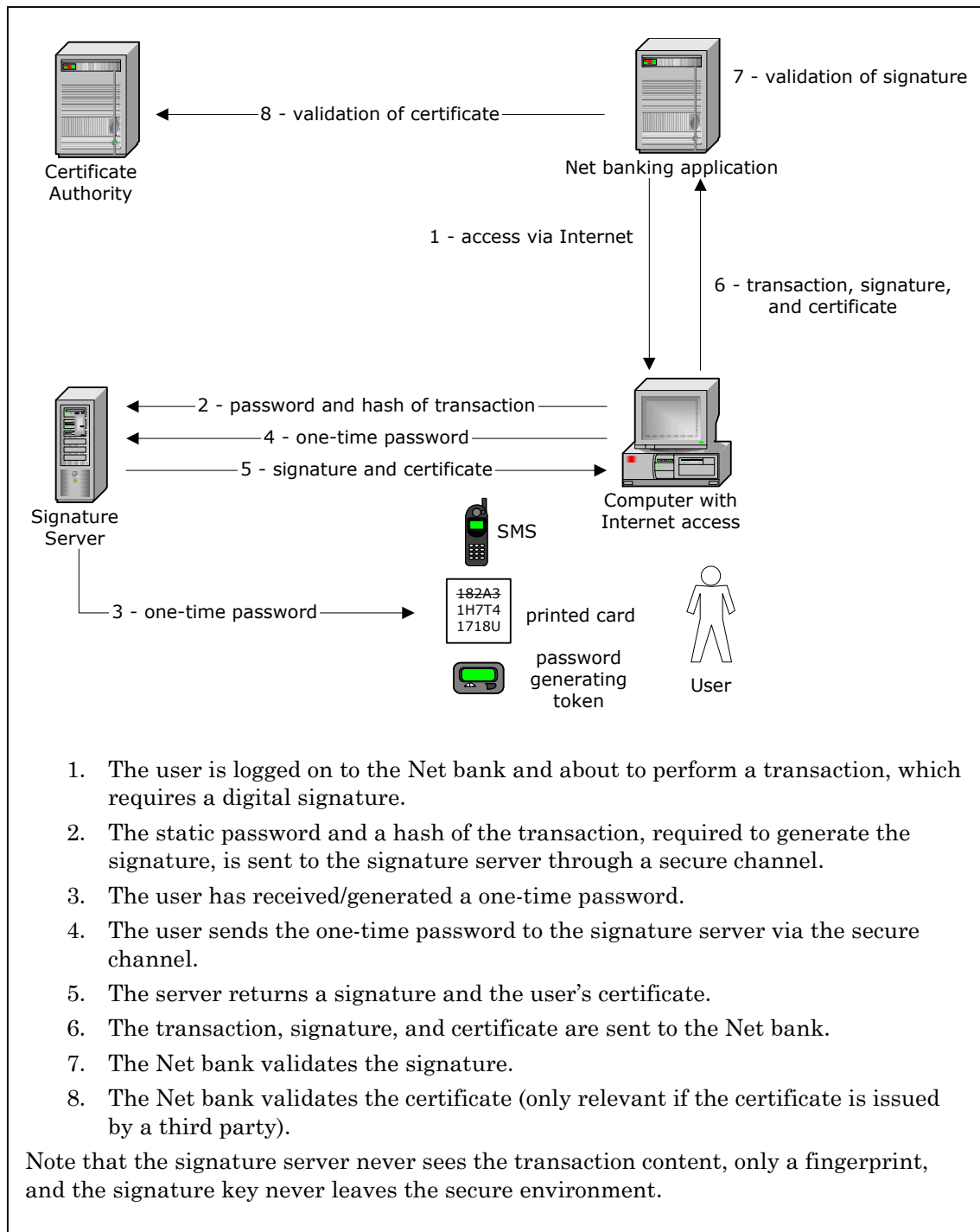
Cryptomathic has found a novel solution, which compromises neither security nor usability, quite the contrary in fact. Since the weakness is storage and handling of the signature key, the straightforward solution is to free the user from this responsibility. Instead, the keys are generated and stored centrally on a secure server, and the signature key never leaves this protected environment. Yet it is controlled entirely by the user through secure channels at all times. This has some evident advantages:

- **Optimum physical security:** The key is far better protected on a secure server than on the user's hard disk or on a smart card.
- **Protection against theft:** It is practically infeasible to steal a key from a secure server – even for the system administrator.
- **Mobility:** The owner can use the key from any terminal with Internet access.
- **Logging:** Access and use of the key is logged which makes it easy to detect misuse.
- **Centralised key management:** The periodic key renewal needs not involve the end user, and the key can easily be suspended if required.



## Two factor authentication

The security challenge has now been reduced to protection of key usage, and again this new approach has superior possibilities. On the user's hard disk the key is only protected by a (static) password. On a signature server the security level is easily increased with a well-known technique: authentication through two independent channels – typically something you *know* and something you *possess*. In Net banking the natural solution is a (static) password combined with a one-time password, which can be delivered as an SMS to the user's mobile phone, printed on a card, generated by a token, etc. I.e. in order to access the key, the user has to prove that he (1) knows his password and (2) is in possession of his phone/card/token.



**Signing a Net banking transaction with a signature server**



## Flexibility and Migration

Detaching the security mechanisms from the banking application makes the solution very flexible and opens several migration paths. The scope of the banking application can easily be widened to include, e.g. on-line loan applications and securities trading. Likewise, once a banking application is able to handle digital signatures, the security level can easily be adjusted as access to signature generation is under centralised control. In particular, the signature server makes migration from PIN-based security to digital signatures extremely easy and absolutely transparent to the end-user, who will still enjoy mobility and ease-of use, only with enhanced security.



## Cryptomathic Signer

Cryptomathic Signer was developed for a Danish Net banking solution, which operates as described above. The security has been reviewed and approved by certified public accountants, and the solution becomes operational this year.

A patent application has been filed.

Learn more about Cryptomathic Signer at our Web site [www.cryptomathic.com](http://www.cryptomathic.com).

