



CRYPTOMATHIC
www.cryptomathic.com

Signer Case Study - Savings Bank Data Centre



Health Services

Internet banking

Loan applications

Land registry

Legal documents



HOME BANKING LEAVES HOME

More than one million customers in Danish savings banks now have the possibility to do secure banking from Web browsers anywhere in the world. The new Internet banking solution from the Savings Banks Data Center (SDC) is based on Cryptomathic's mobile digital signatures.

HOME BANKING LEAVES HOME

Savings Banks Data Centre

The Savings Banks Data Centre (SDC) provides IT and related services to Danish banks. The IT services range from development to hosting. SDC was established in 1963 as a data processing centre for the Danish savings banks; today it services 80 banks with 506 branch offices and 1.1 million customers.

Imagine a Café Bank

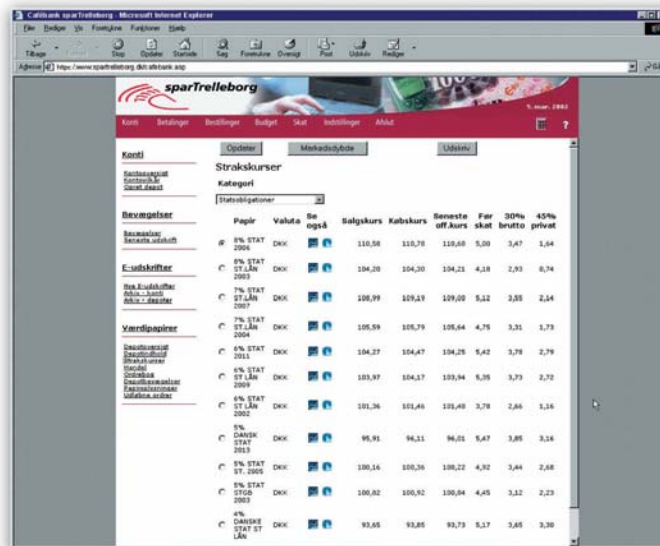
Imagine that you are at work, attending a course in Paris, abroad on holiday, or stuck in an airport due to heavy snowfall. And imagine that you forgot to pay a bill, just received a hot tip for the stock market, need to check the status of a banking transaction, or just want to kill time in a productive way. So, what do you do? Your home PC is out of reach; but that is not a problem. You just go to the nearest computer with Internet access and start home banking. With SDC's Café Bank based on Cryptomathic's mobile digital signatures, it is as easy as that.

Easy for the User

To use Café Bank the travelling home bank user only needs a mobile phone and a computer with Internet access. The user accesses the bank's Web site as usual. To log on she enters her password as usual, and a few seconds later she receives an SMS with a Café id-code. She enters the id-code and is now able to use the banking application as usual.

Still Secure

For paying bills, moving money between accounts, etc. in Home Bank — SDC's traditional home banking solution — a digital signature is required. To apply a digital signature to a transaction, the user needs a signature key. This key is stored on her home PC, but a copy is kept on a central server. When travelling, she uses the Café id-code to identify herself and access the key stored centrally.



Jacob Hertz, SDC chief security architect, says:

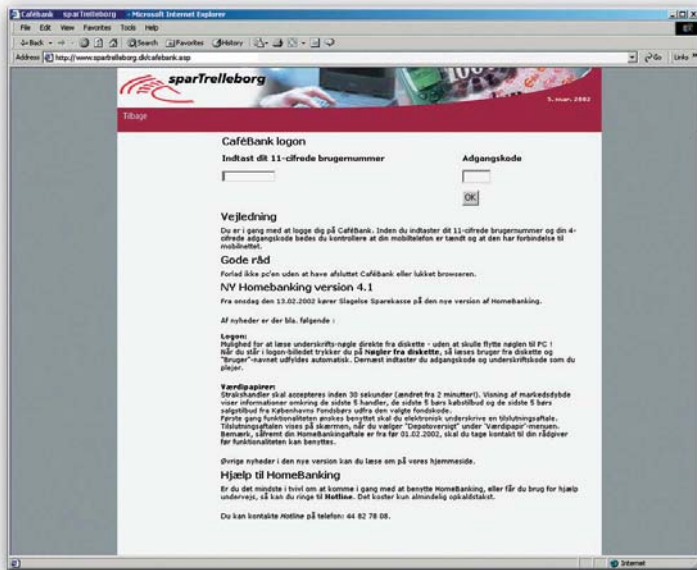
"Our original home banking solution (Home Bank) is extremely popular, and we wanted to make it even more user-friendly and truly mobile. It has always been technically possible to do mobile home banking, but only by relaxing security. This was never an option to our customers, nor to us. SDC's home banking concept is one of the most secure solutions in the market, and we did not compromise our high security to obtain mobility, far from it!

Café Bank started as a supplement to the traditional Home Bank; but we expect that more and more customers will use Café Bank only. The reason for this is the increasingly popular always-on Internet connections like ADSL. An online PC is exposed to attacks from outside, and so is a key stored on the PC. The security state of the PC at home may be doubtful, but our central server is absolutely secure."



Jacob Hertz,
SDC

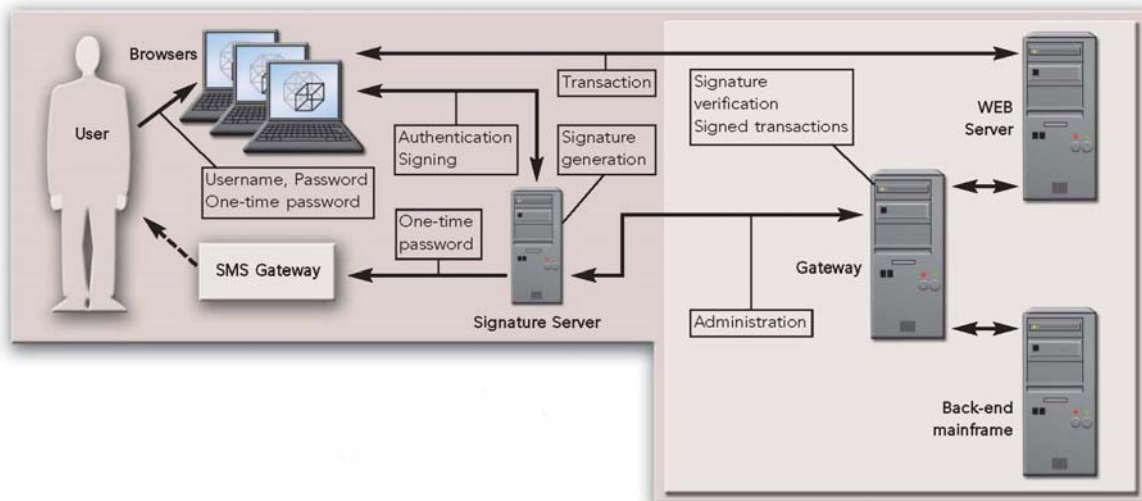
With SDC's Café Bank we are now able to offer our customers a home banking solution which is not only secure and user-friendly but also fully mobile."



Solution Overview

The signature server delivered by Cryptomathic makes the unique combination of mobility and security in Café Bank possible. The banking part of the solution is similar to any other Internet bank. The security part, however, is different because the central security operation – generation of digital signatures – has been moved from the client to a central server.

To access Café Bank and perform transactions, the users have to authenticate themselves towards the signature server. Thus, this server delivers both strong access control to the application and digital signatures on the transactions. In Café Bank, the signature server provides strong two-factor authentication using a static password and a one-time password: the Café id-code sent to the user's mobile phone via SMS.



The keys stored on the signature server are protected by a Hardware Security Module, where the signatures are created. Firewalls (not shown) are set up to form a demilitarised zone around the Web server.

Solving the Key Store Problem

In any solution involving digital signatures, it is essential to choose the right store for the user's signature key.

Software key stores remain the most common choice. While they are quite easy to deploy, they offer only limited security and no mobility at all. Hardware key stores, like chip cards, offer higher security and even promise some degree of mobility. However, smart card readers are not yet included in standard PCs.

Cryptomathic's signature server combines the best of the two worlds. With no software to install on the client side, deployment is not an issue. For the signature key, the server offers optimum protection and physical security, while the user enjoys full mobility.

Mobility Expected to Boom

Still more customers are expected to switch to mobile home banking for reasons of convenience as well as security. Furthermore, SDC can now provide these users with mobile, general-purpose digital signatures, which can be used for anything from secure authentication to signing e-mails and Web forms.

CRYPTOMATHIC PRODUCTS IN THE AUTHENTICATION AND SIGNING SUITE

CRYPTOMATHIC SIGNER

Cryptomathic Signer is an innovation in digitally signing and certifying electronic documents, from emails through to pdf and any other document type. The basis of the solution differs from other PKI implementations in that the user does not have to carry their private key around with them or store it on their computer. Instead, they simply have to authenticate themselves to the service and sign the relevant electronic document within the server itself. This means that they are not only signing exactly what they see but they also maintain the security of the private signing key.



CRYPTOMATHIC AUTHENTICATOR

The Authenticator is an independent authentication server. Firstly, it is independent of token suppliers so customers are not tied to any particular authentication vendors or technologies when choosing the Authenticator. Secondly, the same level of independence applies to HSMs, allowing the Authenticator to support the customer's preferred HSM brands and models.

Through a wide and growing range of user and transaction authentication methods, the Authenticator is able to adapt to future requirements and safeguard the value of the initial investment. It is also possible to provide your customer base with tokens that meet their individual needs without the need for additional infrastructure costs. For example: high risk customers could be provided with tokens based on more complex authentication techniques or even multiple authentication techniques, while low risk customers could be issued with tokens using less complex authentication therefore maximising protection while also minimising costs. Cryptomathic Authenticator allows the business to tailor the authentication needs across the business and to migrate between authentication mechanisms as the prevalent fraud migrates.

CRYPTOMATHIC TOKEN MANGER

Cryptomathic Token Manger is designed to provide full lifecycle management of physical tokens to those organizations who require a strong authentication solution but have no existing management infrastructure. The product is designed to manage the end-2-end lifecycle of the token from the point at which it is initially requested, through its manufacture and distribution and on to its expiry and replacement. As part of this overall management process the issuer can also manage stock in several locations, handle multiple manufacturers and distributors and track various token types within a single implementation.

Tokens can be managed through a simple GUI interface on a customer services workstation or via direct web service integration into existing customer services workflow tools. The flexibility of this interface allows the token status to be managed at the single token level, the distributed packet level, the batch level or the stock location level which simplifies the management process.



ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With over 20 years' experience, Cryptomathic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing

and advanced key management utilizing best-of-breed security software and services. Cryptomathic prides itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com