

## Smartcards and electronic signatures

Smartcard technology was invented in France in the early 1970s and has since gained widespread acceptance in most European countries as an important tool for business and communications. Today Smartcards are widely used for mobile phones, bankcards, health insurance cards and ID cards. New applications are rapidly emerging and with advancements in technology, Smartcards are set to provide a security and multi-functional role in many areas of our business and personal lives.

A Smartcard is a plastic card with an embedded microprocessor or "chip" that enables the card to store information. Most Smartcards used today are read only, the information – account details and personal identification number - PIN is loaded once i.e. bankcards or health insurance cards. The next generation cards use erasable memory chip technology and are capable of storing larger amounts of different types of information such as medical and insurance records and this data can be updated and encrypted on the card. Smartcards can also store cash values from either a bank or a credit card account and this stored monetary value may be used instead of cash for payments. Another type of Smartcards is the SIM (subscriber identification module) card, these are used in mobile phones and store information such as phone numbers list and personal settings that can be stored and erased. As the processing power and memory size has increased, Smartcards containing small Java based computer programmes, have been developed and are set to be the future standard.

Credit card transaction fraud continues to increase and is cited as one of the reasons for reluctance to make payments over the Internet. Generally people feel uneasy to give their credit card details, as there have been many incidents where hackers have accessed unsecured web sites and accessed customer credit card details.

What makes credit cards vulnerable is their weakness in authentication of the cardholder. Most credit cards use a signature on the back of the card to verify the cardholder. This makes it easy for a thief to practice the signature and use the card until it is reported stolen. Over the phone or Internet it is not possible to make a visible comparison of the signature, so unless the card is reported stolen the transaction will proceed.

Smartcards provide an intelligent solution to this recurring problem of user authentication, as the system software in the card facilitates enhanced security control. Unlike the mag-stripe cards available on the market, the Smartcard has the ability to enhance data security by incorporating unique personal characteristics known as biometrics as an identifier. Should cards be lost or stolen, these personal characteristics are nearly impossible to forge and cannot be duplicated.

Cyber SIGN's biometric signature technology uses a different approach to other biometrics such as fingerprint and iris scan. The signature technology is 'dynamic' and the user gives his authority through the act of signing. This technology is ideally suited to eBusiness and secures Workflow applications where the combined security of user authentication and the appearance of a written signature on a document are required.

The Cyber SIGN solution extracts the hidden dynamic biometric data - speed, pressure and stroke order - of the written signature, thereby significantly reducing the chances of forgery. When the Smartcard is used there is no password or PIN – which can be lost, copied or stolen – and the digital certificate can only be released from the card if the cardholder signs and the signature is authenticated. Furthermore if the signature is not identical to the encrypted signature template stored on the card it is rejected and the digital certificate is not released. System

requirements include a pen-enabled device such as a PDA or pen tablet, Smartcard reader-writer, and the Cyber-SIGN Personal software development kit for real-time signature verification and user registration applications.

In the transaction process the cardholder inserts the card into a card reader/writer and gives a sample signature using an electronic “ink” pen. A verification application then runs to determine if the data from the dynamic signature matches the template already stored on the card. This verification process takes milliseconds and the security level (variance between template and signature) can be adjusted to suit specific needs. The initial enrolment is done at the point of issue of the Smartcard, and requires three signatures to create the signature template which is stored on the card. This enrolment process typically takes less than two minutes. Once enrolled, the cardholder retains his electronic signature with his personal information and details on the card. The cardholder’s personal data is therefore always retained by the cardholder and not stored on a remote database, which may be subject to misuse.

Current European-wide legislation provides for secure transactions over a network, but the missing link is the personal authentication of the cardholder, in effect the “I am who I say I am”. By using a Smartcard for the electronic signature or digital certificate, the cardholder can be irrefutably authenticated by having their normal hand written signature verified electronically on the card. On authentication, the legally binding e-signature or digital certificate is released. One of the most important issues in eBusiness and eCommerce is the control of private key usage. Cyber SIGN has integrated the written signature – something we all use daily and is therefore highly intuitive – as a security measure to enhance the existing security of PKI and e-signature enabled Smartcards.

The market for biometric based Smartcard solutions is experiencing rapid growth, applications are numerous and include the existing access, loyalty and bankcards, in addition to which the next generation Smart phones and PDA’s already have the hardware to capture signature data through the touch screen interface and will enable mobile and point of sales payment systems. Smartcards offer additional security for the Applications Provider and a comfort level to the cardholder similar to, but with greater security than, existing PIN based systems. Cyber SIGN’s biometric signature solution enables Application Providers to cut their costs through reduced password and PIN administration.”

#### *Netherlands Pilot Signature Verification Programme*

The Institute of Information on Addicted Care Administration has completed a pilot of a drug release programme using Signature Verification from Cyber SIGN. The system, designed and implemented by Healthcare Systems Benelux, implements a Smartcard system.

For user privacy and legal reasons user data are not store on the centrally managed card administration system – instead, the biometric signature template is stored on the Smartcard and all signature verification and authentication of cardholders takes place ‘off-line’ at the point of issuance.

#### *Indian Smartcard Driving Licence*

The Indian state of Gujarat is the first authority in the world to introduce a Smartcard Driving License programme and the government driven scheme will be for an estimated 10 million driving licenses. Using a fingerprint and signature biometric printed and stored on the card. The

fingerprint is used for verification with the signature being used for 'on the spot' user ID.

The project began with 25 enrolment stations - each with Cyber-SIGN Personal licensed technology and a graphics tablet – before rolling out statewide with the issue of a State Government mandate.