HOW DOES THE NEW MOBILE BIOMETRIC SMARTCARD WORK?

»The true three-factor mobile biometric authentication solution«

1. *Something you are (fingerprint)*
2. *Something you have (biometric smartcard)*
3. *Something you know (one-time password)*

- *Outstanding and futuristic security*
- *simple, swift and cost-effective implementation*
- *Utilizing the existing digital infrastructure*
- *True mobility for the user*
- *No violation of personal integrity*

The fingerprint scanning and the matching are primed in the same secure and closed component on the smartcard without any help from external devices. With its built-in processor, battery, sensor and display it is undisputedly the world's first true mobile biometric smartcard providing outstanding and futuristic security for both the user and the related organisational network at large.

APPLICATIONS

Dynamic password generator

The most prevalent authentication devices in the market today are just tokens that produce a one-time password. Since it provides more security and less administrative work with cumbersome password policies, this technology is used in more and more networks around the world. The Biometric Smartcard can and will add outstanding security to this technology.

The implementation of a dynamic password generator in the Biometric Smartcard will make a biometric log on possible to any computer system anywhere in the world. It will be a true three-factor mobile biometric authentication solution ready for use worldwide.

Upon verification of a fingerprint the Biometric Smartcard itself will generate the next password in an endless stream of dynamic passwords without being dependent of external fingerprint scanning devices. All you have to do is to type in the password that is displayed on the Biometric Smartcard. Each password is only valid for one time and in combination with the biometric verification of the end user it provides the highest possible security level expected for authentication systems based on one-time passwords.

Quard Technology offers its own dynamic password software fully implemented in the Biometric Smartcard, and it is also possible to implement other vendor's software. In this case, the Biometric Smartcard will work as a token that produces a one-time password with no need for making any changes whatsoever to the existing network infrastructure. In truth, It is a simple, swift and cost-effective implementation of a biometric authentication system, necessary for forward organisat ions and their data security.

PKI certificate

The Biometric Smartcard works with a PKI (digital signatures, authentication over networks, encryption) without the need of new infrastructure. By storing your private key directly on the Biometric Smartcard, you can make your digital certificate personal and protect it against abuse if it is lost or stolen.

The one stop shop solution

Since the Biometric Smartcard is mobile and works without any help from external devices, it can be used as an "all in one solution" performing all the tasks and applications that a modern digital environment requires. It can be used in the following ways;

- As a token providing a one-time password
- As a secure storing media (PKI digital certificate/private key)
- As a biometric door access key
- As a biometric passport
- As a biometric Health Card
- As a biometric credit card (Visa, American Express etc.)
- As a biometric national ID Card

SECURITY/ LEGAL ISSUES

Existing Match on Card technology

To gain maximum security, the fingerprint template must be stored securely in a closed environment. This closed environment is normally a traditional smartcard. If the fingerprint matching procedure is performed outside this closed environment, it is exposed to the open environment where anyone could steal the template. Even if the fingerprint template is protected by another security mechanism, this is to be viewed as the weakest link, and the biometrics does not really add any security. The only way to ensure that security is kept is to;

- Never let the fingerprint template leave the closed environment
- The fingerprint matching has to take place in this closed environment
- Ideally the acquisition and pre-processing of the original fingerprint image should also take place in this closed environment

The existing Match on Card can only take place if a biometric smartcard reader connected to a computer is present. In other words, the smartcard only stores the fingerprint template and needs power from a biometric smartcard reader to do the matching. When it comes to acquisition and pre-processing of the original fingerprint image further help from a PC is needed. This has to be viewed as the weakest link in the existing Match on Card technology since there is no guarantee for a non-tamper proof environment outside the smartcard. Mobility is also a problem since the smartcard is dependent of a biometric smartcard reader and a connected PC to work.

Taking our technology a step further

Quard Technology takes the Match on Card technology a quantum step further by undertaking all the processing in one and same component on the smartcard, without any help from external devices like smartcard readers or computers.

It offers true mobility for the user, but also some other benefits related to security and legal issues.

This is the present prototype of the quard card

Personal security

Since acquisition, enrolment and verification of the original fingerprint image are done directly inside the Biometric Smartcards secure environment without any help from external devices, any concerns about violating personal integrity and the whereabouts of the user's personal biometric data is eliminated. The Biometric Smartcard is made personal and cannot be accessed by anyone else. The templates are never exposed to a non-tamper proof environment and the users carry their own templates around with them.

No more concerns about legal issues

Since the Biometric Smartcard during acquisition, enrolment and verification of a fingerprint will never be in physical contact with any external device and since the fingerprint template never leaves the card, there is no longer a need for the card issuer to ask any authority for permission to use this technology. A fingerprint template cannot be compromised by anyone or any system and will therefore eliminate any concerns about security and legal issues for good.

Online/Offline communication

The Biometric Smartcard can perform both online and offline communication with networks, door access points etc. Online communication can be performed through a standard smartcard reader, wireless via RF, Bluetooth or infrared. Offline communication can be performed by manually typing in a one-time password produced by the Biometric Smartcard.

ISSUING AND INITIALIZING OF BIOMETRIC SMARTCARDS

Step one – issue and initialize biometric smartcard

Step two – hand over biometric smartcard to the user

Step three – the user swipes finger across sensor on the biometric smartcard

Step four – template of the fingerprint is created

Step five – template is encrypted and stored in internal memory on the biometric smartcard

Step six – the biometric smartcard is locked and fingerprint template can never be reset

Step seven – the user swipes finger across sensor and verification takes place

Step eight – upon verification of the user all applications will be opened

quard technology aps: Algade 44 - 4000 Roskilde Denmark. Telephone: 70 22 51 83 Fax: 46 327 328 Email: mail@quardcard.com

www.quard.dk

quard card

MOBILE BIOMETRIC AUTHENTICATION

Stand-alone Match on Card

No need for external devices

Dynamic password generator

quard technology aps

www.quard.dk