Oberthur Card Systems
The Key to an Open World

ID-One BiothentIC

Oberthur Card Systems offers one of the first card-based biometrics authentication solutions which secures all information within the card itself.

ID-One is Oberthur Card Systems' tailor-made smart identity solution for governments. Embracing a wide range of technologies, the ID-One solution also supports biometrics - physical verification technology which can be integrated into a smart card to allow highly secure transactions. Oberthur Card Systems' ID-One BiothentIC solution combines biometrics technology with PKI (Public Key Infrastructure), introducing physical contact to electronic authentication.

ID-One BiothentIC is a unique end-to-end solution which allows users to conduct secure electronic transactions by authenticating themselves via fingerprint matching, thus reinforcing the security of electronic signatures, network access control and similar authentication processes in the electronic world.

"One Touch" Security Pack

Developed in partnership with id3 Semiconductors, ID-One BiothentIC is offered as a software package which can be customized to meet clients' needs. The ID-One BiothentIC software package includes:

- ID-One Cosmo 64 card
- Biometrics smart card reader
- Client software
- Enrollment software

Biometrics Authentication Solution

ID-One BiothentIC is based on Java™, the unique open standard application programming language. Java brings advanced security and flexibility to the solution and can be easily adapted to a wide range of applications:

- Online authentication on public networks
- Private network access control
- Physical access control (buildings)

ID-One BiothentIC marks a real breakthrough in terms of securing access to PKI-based networks. In most biometrics identification methods, the matching operation is performed outside the card and information needs to be sent to an external device for authentication. With ID-One BiothentIC, the reference template and the matching algorithm are stored in the card itself, preventing crucial information being tampered with or stolen.

The fingerprint authentication process is extremely user-friendly. It offers more convenience than a PIN code which can easily be forgotten or copied. The fact that the matching fingerprint template is stored in the card (portable and personal) offers great flexibility and eliminates possible concerns about a virtual biometrics/fingerprints database.

Further Information:
www.oberthurcs.com
info@oberthurcs.com

ID-One BiothentIC in Action

How does it work?

- The user inserts the ID-One card into a smart card reader. By sweeping his or her finger across the biometrics sensor on the reader, the fingerprint acquisition and image processing begins.
- The ASIC (Application Specific Integrated Circuit) located within the smart card reader performs a reconstruction of the image in order to extract the essential information from the fingerprint. This information is then sent to the smart card, where a reference template has been stored in the chip.
- If both templates match, the card is temporarily "unlocked" - authorization is given for the card to become active in the existing PKI structure, and a successful verification message is generated. If the templates fail to match, the card remains locked.

Technical Features

- **Interface:** standard serial port or USB.
- **Hardware:** ASIC technology for image processing.
- **Compliance:** ISO 7816-3 (T=0, T=1) PC/SC compatible.
- **Security:** matching process and reference template stored inside smart card. Reference template created inside the reader (not on the PC) at Enrollment stage.
- **Biometrics:** 500dpi FingerChip™ based imaging system.
- **Software environment:** Bio-PKCS#11, Bio-CSP for integration in PKI, Enrollment software, SDK for integration.
- **Performance:** average verification time < 2 seconds. False Acceptance Rate (FAR) < 10^{-5}. False Rejection Rate (FRR) < 1%-5% (can be adjusted). Template size ± 200 bytes.

Further Information:

www.oberthurcs.com

info@oberthurcs.com