



SaveGarde

Access Control with IrisGuard:



Largest Iris Application in the World ...

Security in a humane atmosphere

The World's Largest Iris Homeland Security Deployment ... More than 30 Million people searched ... More than 40 trillion comparisons made ...

Why Iris-Recognition?

Most of the current means of access control carry considerable risks. Passports or RFID cards can be stolen or falsified, finger-prints and face scans show problems of inaccuracy. The only safe approach to protect identity and to prevent unwanted intruders is Iris-based identification. The IrisGuard system, which we apply is "... the first devices tested under IBG's cross-comparative methodology to achieve perfect transactional matching error rates (0.00% ...)" as testified by the International Biometric Group. This means, it is completely unbeatable. The methodology is not DNA based, emits no radiation, is non-invasive, contact-free (no communicable diseases) and 10-times more accurate than fingerprints. With 580,000 comparisons per second, analysis is extremely fast. No moving parts or contact handling, as well as high quality materials, leads to low maintenance costs. The data used is encrypted and highly protected against misuse. Ietely insurmountable.

How does it work?

The visitor stands for a moment in front of the Iris-Camera aided by automatic voice control. Our Iris-cameras have an incorporated eye-finding mechanism, optimize light and focus (we learned from 24 million trial runs), detect glasses or contact lenses - and can handle them, and verify the liveliness of the eye. Enrollment and Visitor Identification can be accomplished from the same desk, so separate enrollment stations are no longer required. Iris-Recognition is completely sufficient as stand-alone means of identification. Visitors once enrolled are only identified by Iris-recognition. This slimmed down process of access control is thus made fraud-proof and visitor flow faster. It can be complemented by a card or passport reading process. In that case, the visitor's identification document is also verified.



*Iris Recognition is non-invasive,
contact-free and emits no radiation*

Technical Data on the Camera System:

Very Fast:

- 580,000 Comparisons/Second

Perfect Focus

- Auto focus
- Fine Focus
- Focus QC

Pupil Dilation

- Pupil/Iris ratio detection
- Flash tickler
- Eye Openness
- Openness QC

Specular reflections

- Glass neutralization

Ambient conditions

- Auto saturation
- Auto shutter speed
- Tolerant of lighting

Motion blur

- Auto shutter speed

Interfaces for 'solution in a box' application:

- Industrial quality server for continuous operation
- Scalable from small user sizes up to millions of users
- Operates as intra- and inter-corporate device
- Local or Web based Iris bank solutions
- Customer special surface with easy to use functions for enrollment, recognition and evaluation in combination with a reaction to the customer own automation and process level
- RJ45 (Gigabit) connection ports, USB ports
- Output data can be integrated in all relevant access control and intrusion detection systems through standard interfaces.
- Interfaces to PROFIBUS DP, PROFINET, CANBUS, DEVICENET, ETHERNET, TCP/IP etc
- IG-AD100 Camera
- Possibility to add enrollment and recognition components such as Chipcard reader, Passport reader

The security Model:

Imager USB protection

- 24 Byte OTP
- Two 3DES Keys
- SHA2 signature

Client-server-client protection

- Expiring OTP (5 seconds)
- SHA2 signature
- 3DES key (site specific)

Attack detection

- Client lockdown after 3 failed:
 - Recognitions
 - Acquisitions
 - Inquiries

Tamper-detection of:

- User Data
- Iris templates
- System logs

Template protection

- 3DES key (site specific)
- SHA2 signature
- Template never returned to caller.

Key generation

- Client generated
- Three keys (storage, transmission and images)
- 3DES-based
- Templates permuted

Client Authentication

- Username/password
- Username/password & Iris logon
- Username/MaClD
- Username/MaClD & Iris logon

Client Authorization

- Separate business and IT management
- Enroll, modify, delete, Recog and activate privileges.

Network separation

- Web servers and Database and Application servers can be on different segments

Data-Security Standards used:

Triple DES Encryption that complies with:

- FIPS PUB 46-3, Data Encryption Standard (DES), [FIPS46].
- FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, [FIPS74].
- FIPS PUB 81, DES Modes of Operation, [FIPS81].
- NIST Special Publication 800-20 Modes of Operation Validation System for the Triple Data Encryption Algorithm [TMOVS].

SHA-256 Digital Signature algorithms that complies with:

- FIPS PUB 180-2 Secure Hash Standard, [FIPS180].

The OTP random number generator that complies with:

- ANSI X9.31 Appendix A [AX931] (which replaces X9.17 Appendix C).
- FIPS PUB 140-2, Security Requirements For Cryptographic Modules [FIPS140] (as updated on 3 December 2002).
- Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program [FIPS140IG].