

LSEC Biometrics 2011

How biometrics is merging the roles of Physical and Logical Access Control

Martin George - CEO

Smart Sensors Ltd

UbiCenter
Heverlee

1 December 2011



© Smart Sensors Ltd, 2011

World e-ID 

Agenda – key topics



- It's an Interconnected World
- Networked systems: why authenticate user identity?
- Where should I authenticate users?
- Using biometrics to control access policy via identities and permissions of logged-on users
- The role of Privacy Enhancing Techniques
- A recent airport implementation

What's the problem?




- Increasing use of cloud-type resources for industrial purposes
- Global ID Fraud already costs many € billions
- Unidentified network traffic is rapidly increasing
- Ubiquitous IP addresses
- Government and Industrial espionage is a highly lucrative sport
- All Organisations need to protect on-line resources intended only for authorised workers



They've had the same problem since 1997!

Where are we today?



- Today's internet has billions of global users

- Cloud Computing:

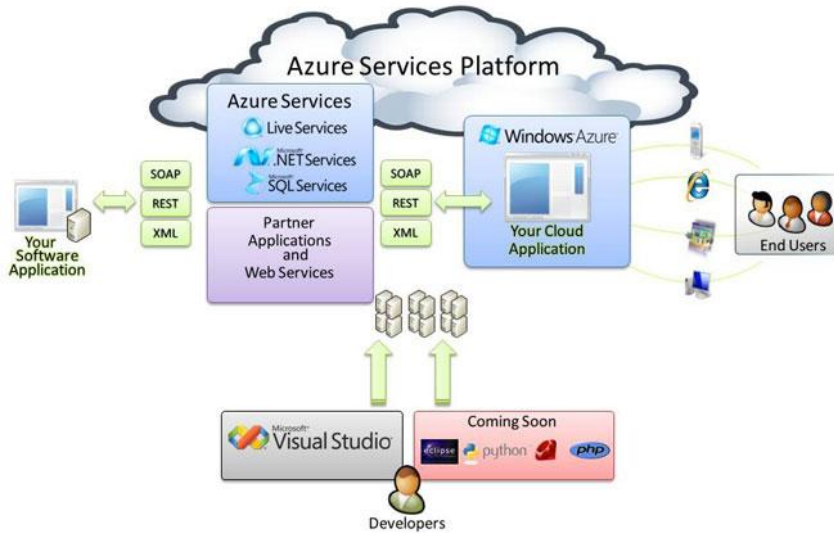
- ✓ A huge market opportunity
- ✓ Many user benefits
- ✓ Truly "disruptive" new applications
- In its infancy
- Security, Privacy



- Corporates making use of similar architectures

⊗ **How to protect and secure resources that may open up € trillions in business opportunities?**

Typical cloud services architecture

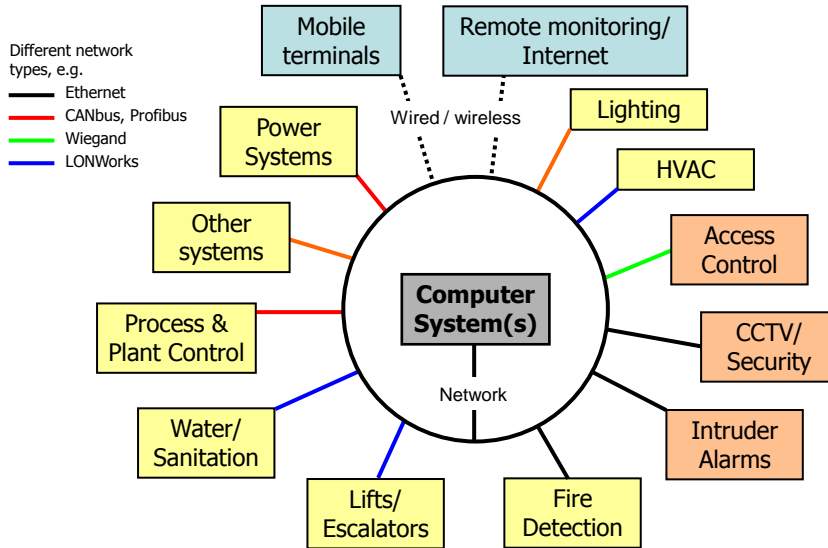


Current security and access policies



- Microsoft's Cloud security policy white paper (May 2009):
<http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf>
 - "Need-to-know" and "Least Privilege" models; Role-based access
 - "Appropriate measures to gain access: ... multi-factor, passwords, tokens, smart cards, or *biometrics*" → **CLAIMS**
 - Reconciliation of user accounts against authorisations
- Amazon S3 security policy/access credentials (Aug 2010):
 - http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
 - "Controls [that] provide reasonable assurance" over aspects including Amazon employee access, Logical and Physical security, Secure data handling, Data integrity availability and redundancy
 - **Sign-In:** e-mail address and password; [optional] Gemalto sync token
 - **Request Authentication:** Access Keys, X509 certificates, Key pairs

Typical BMS connectivity



Isn't that a worry?

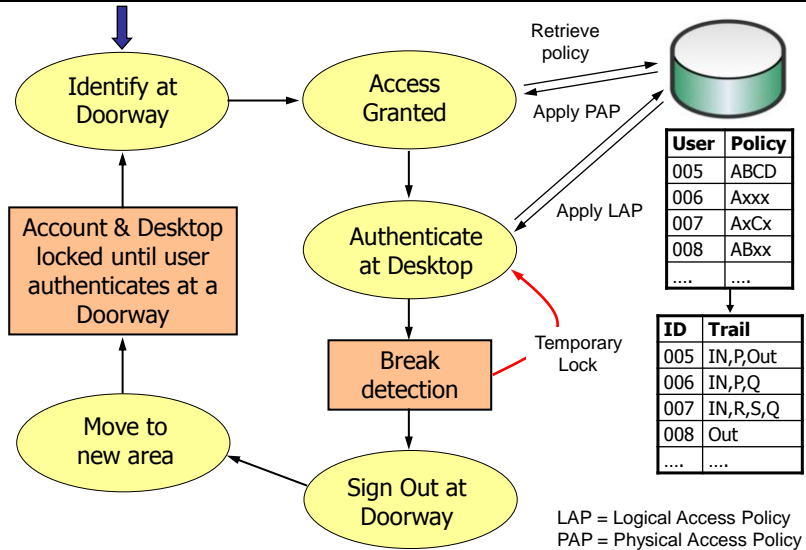


No wonder bodies concerned with Critical National Infrastructure are taking notice....

Requirements of a solution


- ✓ Secure the communications channel for a specific ID
- ✓ Exploit existing ID access control structures like SSO
- ✓ Apply and enforce policies appropriate to access level
- ✗ BUT – Existing credentials (passwords, PINs, cards) are too easily shared, stolen or hacked
- ?
- How to use Biometrics as a vital authentication factor
 - Face Recognition often not accurate enough
 - Fingerprints often inconvenient, can be spoofed, need additional sensors
 - Iris Recognition seen as expensive (until now)
 - Methods of ensuring “persistent ID”
 - Address “Human Factors” and privacy concerns

“Doorway-to-Desktop” user process



Core Management Components 

Enrolment	Authentication/ Identification	Policy Admin	Monitoring
Enrols new users into system	Captures presenter's biometric(s) and searches database to authenticate / identify	Manage / update user information including roles and permissions	Alert detection and handling system
Gathers and stores biometric samples and/or templates in a database	Retrieval of hierarchy level, and access policies associated with presenter	Manage / update security policy	Keep track of system activity and access events
Moves users' biometric data between authentication repositories	Biometric challenge / response feature (may be enabled via break detection)	System configuration	Logging and responding to access failures
Visitor/guest creation tool	At doorway – apply PAP At desktop – apply LAP	Manage physical locations of computers and access devices	Hand off user information and status to other parts of BMS
	Manage exit events		Inboard / outboard status display

Potential benefits and added value 

- Combination of logical and physical access control
- Potential for non-contact, hands-free access
- Time saved in getting staff productive upon sign-on
- Automatic enforcement of access policies and hierarchies
- Natural integration with time and attendance systems
- Extend attendance audit trail to remote + "hot-desk" workers
- Remote monitoring and alerts for security personnel
- Avoid card systems and pin-pads, or strengthen their use
- Same generic system structure – many applications

Why Iris Recognition?

- Fundamentally simple
 - A digital photo of the eye, using night-vision illumination (Near Infra-Red = NIR)
 - Small match template sizes <600 bytes
- Exceptional discrimination power
 - Excellent for IDENTIFICATION applications
 - De-duplication in large scale enrolment programs
- Non-contact, hands-free usage
 - Non-intrusive, Convenient, Versatile
- Good where fingerprints are not good
 - Low and high humidity, manual workers, elderly, ...

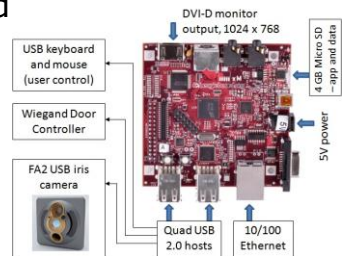
ID Appliance for door / desktop

- Megapixel camera with autofocus Iris Capture
- Persistent ID feature (via camera)
- On board image processing and template creation with data encryption



- No raw/unprotected biometric data need leave the sensor head

- Modular OEM design
- Demonstrated with ARM Cortex A8



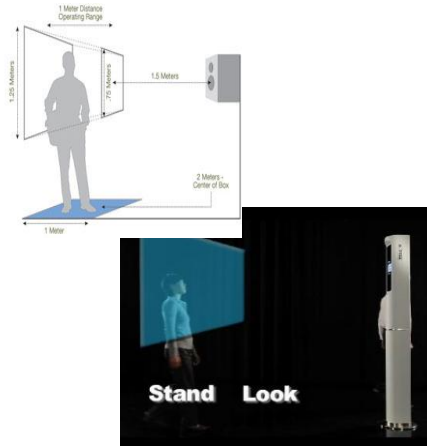
Biometric Access – at a distance



- Example 1 – Iris On the Move™ by Sarnoff Corporation



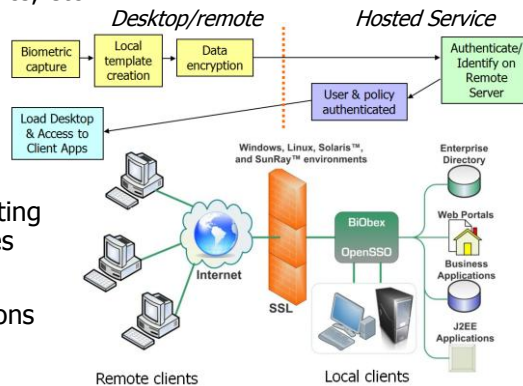
- Example 2 – InSight™ by AOptix Technologies



Distributed Enterprise computing example



- Open Source, Open Standards
- Highly secure, meets international privacy standards
- Extendable for different authentication schemes like Java cards, PIV cards, other biometrics, etc.
- Highly scalable to large numbers of users
- Flexible hot-desk access policy using OpenSSO
- Interoperable across different vendors, operating systems and technologies
- Good fit for Customer's Java EE (J2EE) applications



Human factors considerations



- Non-contact or Contact?
- Verification or Identification?
- Ease of use and intuitiveness
- Motivations to use or abuse the system
- Attitudes to organisation's access/attendance policies
- Managing exceptions and incorrect use
- Education and training

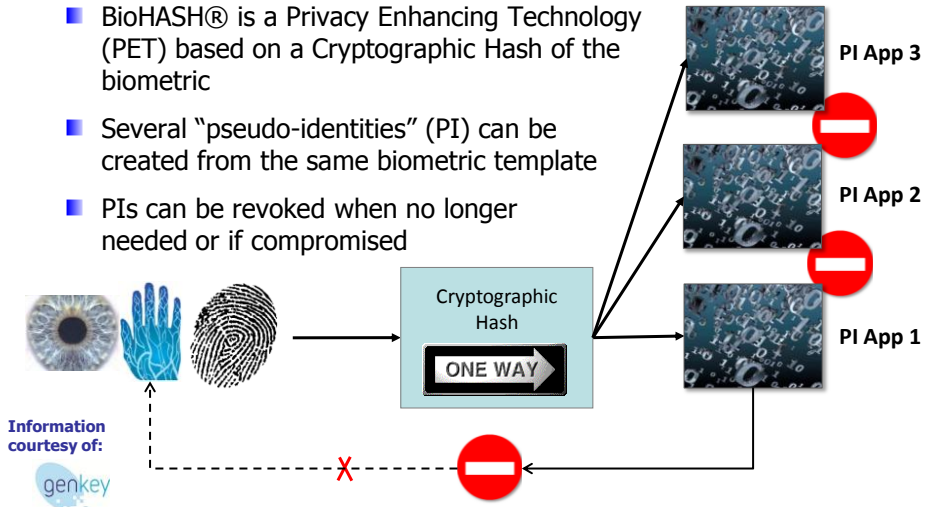
Data Protection and Privacy



- Biometric data is the personal data of the individual
 - Falls within Data Protection law in UK, EU, USA
- Is a template biometric data?
- The role of data encryption and key infrastructure
- Local versus central database matching
- Techniques for revocable biometrics

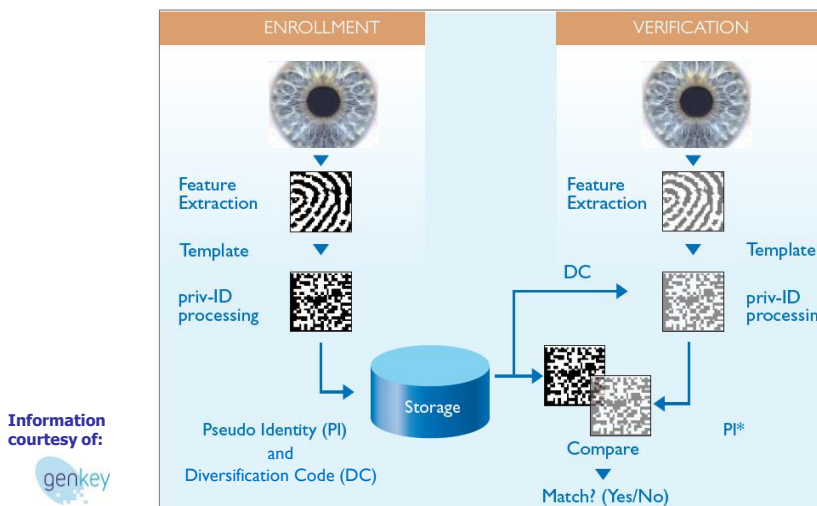
Example of Privacy Enhancing Technology

- BioHASH® is a Privacy Enhancing Technology (PET) based on a Cryptographic Hash of the biometric
- Several "pseudo-identities" (PI) can be created from the same biometric template
- PIs can be revoked when no longer needed or if compromised



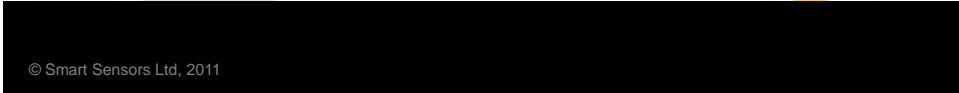
BioHASH® Deployment Procedure

Same enrolment and verification procedure as traditional biometrics



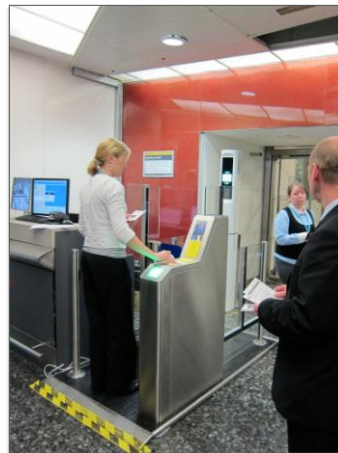
Airport application

London Gatwick South Terminal



Gatwick Airport Joint Boarding Lounge


- Joint Boarding Lounge Challenge
 - Domestic and international transit passengers in the same area
 - If domestic and int'l travelers swap boarding passes, the int'l passengers could skip immigration
 - 6,000 – 10,000 enrollees per day
- Security Solution
 - Uses Smart Sensors' Iris Biometrics to authenticate passengers in AND out
 - Automated enrollment of passengers before security
 - Automated authentication before domestic-only boarding lounge
- Deployment Requirements
 - Usability
 - Throughput
 - Consistency of performance



Smart Sensors Ltd
Tools for Iris Recognition Engines

© Smart Sensors Ltd, 2011. Company proprietary – please do not distribute without permission

Gatwick Airport
Joint Boarding Lounge



34 Lanes – Go-Live: May 23, 2011



Enrollment: Fully automated e-Gates (as in picture)
Reconciliation: Attended, at Boarding Gate (not shown)

Smart Sensors Ltd

Tools for Iris Recognition Engines

© Smart Sensors Ltd, 2011. Company proprietary – please do not distribute without permission


Concept of Operations

1. Scan boarding pass barcode
2. Stand at foot marks
3. Look at *InSight* system
4. Two eye capture (for enrollment) / One eye capture (for reconciliation)
5. Gate opens (if successful)

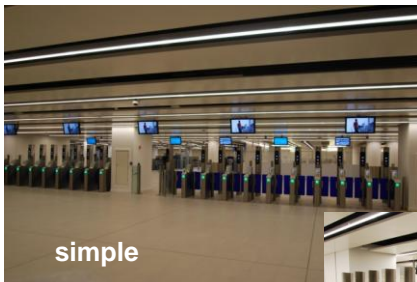
In case of usage issues

- Manual gates will be available
- Face-only capture will be available for those who cannot capture iris

Gatwick Airport
Joint Boarding Lounge



Joint Boarding Lounge System in Operation



simple



quick



hygienic



user-friendly

Smart Sensors Ltd

Tools for Iris Recognition Engines

© Smart Sensors Ltd, 2011. Company proprietary – please do not distribute without permission

Contact Details



■ Further information available from:

- Smart Sensors Limited
Carpenter House Innovation Centre
BATH, BA1 1UD
United Kingdom

Tel: +44 (0) 1225 388690

Martin George – CEO
mgeorge@smartsensors.co.uk

