



**IFSEC2010**

10 - 13 May 2010  
NEC Birmingham

**IFSEC 2010 Conference Programme**  
**Birmingham, 10-13 May 2010**



*Module C3 – Next Generation Biometrics*

# **Integrating biometrics into smart buildings management**

**Martin George**

**Smart Sensors Ltd**

# Agenda



- Applications, advantages and added value that biometrics can facilitate
- Understanding the challenges of incorporating biometrics into a security system
- Biometric modes – which are appropriate and what performance can you expect?
- Data protection and privacy considerations for biometrics in access control

# Applications, advantages, added value



- Focus on Buildings Management and Access control
  - ∅ Avoid card systems and pin-pads, or strengthen their use
  - ∅ Potential for non-contact, hands-free access
  - ∅ Automatic control of access policy and hierarchy
  - ∅ Combination of logical and physical access control
  - ∅ Natural integration with time and attendance systems
  - ∅ Extend attendance audit trail to remote + “hot-desk” workers
  - ∅ Remote monitoring and alerts for mobile security staff

# Challenges of biometrics systems



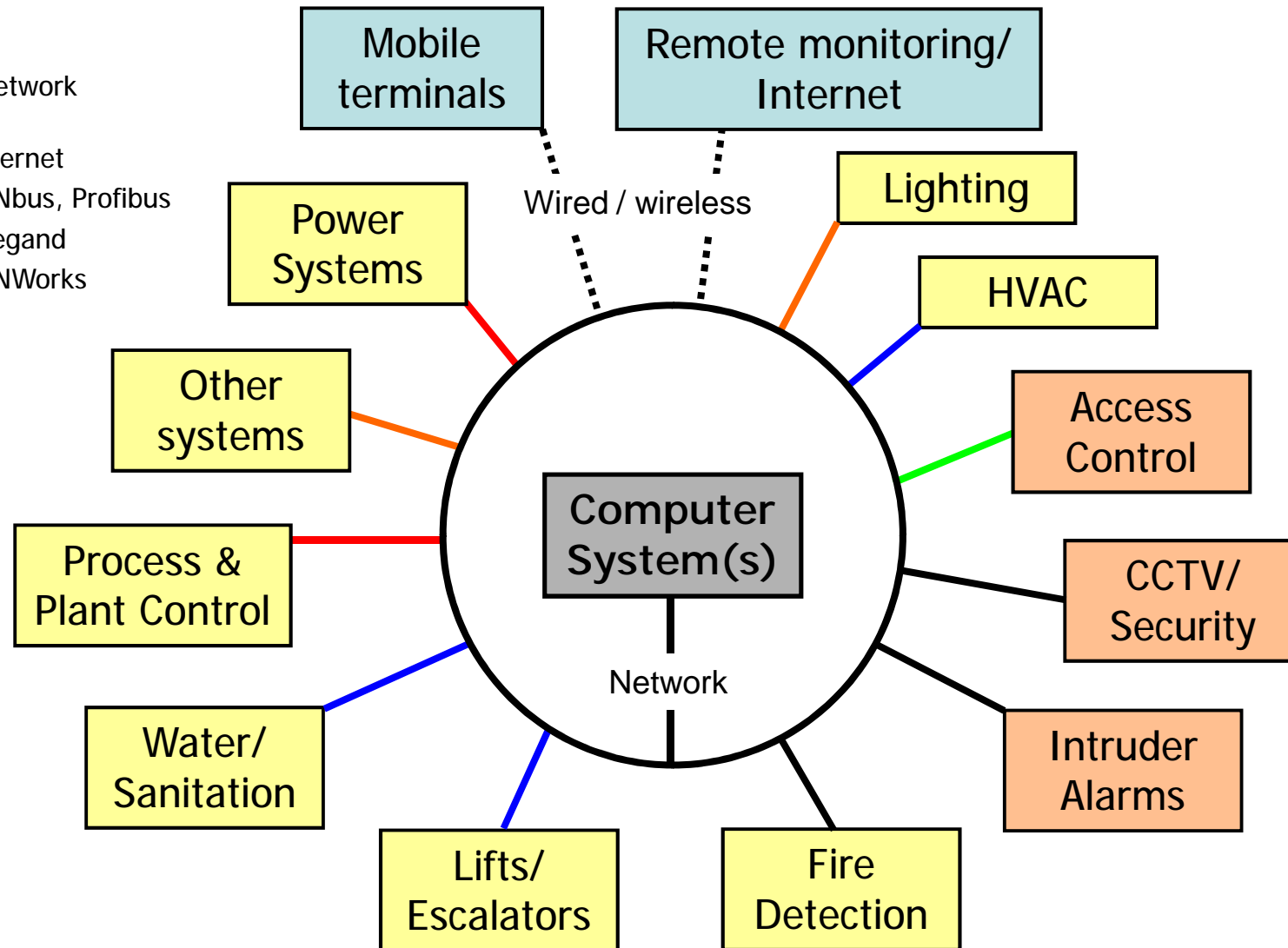
- Building management systems (BMS) architecture
- Managing Physical and Logical Access policy and the hierarchy enabled by Biometrics
- Controlling building and site systems / facilities according to identities and permissions of those present
- Managing errors and exceptions
- Human factors

# Typical BMS connectivity

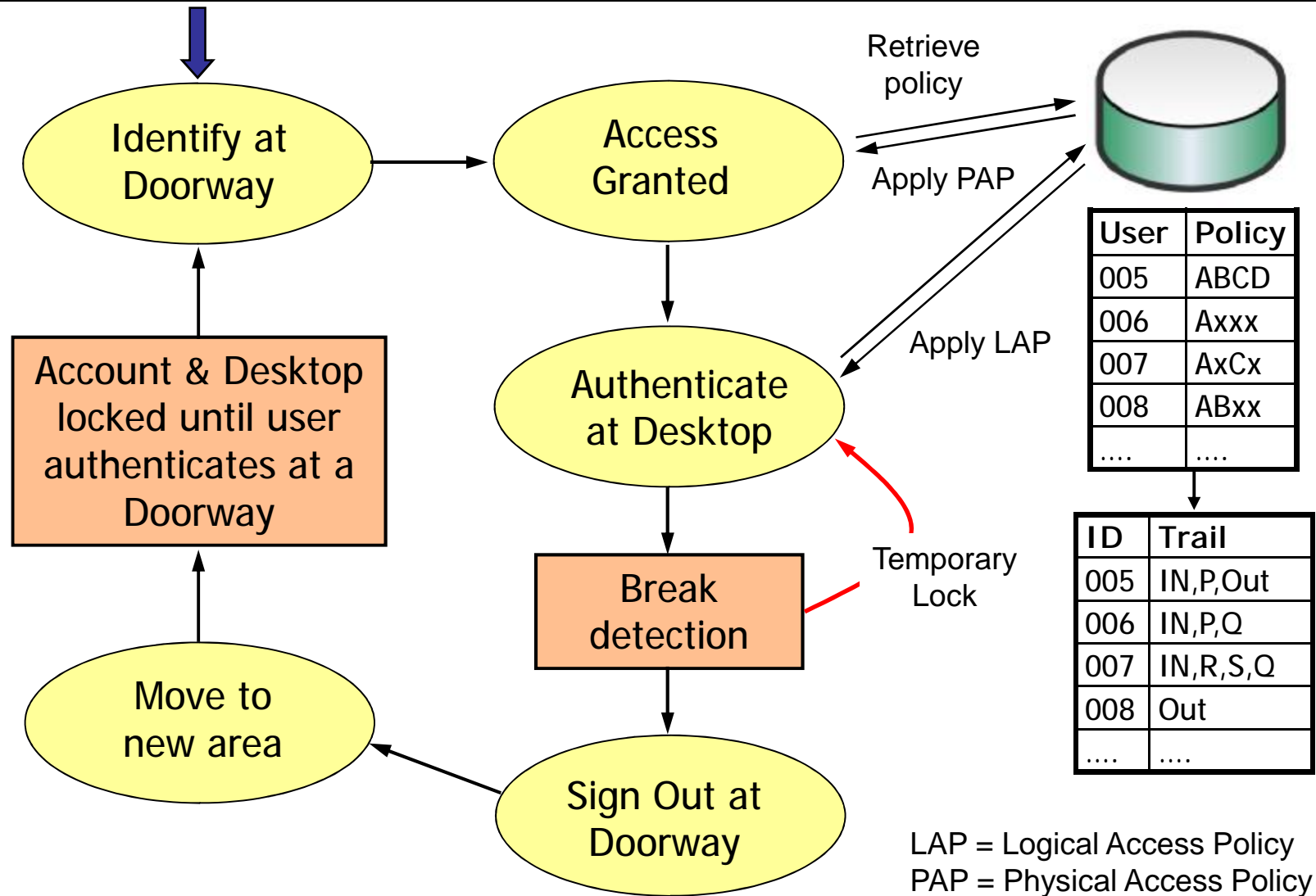


Different network types, e.g.

- Ethernet
- CANbus, Profibus
- Wiegand
- LONWorks



# “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

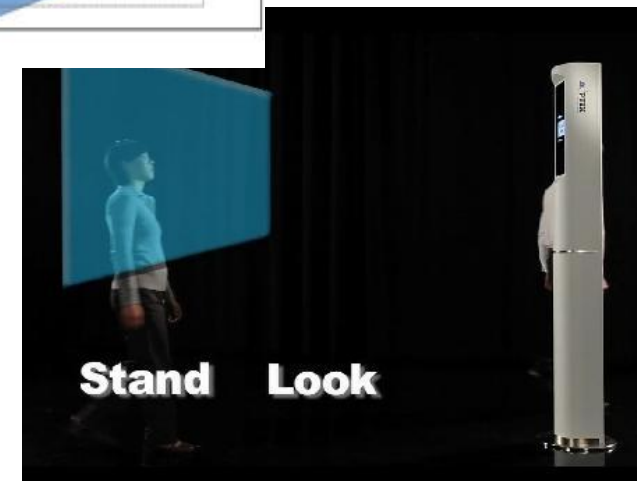
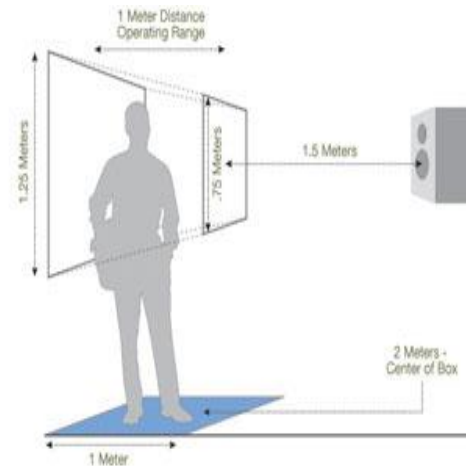
# Biometric Access – at a distance



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



- Example 2 – InSight™ by AOptix Technologies



# Biometric Access – at the doorway



- Professional fingerprint unit with pin-pad and card reader
- Iris cameras for door access with Wiegand and card reader interfaces



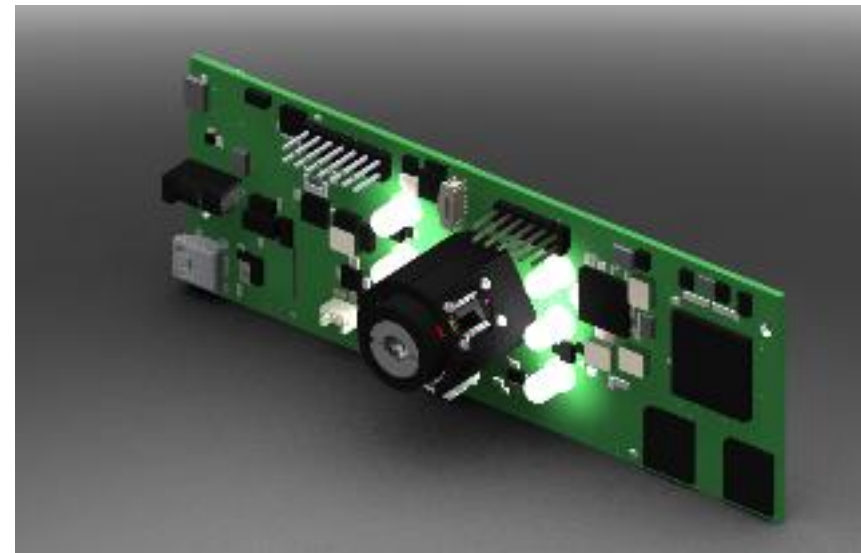
- Low cost wall/door units



# Biometric Access – at the desktop



- Fingerprint sensors already integrated into laptops
- Modified webcam with autofocus Iris Capture
- Persistent ID feature (via camera)
- On board image processing and template creation with data encryption
- No recognisable biometric data need leave the sensor head



# Interoperability

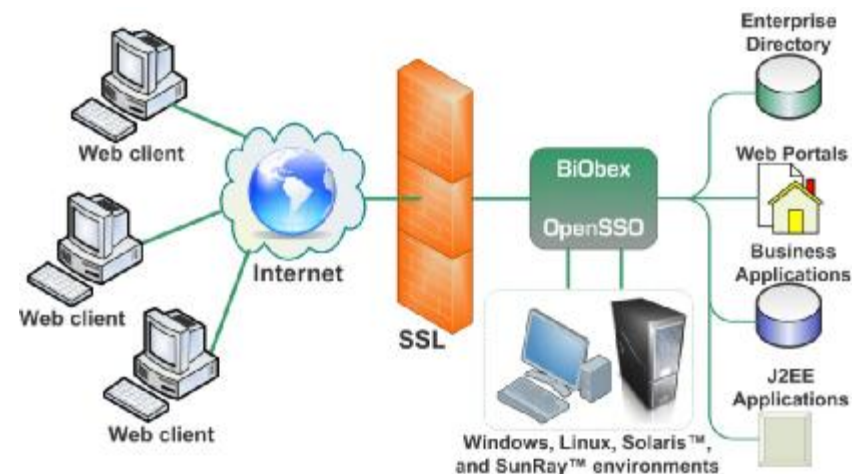


- Desktop Login
  - ∅ Microsoft Windows®
  - ∅ Solaris™
  - ∅ Linux®
  - ∅ Trusted Solaris™ and NSE Linux®
  - ∅ SunRay™ UTC
- Database Support
  - ∅ DB2, 7.2-Current
  - ∅ Oracle
  - ∅ SQL Server
  - ∅ MySQL
  - ∅ PostgreSQL
  - ∅ JDBC compliant DB
- Capture Device Interface
  - ∅ USB (1.1 and 2.0)
  - ∅ Ethernet (10/100, GigE)
- Directory Services Support
  - ∅ Netscape Directory Server
  - ∅ Microsoft Active Directory
  - ∅ Sun Java™ system Directory Server
  - ∅ LDAP
- Browser Support
  - ∅ Mozilla
  - ∅ Netscape
  - ∅ Internet Explorer
- Biometric Algorithms Support
  - ∅ Fingerprint
  - ∅ Iris
  - ∅ Face recognition (2D, 3D)
  - ∅ Palm, Vein
  - ∅ Standards based – agnostic to capture device

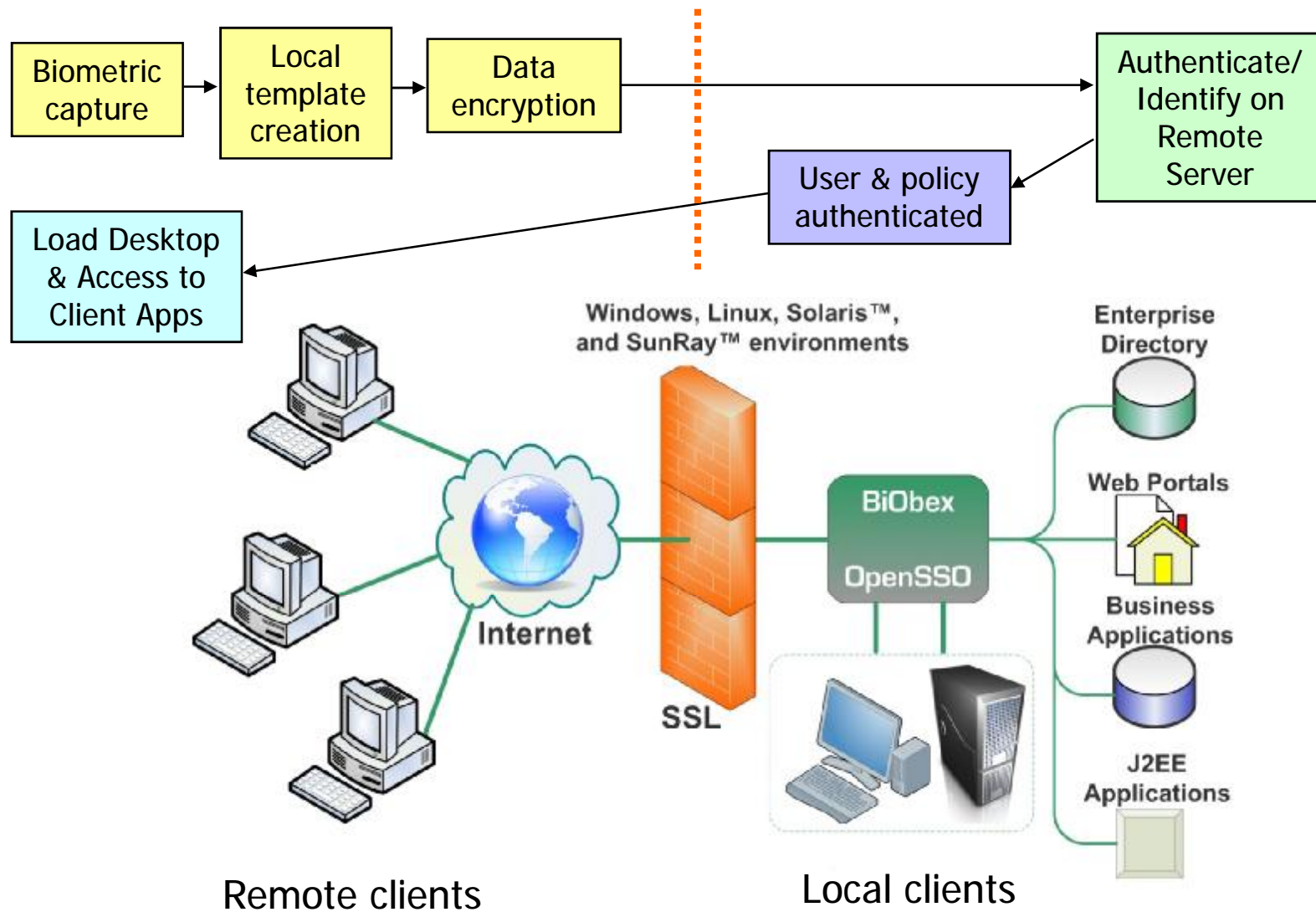
# Case Study – SunRay™ thin client system



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



# Case Study – SunRay™ thin client system

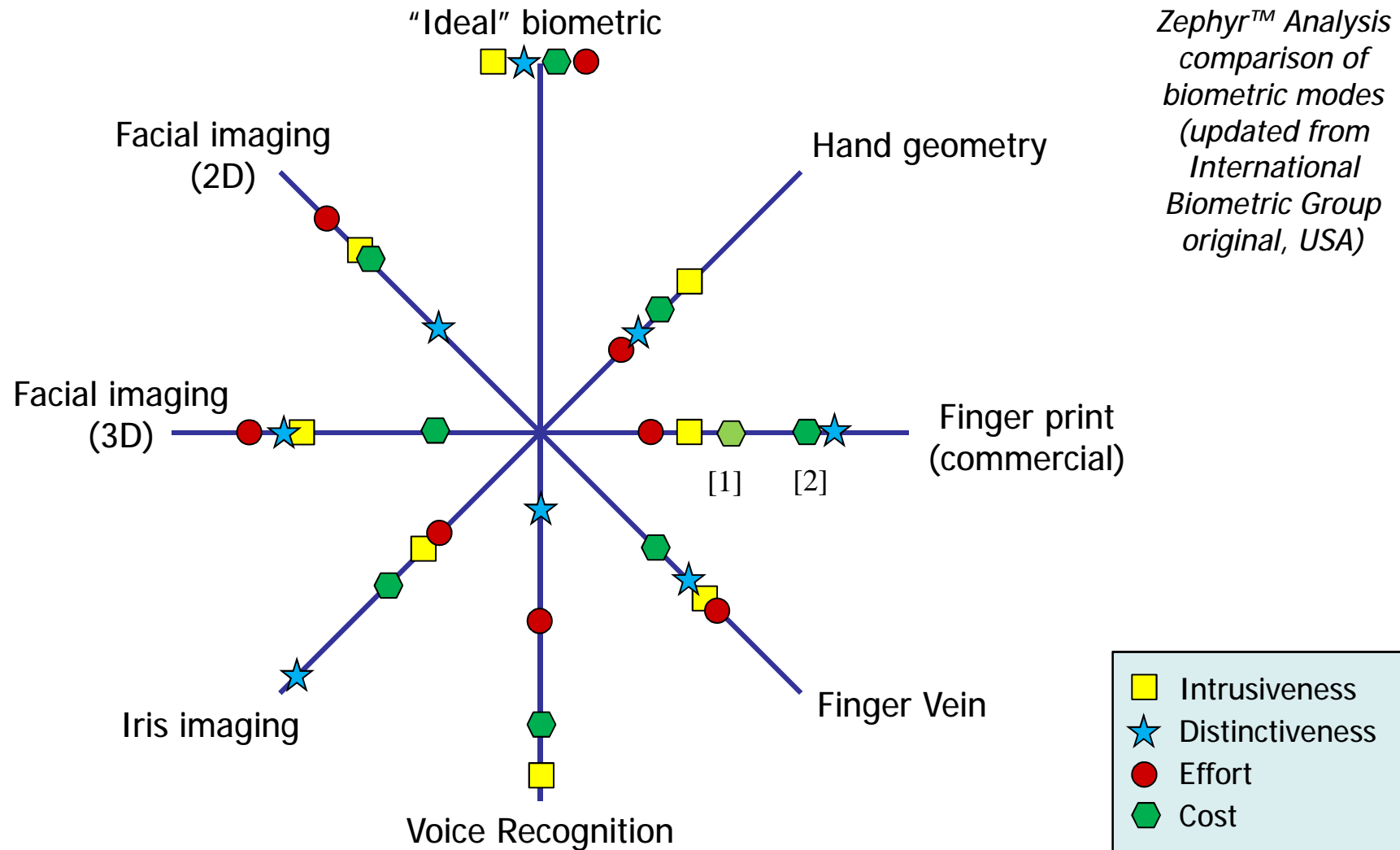


# Human factors considerations



- 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

# Key biometric modes for access control



# 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

# 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](mailto:mgeorge@smartsensors.co.uk)

