



# Biometrics and (e-) Identity

European Biometrics Forum

Max Snijder, CEO

**HIDE**

Policy Forum on Outsourcing of Systems  
for Detection, Identification and Authentication

London, February 9th, 2009



# AGENDA

- EBF Introduction
- Biometrics: a definition
- Business drivers
- Biometrics and (e-) identity
- Anonymous biometrics
- Risks
- Conclusions



# European Biometrics Forum

## **Mission:**

### **Advancing the proper and beneficial use of biometrics in Europe**

- Independent, multi stakeholder interest group to bring further the proper and beneficial use of biometrics in Europe and abroad
- Initiating, organizing, supporting, facilitating activities that support that goal
- Not for profit

Government

Academia

Industry

Citizens

# Biometrics: a definition

## **Definition**

Determining a persons identity or verifying a claimed identity by automatic means, based on a persons unique physical characteristics

ICAO: Face, finger, iris (passports & travel documents)

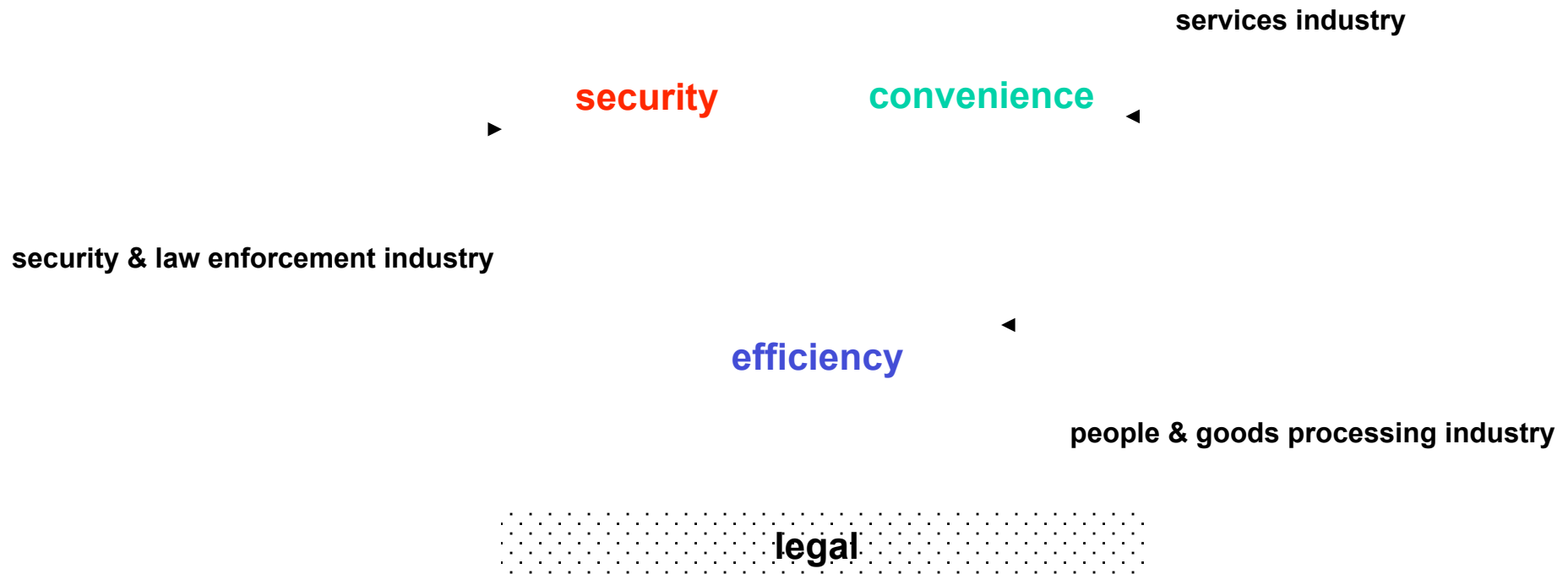
Other: vein, voice, retina, handgeometry, ...

Soft biometrics: hight, eye color, weight, ...

- Central identification (1:n)
- Central verification (1:1 with pointer)
- Local verification (1:1 with token)
- Local identification (1:n with distributed db)



# Business Drivers



# Biometrics and Identity

- Classic Biometrics = who you are (identification, law enforcement)
- Perceived link between identity and biometrics
- History of biometrics comes from physical world
  - Law enforcement
  - Supervised applications
- Crossover between physical and digital world
- Different risk profiles (stealing, spoofing, manipulating):
  - Physical risk is limited and managable
  - Digital risk is hard to manage

# What do Biometrics say about Identity?

- Answer:
  - as much as you want
  - as less as you want
- Depends on what data are connected to the biometric information (by the user / with consent)
- Depends on what biometric modality is being used
- If no data are connected, biometrics are anonymous and can be disconnected from identity
- Moving from identification/verification of identity to authentication

# Two different functionalities

- Establishing/verifying root identity
  - ”Identifying” Biometrics
  - 100% link to Identity
  - High value
  - High risk (spoofing, steeling)
  - Controlled/supervised environment
  - Who you are
- Biometrics for authentication
  - Anonymous Biometrics
  - 0% link to identity
  - Low risk
  - Unsupervised environment
  - What you know + what you have

# Two different scenarios

- Supervised
  - Border control
  - Access control
  - Surveillance
  
- Un-supervised
  - At home
  - E-services

- Generic risks of "identifying" biometrics:
  - Spoofing
  - Stealing
  - Manipulating
  - Uncontrolled labeling
  - Surveillance
  - False Match
  - Social engineering
  - Revealing personal information

# Biometrics and Privacy

EBF study for EC JRC / IPTS:

“Privacy and Security in large scale biometrics systems”

- Proportionality of the measures
- Purpose of the measures, and restrictions on the use of the data collected
- Voluntary vs obligatory
- Covert vs Overt
- Place of storage of biometric data
- Type of biometrics being used
- Effects of interoperability of databases
- International data exchange
- Control: rights of those providing their biometric data and transparency of purpose and authorised use
- Testing and certification of biometric techniques

Full report: [www.eubiometricsforum.com](http://www.eubiometricsforum.com)

# Anonymous Biometrics

- Biometric reference template can not be used to re-create the biometric raw data
- Template is not being recognized as being biometric data
- Biometric can not be used for 1:n search (no identification) based on image
- No raw biometric data shall leave the user's biometric template generating system
- No link to root identity or claimed identity
- Biometric information can be any modality from any person ("I am the only one who knows which biometric and from who")
- As long as it is the same as originally enrolled for a specific service
- Unsupervised enrolment
- Biometrics: what you know + what you have
- **Result: full user empowerment**

## We need guidance

- Policies/guidelines on how to manage biometric data for both scenarios:
  - ”identifying”biometrics (supervised)
  - anonymous biometrics (unsupervised, eID)
- Where do we get such policies?
- How do we make sure that there are European/international rules?
- How can the individual be empowered to manage his own biometric information?



# European Biometrics Forum

## Contact:

[max.snijder@eubiometricsforum.com](mailto:max.snijder@eubiometricsforum.com)

+31 624 603809 (direct)

+353 1 488 5810 (secretariat)