

# PETs FOR BIOMETRICS

**Nicolas Delvaux**

*Brussels, December 10<sup>th</sup>, 2010*



# THE PRIVACY/SECURITY DILEMNA

- **PRIVACY / SECURITY shall be reconciled**
- **PRIVACY and SECURITY are both dynamic concepts**
- **Just say: my solution is PET ?**

# PRIVACY: THE SECURITY'S UNFORTUNATE TWIN SISTER

## ▶ Much effort has been dedicated to SECURITY:

- Operational definition of a « secure » environment / application / usage / device with regards to a precise THREAT definition
- Formal requirements, evaluation and certification protocols with appointed authorities

## ▶ Similar effort shall be devoted to PRIVACY, with a strong need to develop:

- operational definitions for PRIVACY
- objective and transparent criteria to measure the level of SECURITY and PRIVACY provided by any given device / technology / usage .

# Biometrics as a “SET” (*Security Enhanced Technology*)

■ Biometrics is a set of tools enabling authentication or identification based upon physiological/behavioural traits of individuals

- Many modalities : fingerprint, face, iris, vein, DNA..
  - ✓ But also voice, signature, gait...
- With different performances and issues
- No « silver bullet » modality or technology



■ As any “SET”, use of biometrics can potentially raise privacy concerns:

- Misuse / Abuse
- Breach
- Function Creep

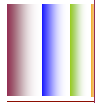
■ With issues specific to biometrics

- A priori non revokability



# BIOMETRIC DATA ARE PERSONAL DATA (DP)

- Biometric data fall under Directive 95/46 on personal data protection
  
- However, different legal perceptions into national transposition laws:
  - In most countries no specific provisions on biometrics in DP laws
  
  - Some tentative to consider biometric data as « sensitive data »:
    - ✓ “sensitive data”, like opinion, medical diseases, etc.
    - ✓ Biometrics can not be “hidden”
    - ✓ Only few modalities (face & DNA) reveal some sensitive data



# TO PROVIDE SOLUTIONS, INDUSTRY NEEDS MORE LISIBILITY

- **Different legal regimes across the Member States (MS): from prior authorisation to simple notification**
- **Key role of PROPORTIONALITY PRINCIPLE : It gives DPAs a wide margin of interpretation in deciding whether a specific system is compliant**
- **As a result: conflicting opinions in different MS on similar biometric applications**

# PROPORTIONALITY: A COMPLEX PRINCIPLE

## Time attendance



## Access control in sport stadium



## Access control in swimming pool



## At school



# HOW ABOUT THOSE BIOMETRIC DATABASES?



	<b>Juan Fernando LÓPEZ AGUILAR</b> <b>Groupe de l'Alliance Progressiste des Socialistes et Démocrates au Parlement européen</b> Membre <b>Espagne</b> Partido Socialista Obrero Español Né le 10 juin 1961, Las Palmas juanfernando.lopezagular@europarl.europa.eu
	<b>Kinga GÁL</b> <b>Groupe du Parti Populaire Européen (Démocrates-Chrétiens)</b> Membre <b>Hongrie</b> Fidesz-Magyar Polgári Szövetség-Keresztény Demokrata Néppárt http://www.galkinga.hu
	<b>Sophia in 't VELD</b> <b>Groupe Alliance des démocrates et des libéraux pour l'Europe</b> Membre du Bureau <b>Pays-Bas</b> Democraten 66 sophie.intveld@europarl.europa.eu http://www.sophieintveld.eu
	<b>Salvatore IACOLINO</b> <b>Groupe du Parti Populaire Européen (Démocrates-Chrétiens)</b> Membre <b>Italie</b> Il Popolo della Libertà Né le 18 novembre 1963, Favara salvatore.iacolino@europarl.europa.eu

# BIOMETRICS AS A PET?

- ▶ BIOMETRICS can be used as a tool to enable ANONYMITY



- ▶ Examples for welfare usages:

AUSTRALIA



biometric Methadone Dispensers can be used to assist drug addicts

U.S.



pilot programs using fingerprint have been implemented at the Mayo Clinic in Minneapolis and Catholic Health Systems in Buffalo for undocumented patients

## ■ MAIN OBJECTIVES:

- **Protect consumers' privacy and enhance users confidence**
- **Prevent impersonation**
- **Enable industry to build solution on a solide foundation**
- **Develop standardised process instead of a case-by-case approach**

## ■ A PREREQUISITE:

- **a precise and operational definition of risks, threats and vulnerability**

# PRIVACY ENHANCES SECURITY

- **Today, the evaluation of biometric products is limited to performance evaluation:**
  - speed characteristics
  - accuracy measures such as FAR, FRR, FTE
- **Privacy and Security shall become “a positive-Sum Paradigm”**
- **To do so, different tools are available or under development**

# PETs BASED ON COMMON CRITERIA METHOD (1/2)

- **“Common Criteria” (CC) an internationally recognised methodology used for security features and performance of IT security products and services**
  
- **CC certification is a mandated requirement in defence and national security applications and is becoming increasingly desirable in other Government services**
  
- **CC are based on 2 types of requirements:**
  - **Functional for security functions**
  - **Assurance for IT processes, uses and development**
  - ⇒ **different « security level » from EAL1 to EAL4**
  
- **The authority issuing certifications must be:**
  - **independent from the industry**
  - **a State trusted authority**

■ Such a scheme can be derived for biometrics

■ Specifications and requirements shall be defined by DPAs according to the CC methodology:

➤ Defining a Target of evaluation

- ✓ Defining the types of threats and vulnerability of the product/software/hardware
- ✓ Defining the levels of threats
- ✓ Defining the hackers typology:
  - *Ressources,*
  - *Expertise*
  - *time to prepare/operate an attack*

➤ Define level of robustness to attack

# PETs BASED ON COMMON CRITERIA METHOD

## ■ Advantages:

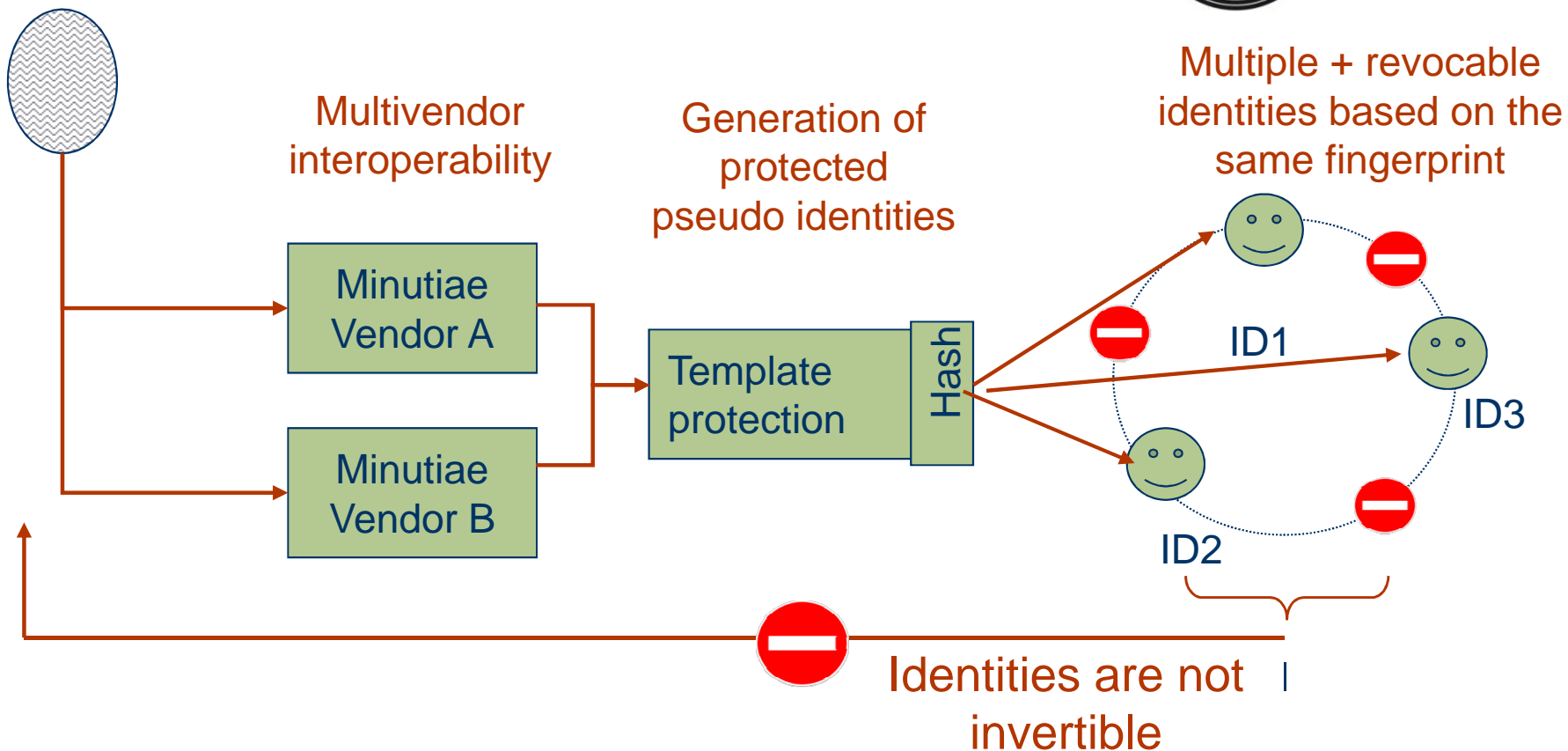
- A well-proven scheme
- Set the ground to structure the european market
- A win-win solution for end-users, DPA and the industry
- A technology neutral approach

## ■ Disadvantages:

- A significant initial collaboration effort between the different stakeholders
- Certification fees for the industry: need to find a business model for a niche market with a lot of small players

# PETs BASED ON BIO-ENCRYPTION

Fingerprint biometry



# CONCLUSION AND RECOMMANDATIONS

■ **Tools to protect privacy are available or can be developed**

▶ **DPA and industry collaboration is paramount:**

- ▶ For a precise definition of risks, threats and targets
- ▶ To drive an objective and transparent evaluation protocol
- ▶ To define a relevant certification business model

■ **Vertuous schemes could enable and favour the emergence of industrial solutions**

■ **As a result, both security and privacy would be improved for the benefit of end-users**

**Thank you for your attention**