



A REFLEXION ON PETs FOR BIOMETRICS

Carole PELLEGRINO

*Workshop on Economic Benefits
for Privacy Enhancing Technologies*

Brussels, 12th November 2009



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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».





3 QUESTIONS

- ▶ **Is there a need to adjust the existing legal framework?**
- ▶ **Shall Privacy become a core element of Security?**
- ▶ **Which tools could be used for biometrics?**

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».





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
 - Biometrics data can be considered as sensitive when they reveal racial, ethnic origins or health
 - Some MS consider biometric data as « sensitive data »

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



TO PROVIDE SOLUTIONS, INDUSTRY NEEDS MORE LISIBILITY

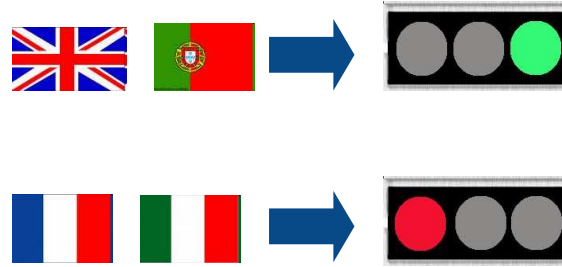
- ▶ **Different legal regimes across the Member States (MS): from prior authorisation to simple notification**
- ▶ **Key role of PROPORTIONALITY PRINCIPLE : It gives DPAs a wide margin of interpretation in deciding whether a specific system is compliant**
- ▶ **As a result: conflicting opinions in different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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

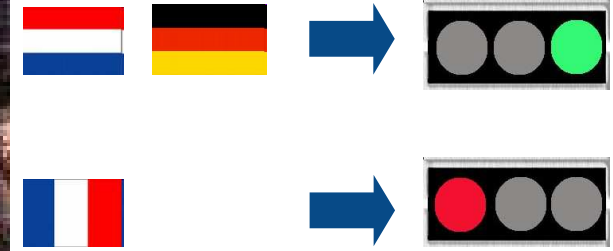


PROPORTIONALITY: A COMPLEX PRINCIPLE

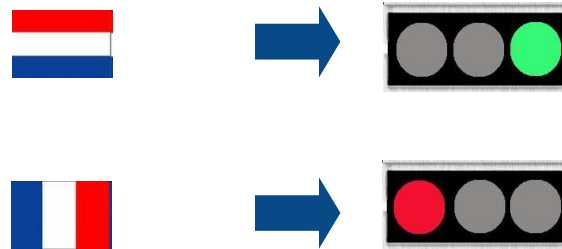
Time attendance



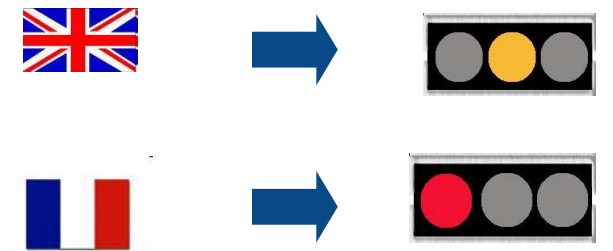
Access control in sport stadium



Access control in swimming pool



At school (Fingerprint)



« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



HOW ABOUT THOSE BIOMETRIC DATABASES?



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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



DEVELOPING PETs FOR BIOMETRICS

▶ 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**

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

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 .

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



PRIVACY ENHANCES SECURITY

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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

■ ■ ■ ■ ■ PETs BASED ON COMMON CRITERIA METHODOLOGY (1/3)

- ▶ “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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

■ ■ ■ ■ ■ PETs BASED ON COMMON CRITERIA METHODOLOGY (2/3)

- ▶ 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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

■ ■ ■ ■ ■ PETs BASED ON COMMON CRITERIA METHODOLOGY (3/3)

▶ Advantages:

- A well-proven scheme
- Sets 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

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



PETs BASED ON BIO-ENCRYPTION TECHNIQUES

▶ BE implies template protection:

- Initial biometric data is converted and encrypted so that the original data can not be retrieved
- Converted data can serve as password, anonymous identifier, or pseudo identity
- A compromised identifier can be easily revoked
- A new identifier can be easily generated from the same initial biometric data
- Performance of converted biometric data is lower



« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

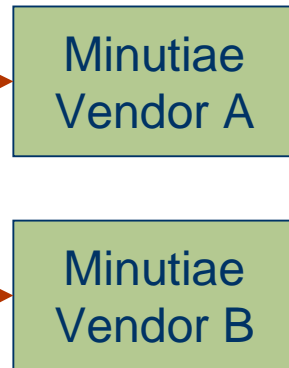


AN IMPLEMENTATION ON BIO-ENCRYPTION

Fingerprint biometry



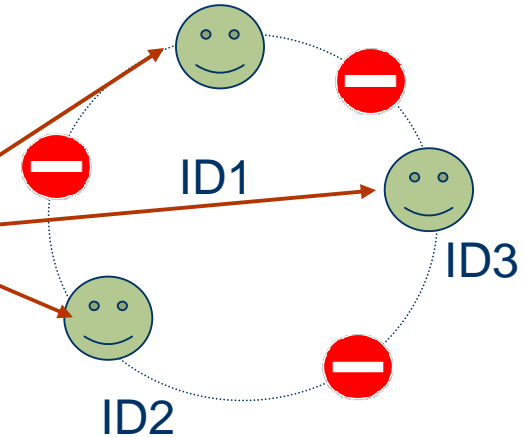
Multivendor interoperability



Generation of protected pseudo identities



Multiple + revocable identities based on the same fingerprint



Identities are not invertible



« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



PETS: THE MULTI-BIOMETRIC APPROACH

▶ Combine two biometrics

- The templates are degraded to weaken the probability of recognition
- The combination of the two templates allow recognition

▶ Trade-off between accuracy and privacy



« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».



CONCLUSION AND RECOMMANDATIONS

- ▶ **The current legal framework needs to be updated**
- ▶ **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**

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».





THANK YOU FOR YOUR ATTENTION

carole.pellegrino@sagem.com

« Ce document et les informations qu'il contient sont la propriété de Sagem Sécurité. Ils ne doivent pas être copiés ni communiqués à un tiers sans l'autorisation préalable et écrite de Sagem Sécurité. ».

