Privacy by design ?

The case of biometrics

PrimeLife/IFIP Summer School 2009

Els Kindt, Legal Researcher, K.U. Leuven – ICRI

Introduction

Theme of PrimeLife/IFIP Summer School 2009

'privacy and identity management for emerging internet applications throughout a person's life'

Biometrics : advantages and disadvantages

- Link person - identity in online/offline situations (authentication)
- Risks of abuse (re-use of data for other purposes)
- Risks of theft
- …

Question : Is there a 'safe' way of using biometrics ?

Overview

1. Issues inherent to the use of biometrics in identity management

2. Solution : privacy by design ?
   - definition ?
   - how ?
   - solutions by Turbine

3. Towards best practices

1. Issues inherent to the use of biometrics

Advantages of biometric data

- Enhances authentication means / security
  - E.g., password management, control of restricted access
  - Creates link between real and virtual world
- Ability to verify if holder of document is person to whom document is issued
- Ability to identify individuals
  - E.g., if no other means available
- Convenience

1. Issues inherent to the use of biometrics

Privacy risks for the data subject

- Unique
  - Theft
  - Unique identifier : linking of information
- 'Sensitive' information
  - Health related information
- Re-use
  - E.g., Eurodac
- Permits identification

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics:

many open legal issues

- Biometrics : problems with legal definitions
  - Are biometric data personal data which are subject to the Data Protection Directive 95/46/EC ?

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics :

many open legal issues

- Are biometric data personal data ?

Distinction between ‘images’ and ‘templates’

min_T.txt

33 Minutiae Detected

0 :	18,	84 :	13 :	0.12 :	BIF
1 :	22,	41 :	16 :	0.13 :	RIG
2 :	25,	127 :	26 :	0.28 :	BIF
3 :	27,	67 :	29 :	0.58 :	RIG
4 :	39,	26 :	17 :	0.12 :	RIG
5 :	45,	157 :	25 :	0.12 :	BIF
6 :	52,	40 :	16 :	0.29 :	RIG
7 :	54,	28 :	2 :	0.29 :	RIG
8 :	55,	63 :	29 :	0.30 :	RIG
9 :	61,	80 :	27 :	0.30 :	RIG
10 :	65,	177 :	23 :	0.12 :	BIF
11 :	78,	41 :	14 :	0.13 :	RIG
12 :	80,	73 :	25 :	0.29 :	RIG
13 :	82,	37 :	11 :	0.29 :	BIF
14 :	82,	102 :	23 :	0.29 :	BIF
15 :	83,	65 :	29 :	0.12 :	BIF
16 :	83,	76 :	26 :	0.29 :	BIF
17 :	105,	152 :	21 :	0.62 :	RIG
18 :	107,	25 :	28 :	0.31 :	RIG
19 :	110,	83 :	19 :	0.29 :	RIG
20 :	110,	108 :	20 :	0.29 :	RIG
21 :	113,	41 :	14 :	0.58 :	BIF
22 :	132,	161 :	20 :	0.60 :	BIF
23 :	136,	104 :	18 :	0.59 :	RIG
24 :	145,	168 :	4 :	0.60 :	RIG
25 :	156,	71 :	16 :	0.59 :	BIF
26 :	171,	160 :	19 :	0.57 :	RIG
27 :	173,	184 :	19 :	0.12 :	RIG
28 :	175,	210 :	4 :	0.06 :	RIG
29 :	175,	212 :	4 :	0.06 :	BIF
30 :	214,	98 :	16 :	0.58 :	BIF
31 :	249,	77 :	0 :	0.59 :	BIF
32 :	273,	179 :	1 :	0.06 :	RIG

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics: many open legal issues

- Are biometric data personal data ?

Recital 26 of the Data Protection Directive 95/46/EC :

> '(…) whereas, to determine whether a person is identifiable, account should be taken of **all the means** likely **reasonably to be used** either by the **controller or by any other person** to identify the said person : (…)' (emphasis added)

1. Issues inherent to the use of biometrics

"measures of biometric identification or their digital translation in a template form in most cases are personal data"

Art. 29 WP Working document on biometrics, adopted 1 August 2003

But :

Exception : in case templates would be stored in such a way that (1) *no reasonable means* can be used by (2) the controller or (3) by any other person to identify the data subject

Different implementation and interpretation in the Member States, e.g., United Kingdom

Local storage on card : could be considered as 'private use' ?

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics : many open legal issues

- Biometrics : problems with legal definitions
  - Are biometric data sensitive data ?
  - Which personal data are biometric data ?
    - e.g., digital picture ?

      cfr. France, the Netherlands
  - Quid ‘protected templates’ ?

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics: many open legal issues

- May biometric data be centrally stored ?
- Which human characteristics shall be used ?
- What security measures shall be applied ?
- …

Few national laws of EU Member States explicitly regulate the use of biometrics

Exceptions : E.g., France : Modification of 6 August 2004 of Law N°78/17 of 6.01.1978
but : limited

1. Issues inherent to the use of biometrics

EU Legal & Regulatory Framework for Biometrics
Preliminary conclusion :

(1) Biometric applications process (in most cases) personal data
- Inherent to biometric applications : used to identify/authenticate the identity of a person
- Confirmed in opinion Art. 29 WP on personal data 2007

(2) Data Protection Directive 95/46/EC (national laws) will apply
- To processing by companies in EU, or
- If equipment is used on territory of EU Member States
  - Except for transit only

(3) Fundamental Right to privacy involved (art. 8 ECHR)

2. Solution : privacy by design ?

Concept of 'Privacy by design'

- Ontario's Privacy Commissioner, Dr. Ann Cavoukian, back in the 90's
- Stresses concept as an organizations default's way of operating
  - Privacy is embedded in the design
  - Visibility and transparency
  - Respect for user privacy
- Objectives : ensuring privacy and personal *control* over one's information
- See http://www.privacybydesign.ca/

2. Solution : privacy by design ?

Concept of 'Privacy by design'

– **Dutch Data Protection Authority stresses**

- Protection of personal data
- Review of need of identification versus anonymity (e.g. of clients)
- 'Less is more' concept
- Control of access

See http://www.cbpweb.nl/themadossiers/th_pbd_pet.shtml

– **PETs ?** (Borking)

- Tools for realisation of privacy by design (more narrow)
- Dutch Ministery of the Interior : 'PETs. Whitepaper for decision makers'
- See COM/2007/0228final : 'breaches of data protection technically more difficult'; 'eliminating/reducing personal data'

2. Solution : privacy by design ?
What does it mean for biometrics ?

Risks

- Unique
  - Theft
  - Unique identifier : linking of information
- ‘Sensitive’ information
  - Health related information
- Re-use
  - E.g., Eurodac
- Permits identification

Objectives

- Context dependent use of biometrics
  - revocability
  - Transformation and pseudonymity
- Excluding use of ‘sensitive’ data and irreversibility
- Linking use to specific service context and pseudonymity
- Local storage and verification functionality

2. Solution : privacy by design ?

Objectives	Turbine design : use of protected templates

• Context dependent use of biometrics
  • revocability
  • Transformation and pseudonimity
	• Very limited biometric data (Auxiliary data (AD)) is used
	  • for issuance of multiple pseudo-identities (PIs) (**diversification**)
	  • for **renewable** templates which can be revoked

• Excluding use of ‘sensitive’ data and irreversibility	• ‘raw’ data and templates : deleted after extraction and PIs nor AD can be reversed to such data

2. Solution : privacy by design ?

Objectives	**Turbine design : use of protected templates**
• Pseudonimity and preventing database crossmatching	• Independent Pseudonyms (PIs) are linked to specific service provider
• Local storage and verification functionality	• Storage of PIs and ADs seperately and on token

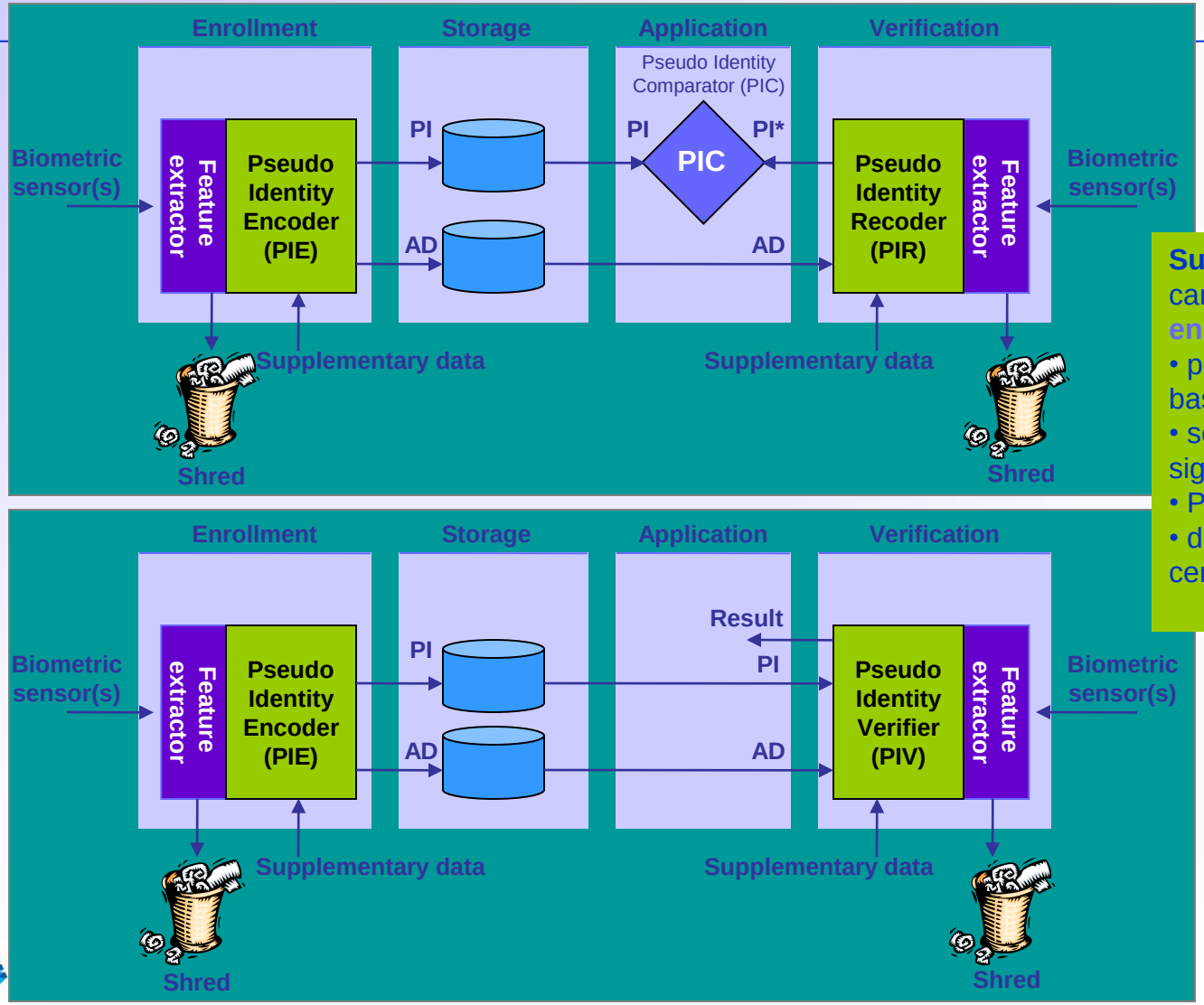
SEVENTH FRAMEWORK PROGRAMME

KATHOLIEKE UNIVERSITEIT LEUVEN

icri

2. Solution : privacy by design ?

Architectures for Pseudo identity management



Supplementary data (SD) can be used for **security enhancement** by :

- possession or knowledge-based secrets
- service specific secrets or signatures
- PI validity data
- digital signature or certification of data

Storage and computations can be local (token, sensor), central (server, database) or shared

SEVENTH FRAMEWORK PROGRAMME

2. Solution : privacy by design ?

Proposed 'Privacy by design' for biometrics and existing data protection regulation

Turbine design

- issuance of multiple pseudo-identities (PIs) (**diversification**)
- **renewable** templates which can be revoked
- 'raw' data and templates : deleted after extraction and PIs nor AD can be reversed to such data

- Data minimisation (Directive 95/46/EC)
- Risks of theft (Working document on biometrics of article 29 Working Party (1 August 2003))
- Prohibition of processing of sensitive data (Directive 95/46/EC)

2. Solution : privacy by design ?

Proposed ‘Privacy by design’ for biometrics and existing data protection regulation

Turbine design

- Independent Pseudonyms (PIs) are linked to specific service provider
- Storage of PIs and ADs seperately and on token

- Risks of unique identifiers and cross linking (Working document on biometrics of article 29 Working Party (1 August 2003)) and specification of purpose principle (Directive 95/46/EC)
- Purpose limitation but no specific storage requirements (Directive 95/46/EC)

2. Solution : privacy by design ?

Comparison with PrimeLife objectives ?

- Use of multiple pseudonyms which are unlinkable (data minimisation)
- User control and consent
- Transparancy for the data subsubject

Leenes, R., Schallaböck, J. & Hansen, M., *Prime white paper,* v.3.0, May 2008, 19 p.

2. Solution : privacy by design ?

But :

Only partial technical measures which improve protection against privacy risks

Does not replace :

- all *technical* measures which may be (legally) required and appropriate e.g., access control
- all appropriate *organizational* measures e.g., confidentiality clauses, education, …
- alternative means e.g., right to appeal at no cost
- appropriate legal regulation e.g., no covert collection, …

2. Solution : privacy by design ?

and : unsolved : including

- Technical safeguards against remote and unobserved collection and use if reference biometric data (e.g., fingerprint and/or face) are stored centrally
  - Need for regulation ?
- Deployment in environments with multilateral security (who is in control) lacking user control (e.g., use of EU passports in the U.S.)
- Typical error rates (FAR, FRR, …)

KATHOLIEKE UNIVERSITEIT LEUVEN

icri

SEVENTH FRAMEWORK PROGRAMME

3. Towards best practices

Albrecht, A., *BioVision. Privacy Best Practices in Deployment of Biometric systems,* August 2003, 49 p.

List of best practices

- organizational
- legal compliance
- some technical means

Should be updated

3. Towards best practices

See also

European Privacy and Data Protection Commissioners

Encourage the development and improvement of comprehensive data protection legislation

That (…) encourage organisations to adopt best practices, including privacy by design; (…)

Declaration on leadership and the future of data protection in Europe, Edinburgh, 23-24 April 2009

3. Towards best practices

Suggested Best Practices for use of biometrics in private sector

- No storage of 'raw images' (deletion)
  - cfr Opinions of DPAs ; findings of study 'Biometrics as a PET' in the Netherlands
- Decentralisation
- Use of verification function only
  - Prohibition to use central databases ? Exceptions ?
- Distinct use in private and public sector
- Transparancy to the data subject
- Specific security measures
  - limited access, encryption, deletion policy, …

3. Towards best practices

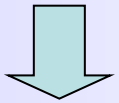
And :

- ‘Anonymous use’ and/or use of various ‘identities’ (pID) (pseudonyms) where possible
- Use of irreversible templates
- Unlinkability of templates
- Revocability
- Considerable degree of control by the data subject
- …

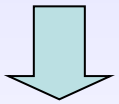
3. Towards best practices

Especially biometric data processing

Insufficient/inadequate legislation



privacy enhancing technologies / best practices



Need to impose PETs /best practices by regulation ?

3. Towards best practices

See also Art. 27 Directive 95/46/EC

'(….) encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions (…) taking account of the specific features of the various sectors'

- Directed towards trade associations/bodies representing categories of controllers
- National level
- Community code

Conclusion

Theme of PrimeLife/IFIP Summer School 2009

‘privacy and identity management for emerging internet applications throughout a person's life’ ?

Especially biometric data processing requires

‘Privacy by design’

Conclusion

‘Privacy by design’

Providing revocable biometric identifiers,
unlinkable and irreversible and under the control of the data subject

Conclusion

Especially biometric data processing requires
'Privacy by design'

goes 'hand in hand' with

appropriate organisational measures, legal compliance and adequate legal regulation of biometrics

Bibliography (selection only)

Albrecht, A., *BioVision. Privacy Best Practices in Deployment of Biometric systems,* August 2003, 49 p.

Cavoukian, A. & Stoianov, A., *Biometric encryption : A Positive-Sum Technology that achieves strong authentication, security and privacy*, March 2007, 48 p.

De Hert, P. & Sprokkereef, A., *The Use of Privacy Enhancing Aspects of Biometrics. Biometrics as a PET (privacy enhancing technology) in the Dutch private and semi-public domain,* January 2009, 50 p.

European Commission, *Communication on Promoting Data Protection by Privacy Enhancing Technologies (TETs),* COM/2007/0228final

European Privacy and Data Protection Commissioners, *Declaration on leadership and the future of data protection in Europe,* Edinburgh, 23-24 April 2009, 1p.

Leenes, R., Schallaböck, J. & Hansen, M., *Prime white paper,* v.3.0, May 2008, 19 p.

Müller, L. and Kindt, E. (eds.), *D3.14 Model implementation for a user controlled biometric authentication*, Frankfurt, Fidis, August 2009, 57 p.