Project no. ICT-2007-216339

TURBINE

TrUsted Revocable Biometric IdeNtitiEs

Grant agreement for: Large-scale integrating project (IP)

Theme 3: ICT - Information and Communication Technologies Secure, dependable and trusted infrastructures

Practical Guidelines for the privacy friendly processing of biometric data for identity verification

Due date of deliverable: M30

Actual submission date: M30

Publication date:

Start date of project: 1 February 2008 Duration: 36 months

Name of lead contractor for this deliverable: K.U.Leuven – ICRI-IBBT – Els Kindt

Name of reviewers for this deliverable: Ileana Buhan (PRE)

Abstract: The present document contains practical and comprehensive recommendations as 'best practice' for the processing of fingerprint (and of biometric data in general) for identity verification in identity management systems in the private sector which should enhance the privacy and the data protection rights of the data subjects. They are not intended to give a (mere) overview of Directive 95/46/EC compliance requirements.

Revision Final R2.3.

Project co-funded by the European Commission within theSeventh Framework Programme (FP7/2007-2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Table of Contents

Glossary

Abbreviation / acronym / term	**Description**
Art. 29 Working Party	Art. 29 Data Protection Working Party
BWG	Biometric Working Group (U.K.)
CBPL	Belgian DPA (‘*Commissie voor de Bescherming van de Persoonlijke Levenssfeer’)*
CNIL	French DPA (‘Commission Nationale de l’informatique et des libertés’)
Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (see Art. 2(d) of Directive 95/46/EC)
Data subject	An identified or identifiable natural person. An identifiable person is an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (see Art. 2(a) of Directive 95/46/EC)
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23.11.1995
DPA	Data Protection Authority
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
FRR	False rejection rate
FAR	False acceptance rate
IdM systems	Identity Management systems
JRC	Joint Research Centre
Processor	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (definition Art. 2(e) of Directive 95/46/EC)
Pseudonym	A pseudonym is an identifier of a data subject other than the data subject’s civil identity (see PRIME White paper v.3.0)

1. Executive Summary

The present document aims at formulating *practical* guidelines for the design, the development and the implementation of biometric identity management systems in the private sector. They should induce the discussion on the adoption of best practices for the privacy friendly processing of biometric data in the private sector, in addition to data protection compliance.

In the past, there have been initiatives promulgating best practices for biometrics, such as the Privacy Best Practices in Deployment of Biometric Systems of 2003 in the BioVision project. These proposed best practices however need to be reviewed in the light of the opinions of the Data Protection Authorities (DPAs) and the advancements of the biometric techniques. Such privacy-enhancing techniques have also been designed, developed and tested in TURBINE in relation with fingerprint.

The proposed best practices are based on the *opinions* of the DPAs and these *new techniques* as tested and implemented in TURBINE. The guidelines do not focus on fingerprint alone but are drafted in such way that they are valid for the processing of biometric data in general. The recommended practices aim in the first place to counter or to limit as much as possible the most serious risks which relate to the special nature of biometric data in general and address the functionality, the design and the implementation of biometric identity management systems.

These guidelines are not intended to give a (mere) overview of Directive 95/46/EC compliance requirements, for which we refer to other initiatives, and do not provide or replace a legal compliance review.

These best practices however may contain elements which can be used for recommending *best available techniques* and for the elaboration of a *code of conduct* of a particular sector for data protection compliance when deploying biometric identity management systems.

2. Introduction

'New technologies evolve today at a frantic rhythm and in a borderless world. Our legal framework and our practices need to adapt to these deep transformations, while keeping at the same time a high level of data protection'.[1]

This deliverable aims at formulating *practical* guidelines which are useful for the design, the development and the implementation of biometric identity management systems. The present guidelines aim to protect the rights and privacy interests of the data subject while at the same time ensuring for the data controller enhanced security by the use of biometric data of the data subjects.

The guidelines are primarily based upon the study of the recommendations of various data protection authorities in *opinions and decisions* issued over the last years in relation with the processing of biometric data. They also take the *privacy-enhancing technical developments* in relation with the use of biometric technologies into account. Some of these technologies have been further researched, tested and implemented in TURBINE.

The guidelines further rely upon various studies and reports in relation with privacy and security of biometric systems of the last five years, including on projects on privacy compliance and certification.[2] Last, but not least, some experiences and developments with regard to existing (often large scale) biometric systems implemented on EU level have inspired the formulation of the present guidelines on how biometric systems should (not) be used.

In this way, the guidelines should reflect the present concerns relating to the use of biometric identity systems, hereby combining mere recommendations for *data protection compliance* with suggestions for *future directions in the use* (and regulation) of biometric systems. It implies that the guidelines for best practices may require more than what is presently required under the existing legal framework of the Directive 95/46/EC.

The present guidelines developed in TURBINE have been presented in the research community[3] and discussed with the Advisory Board of TURBINE**.** They will also be implemented as much as possible in the demonstrators of the project.

It shall be noted at the same time that the suggested best practices do not replace the privacy and data protection compliance measures which remain applicable and required according to national legislations. Best practices are more a way of self-regulation and do not replace the need of a legal review of the implementation of a given system. The present document may contain elements which can be used for recommending best available technologies and for the elaboration of a *code of conduct* of a particular sector for data protection compliance when deploying biometric identity management systems. It may also inspire the legislator.

To conclude, we can say that guidelines should as principles be comprehensible for everyone, developer, controller or data subject. They are therefore formulated as general recommended practices, without containing all details or arguments on which the guidelines are based. This document may however presume from the reader some pre-existing knowledge on the functioning of biometric system and on the privacy and data protection legal framework.

---

[1] A. Türk, *Declaration for the European personal data protection day*, 28 January 2010, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_28_01_10_en.pdf

[2] Some of the relevant recommendations, reports and publications which were used, may be referenced in this document without however being exhaustive.

[3] See E. Kindt, 'The use of privacy enhancing technologies for biometric systems analysed from a legal perspective', in M. Bezzi et al. (eds.), *Privacy and Identity*, IFIP International Federation for Information Processing AICT 320, 2010, pp. 134—145.

3. Recommendations for Best Practices

3.1 General introduction into the proposed TURBINE Best Practices

3.1.1 Objectives and Methodology

The recommended TURBINE Best Practices ('TURBINE Best Practices' or 'Best Practices') address the use of biometric data in the specific context of identity management systems ('IdM' systems). The aim of the Best Practices is to formulate guidelines to reconciliate as much as possible the use of biometric characteristics of individuals in IdM systems with their fundamental rights to respect for privacy and data protection. In biometric IdM systems, biometric data are used for enhanced authentication of the individuals who attempt to access a system or a designated area (security purposes). The biometric data are deployed to verify whether the person who is presenting him or herself is enrolled and is *actually* the person who he or she claims to be.[4] The scenario's in which such verification is meaningful, are plenty. Typical examples are physical and online access control systems which restrict access to *authorized* individuals only, for example officials of the government, specific personnel members of a company, members of a liberal profession (e.g., physicians), citizens intending to access their personal file with the government, travellers crossing borders, etc.

The use of biometric data, however, involves many privacy risks for the data subjects involved.[5] For this reason, the use of biometric data may not be proportional with the benefits sought by the data controller. If the privacy risks however can be mitigated to some extent, this will have a positive effect on the evaluation of the proportionality of the use of biometric data in an identity management system. The Best Practices in fact suggest methods for the processing of biometric data and the use of technologies which exclude or at least mitigate some important privacy risks which have been identified. The TURBINE Best Practices do not purport to be a comprehensive set of guidelines to be a substitute for law or to summarize the laws that may apply. Other initiatives have been taken in this respect, not at least by the Article 29 Data Protection Working Party, the EDPS and the national data protection authorities, and by the consultative committee of the Council of Europe. They point to the difficulties in the interpretation of the applicable data protection legislation and various compliance issues. We refer to these and other initiatives explicitly, and have built further on this work.

The methodology used for establishing these Best Practices was as follows. As already explained, previous recommendations and initiatives on the formulation of best practices in relation with biometric data processing have been reviewed. Several opinions of *data protection authorities* in relation with the processing of biometric data have been studied.[6] It was considered that there was no further need to question these authorities[7], as their opinion on the use of biometric data has in the meantime been set out in various documents issued by them. Legal systems, where (often

[4] Other means for such verification may exist. The use of biometric data, however, offers in addition to what some may know or have, a third factor for authentication.

[5] For a discussion of these privacy risks, we refer, e.g., to Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, 11 p. The opinions of the EDPS on large-scale biometric systems, such as VIS and SIS II, also discuss these risks.

[6] The opinions and advices of data protection authorities which were studied include those of the EDPS and of the data protection authorities of Belgium, Canada, France, Greece and the Netherlands.

[7] This method has, for example, been used during the preparation of the best practices formulated in 2003 in the project BioVision, further referenced below.

minor) adaptations have been made to regulate biometric systems, were also taken into account. The very limited case law on the subject had only limited influence. The drafting of the presently suggested Best Practices has last but not least also been inspired by various recent *studies and reports* in relation with the privacy and the security of biometric systems.[8]

The proposed TURBINE Best Practices will contain a brief motivation for the suggested guidelines. A full analysis of the legal or technical aspects of the use of biometric characteristics, however, is not contained in this document. The expected effect will also be described.

Last, but not least, the notions of 'privacy' and of 'security' which are repeatedly used in the present document, refer to the concepts as generally understood in the context of biometric technologies and human rights without pointing to any specific (technical) definitions.

3.1.2 Comparison with previous initiatives

The TURBINE Best Practices build further on previously issued recommendations for the processing of biometric data[9] and will in most cases not contradict these earlier assessments and guidelines. For example, the use of biometric data for identification purposes has been mentioned already for some time as involving major privacy risks.[10] Another illustration is that of the recommendation to avoid the central storage of biometric data in most cases. The present Best Practices, however, attempt to go one step further and formulate *strategies for which the controller can choose* in order to address various 'unsolved' issues relating to biometric data processing (for example, in relation to required transparency). The Best Practices hereby formulate practical recommendations for the set up and the implementation of a biometric IdM system. As already stated, these are mainly based on the recommendations of various *data protection authorities* in their opinions and advices over the last years and which we have collected and analyzed. In addition, because of the further development of technical means, the use of privacy-enhancing techniques is recommended as well and will also be included in the Best Practices. The identification of legal, technological and organisational criteria in the presently suggested practices make hence also some suggestions for Best Available Techniques which can contribute to data protection regulation.

The TURBINE Best Practices will hence not just give a new overview on how the legal requirements, in particular the requirements resulting from the Directive 95/46/EC, could be interpreted and implemented. Such overview has been given by the Article 29 Data Protection Working Party in its *Working Document on Biometrics* of 1 August 2003. This Working Document is still valuable as it has identified therein the risks while suggesting some methods which could provide (partial) solutions. A useful discussion on the application of the principles of this Directive upon the processing of biometric data and data protection compliance has also been given in various other reports, such as in the Privacy Best Practices document of *BioVision of 2003* and the Progress report of the Council of Europe of 2005.[11] In contrast with those previous and highly relevant attempts to outline the difficulties in the interpretation and the compliance issues upon the processing of biometric data, the present Best Practices clearly aim to advance some very specific suggestions as to how biometric data can be deployed in IdM systems in a privacy preserving way.

---

[8] These reports also include the deliverables of the FIDIS project on various aspects of biometric systems, in particular D3.2, D3.6, D3.10, D3.14 and D13.4, which are available at www.fidis.net

[9] We refer in particular to the best practices formulated in the BioVision project : Albrecht, A., *BioVision. Privacy Best Practices in Deployment of Biometric Systems,* BioVision, 28 August 2003, 49 p.

[10] See, for example, in 2001, by the International Biometric Group, The BioPrivacy Application Impact Framework, 2001, available at http://www.bioprivacy.org/bioprivacy_main.htm

[11] Consultative Committee of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data [CETS No. 108] (T-PD), *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, Council of Europe, CM(2005)43, March 2005, 22 p.

They will also take recommendations and outcomes of other European projects and reports into account, such as, for example, the requirements for identity management set forth in PrimeLife[12], EuroPrise and the report on 'Technology-induced challenges in Privacy & Data Protection in Europe' of the ENISA working Group on Privacy & Technology of 2008.[13] Special attention has been given to the Biometrics Institute Privacy Code of 19 July 2006 as well. This Code has been approved by the Australian Privacy Commissioner as best practice for the processing of biometric data.[14]

The TURBINE Best Practices finally differ with other initiatives on the formulation of codes of conduct and best practices in privacy and data processing in general[15], as the focus is clearly on specific issues with which the controllers and processors have to cope upon the processing of biometric data in IdM systems. These Best Practices will hereby not contain a full list of all general legal compliance requirements for the processing of biometric data.[16] This approach to limit the content of Best Practices has been chosen deliberately, in order to allow to have a focused discussion on those best practices and principles which are specifically required for the processing of biometric data.

Once these Best Practices would have obtained general approval and acceptance, it is clear that they will have to be regularly reviewed and updated.

3.1.3 Structure

The Best Practices outlined below are structured along the various phases in the decision to implement a biometric IdM system: the specification of the controller's need (and the definition of the purposes), followed by the design, the enrolment and the actual deployment of the system. The decisions relating to each of these phases will be taken by the identity provider and/or the service provider. In some cases, the identity provider and the service provider may be one and the same entity.

The specification of the needs that a biometric IdM system has to fulfil is probably the most important decision. Available technologies or systems should not make that decision. Instead, the controller of a biometric IdM system shall clearly define the purposes of the system. At that moment, the controller shall also determine the functionality to be used in the system. We herein plead for a clear guideline to use the biometric characteristics in the biometric system for verification purposes only, as will be set out below.

For the design and architecture, important decisions will have to be made again. In order to minimise privacy and data protection issues, criteria should be adopted. The guidelines below

---

[12] Prime, *Prime White paper*, 2008, v.3.0, p. 11, available at https://www.prime-roject.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf. PrimeLife for example stresses data minimisation, the importance of pseudonyms, and the use of anonymous credentials and transparency for the data subject.

[13] ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-Induced challenges in Privacy & Data Protection in Europe*, M. Langheinrich and M. Roussopoulos (eds.), October 2008, 48 p. available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf The report stresses for example the definition of 'best available techniques' for specific technologies and the use of certification.

[14] Biometrics Institute, *Biometrics Institute Privacy Code*, 19 July 2006 ('Biometrics Institute Privacy Code') , available at http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8 This Code contains principles which are substantially the same as those set out in the Privacy Act, and some supplementary principles specific for biometric data processing.

[15] See e.g., EuroPrise. For a comprehensive overview of other initiatives on the formulation of codes of conduct and best practices in privacy and data processing in general (sometimes also including ecommerce), see Initiative for Initiative on Privacy Standardization in Europe (IPSE), *Initiative on Privacy Standardization in Europe*, Final report, CEN/ISSS, 13 February 2002, pp. 72 – 75, available at http://www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/ipsefinalreportweb version.pdf

[16] Such requirements include, for example, the involvement of the employee representative organisations in some countries. See and compare, however, with the Biometrics Institute Privacy Code.

require that the user has control over the use of his biometric characteristics. This concept is a rather complex notion, which has various elements, and includes enhanced transparency which is also needed during the deployment of the system. Furthermore, best available technologies at the design phase can contribute to strengthen privacy and security. The decision to use techniques for the creation and use of multiple identities in combination with pseudonyms based on the same biometric characteristics considerably limit the risks of the use of the biometric characteristics as unique identifiers and re-use of the personal data. These technologies also allow the revocation in case of misuse or theft or in case of termination of the access to the services.

Biometric systems which attempt to increase security will in most cases involve an enrolment phase. Specific guidelines which address this phase are needed as well.

The operation itself of the biometric system will also require attention. Specific guidelines relate to the use of privacy enhancing technologies which make the identities unlinkable and irreversible. Anonymous verification procedures are hereby recommended as well. The data subject shall also be sufficiently informed of the biometric process. Last, but not least, the controller(s) shall specify a fall back and appeal procedure.

During all these three steps, organization and security measures need to be specified and implemented.

Certification could also contribute to the privacy friendly development of biometric systems. Schemes which address each of the suggested Best Practices could be developed and applied.

We are aware that some of the recommended Best Practices could be mentioned in more than one phase of a biometric system. In that case, a choice has been made to discuss the recommendations under either Design and Architecture, Enrolment or Deployment, which does not exclude however that the recommendations could be discussed as part of another step.

Finally, it was aimed to present the recommendations in a concise way. This should allow stakeholders to keep at all times an overview of the various actions needed. A visual overview of the structure and subject of the Best Practices discussed is shown in figure 1 below.

<table>
<tr><td colspan="3">Functionality of the biometric IdM system
Use of verification mode only</td></tr>
<tr><td>Design and Architecture
1. User control
2. Multiple identities en pseudonyms
3. Revocation and re-issuance</td><td>Enrolment
1. Credential/Identity check
2. Deletion of samples and original templates</td><td>Deployment
1. Use of privacy enhancing technologies
2. Transparency and additional information
3. Fall back procedure and appeal</td></tr>
<tr><td colspan="3">Organization, Security & Certification</td></tr>
</table>

Figure 1: Overview of the suggested TURBINE Best Practices for a biometric IdM system

3.1.4 Scope and nature

The present Best Practices are mainly aimed as guidelines for designers and controllers deploying biometric IdM systems in the *private* sector.[17] They are fit for many use cases of biometric IdM systems. The terms uses are as much as possible in conformity with the biometric vocabulary proposed in ISO/IEC JTC SC 37 and have the meaning set forth therein.[18]

The Best Practices do not address the use of biometric data to be stored in (large) databases or identity management systems used for *inter alia* a so-called 'double enrolment check' or 'negative identification' (comparison with database(s) in order to check whether a particular person is on the list or not). Such IdM systems, which are in most cases operated by government or public authorities, require a specific approach and will be legitimated in most cases by specific legislation.[19] Having said so, it does not mean that some of the methods, practices or technology discussed herein could not be recommended for limiting privacy risks in such identification systems.[20] The architecture and the design of both systems, however, differ, and they should be treated distinctly.

At the same time, these guidelines for IdM systems remain valid for controllers in the public sector, where they, for example, would use biometric methods for access control purposes of their employees.

Based on a study of the legal aspects of biometrics in the TURBINE project[21] and a general understanding of recent privacy-enhancing technological developments, the recommendations for best practices for the enhancement of privacy and data protection in the deployment of biometric systems for identity management purposes are described below.

[17] While there may be some overlap from time to time between public and the private sector (e.g., when private entities perform tasks of public security at border control), the focus is on the intended use of the biometric system (for example, securing access to company premises). If the use is not for the execution of a specific public interest or for public safety, the use of the biometric system is considered to be in the private sector.

[18] See for one of the latest versions, see ISO/IEC JTC 1/SC 37, Standing Document 2 – Harmonized Biometric Vocabulary, version 12, N 3385, New York, ANSI, 16 September 2009, working draft text, 203 p.

[19] See, for example, legislation relating to the national central storage of the biometric data collected for the biometric ePassports.

[20] Other risks and concerns, however, are attached to the deployment of biometric data for identification purposes. Because the biometric data will in such case be stored in data bases, issues as legal basis for identification and unauthorized access and risks of re-use, especially for third pillar purposes, will be among the concerns that need to be addressed by regulation. Best practices can in our view not be used, because of the legal restrictions relating to identification (see below) and relating to the re-use of data (See, in particular, Art. 6.1.(b) Directive 95/46/EC 95/46/EC).

[21] On the legal aspects of biometrics, we refer *inter alia* to Turbine deliverable 1.1.1 and Turbine deliverable 1.4.2 and the references therein cited, which contains several arguments for specific guidelines set out in the present Best Practices.

3.2 Best Practice N°1: Biometric data shall in pri nciple only be used for verification and stored locally

It is generally accepted that biometric data can be used in two ways: the data can be used to compare with specific biometric data previously stored (1:1) *to verify whether the person is the same* or the data can be used in combination of a database of biometric data (1:n) to identify that person. The verification functionality based upon the biometric data offers increased and sufficient security for the data controller, e.g., an employer, aiming at ensuring that the person, who has been previously been registered and enrolled in the system is actually that person and is authorized to enter, because of the use of the biometric data. Biometric data allow to tie a person and his or her presence to a particular access procedure by requiring the submission of the biometric characteristic, such as in combination with the use of a badge or token or of particular documents. It is hereby not required that this person is identified based on the biometric data.

The presently suggested Best Practices are built upon the general underlying recommendation – in our view of crucial importance for the protection of the fundamental rights - that biometric data in an IdM system for use in the private sector shall as a matter of principle only be used in a *verification* mode. This may seem contradictory in view of the use of biometric data in 'identity' management system, but it is not. The identification of a given person is in principle not required for enhancing the security by the use of unique biometric characteristics in an IdM system. It is for example recommended to use 'anonymous' verification where possible, whereby the identity or pseudonym details associated with the biometric data of the individuals concerned are even not revealed during the processing (see *below*).

The choice for use of the verification functionality shall be further completed with the clear determination of the specific purpose(s) for which the biometric data will be processed. The biometric functionality used shall also be made transparent for the data subjects.

Motivation

The use of the verification functionality in a00 biometric IdM system permits to enhance the security. Identification, which is sometimes regarded as less cumbersome for the data subject (no token is required), is for security purposes of an access system in principle not required and therefore from a privacy point of view *excessive*. The security is for most IdM systems guaranteed if the (verification) comparison can confirm that the person is enrolled. Only in exceptional cases, and upon duly motivation, identification could be required.[22] Besides such very specific cases, the use of the identification functionality is in general not proportional with the purposes and the interests of the identity and service provider controllers of IdM systems. Furthermore, identification implies and requires the storage of biometric data in a database. Precisely this database allows to use the identification functionality. The *storage of the biometric data in a central place* which permits identification and over which the data subject may have no further control, will for these reasons equally be regarded as excessive and *not proportional*.[23] Eliminating the central storage of biometric data will also eliminate the use of the identification functionality. The choice as to whether the verification over the identification functionality has to be used, however, is more than a proportionality issue, whereby interests are balanced. Identification also requires an explicit legal basis and the use of the verification functionality is therefore a matter of legality of the processing (see *below*).

The use of the verification functionality also *permits to reduce the error rates*. Systematic and statistical errors of the measurement and the algorithms increase if the comparison is made in the identification mode, whereby the biometric characteristic is to be compared with a database with

[22] See, for example, Eurodac.

[23] See and compare with the decision of the Court of Justice in Huber v Germany, Case C-524/06, 16 December 2008, in which the Court criticizes the central storage of particular personal data.

the measurements of a (high) number of individuals, because of overlapping and scaling problems in the identification mode.[24]

Last but not least, as stated above, identification without an explicit *legal basis* infringes the privacy and data protection rights of the data subjects. Many countries have adopted legislations which specify when citizens are under an obligation to identify themselves or may be identified. Therefore, in many legal systems, identification requires that this is laid down by law (in the broad sense including by regulations and by case law).[25] The use of the identification functionality and the central storage of biometric data is in this case therefore only permitted if there is an appropriate legal basis for the central storage and the identification, the controller can invoke a specific legitimate interest[26] and identification is necessary. This includes in particular that *other methods* which are less infringing on fundamental rights than the use of biometric techniques for identification *do not exist* to attain the same purposes, resulting in the requirement that the biometric identification method shall be *relevant*, and that the biometric identification method shall be *sufficient* (effective). This is for large scale systems still problematic.

It should also be noted that the use of biometric databases for reviewing whether an individual is listed whereby the databases are used as 'black lists' excluding individuals from access rights or practical services, also requires explicit legal provisions authorizing the use of such lists, the more as such lists may imply some form of discrimination.

Since a legal basis is required, the consent of the data subject may not be sufficient for the central storage and the processing of biometric data for identification purposes.[27]

The purpose limitation principle, another core principle of data protection legislation, further motives the choice of the functionality of verification, in combination with a clear determination of the purpose(s) for which the IdM system will be used.

Effect

The use of a biometric IdM system in verification mode and the local storage of the biometric data will not only enhance the accuracy of the performance of the IdM system, they will also enhance data protection compliance as their application will be in accordance with the proportionality principle and the legality principle. By using the verification modality of a biometric IdM system, the biometric data use is minimized and any risk for the privacy and data protection rights of the data subjects will be in better proportion with the security interests of the IdM identity and service providers. Data protection and security enhancement are in this way combined.

While the use of the identification functionality will as a matter of starting point as principle not be allowed or at least not be deemed proportional, the use of this functionality with a limited local database could in exceptional circumstances be considered. These circumstances would be effective privacy guarantees for the data subjects in that (1) the biometric data are securely stored in a tamper free hardware which cannot be accessed by the controller or third parties, such as the police, (2) the biometric data will never leave this hardware, (3) the data can only be deployed when the data subject presents him or herself. In such case, if the identification functionality is used anyway, the *technology used should have the characteristics to provide the evidence* that the data stored in a more central way can not be re-used or accessed by third parties. One could say that the burden would in that case would be on the technology (and the controller who wants to

[24] See, e.g., L. Müller, 'Biometric system errors', in E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 26-36.

[25] See, for example, Belgium and the Netherlands. For France, compare with the requirement of a 'décret' for biometric data processing for the government (Article 27, I, 2° of the Loi n° 78-17 (as modified).

[26] For example, public safety. Other legitimate interests are enumerated in Article 8 of the European Convention on Human Rights. Some jurisdictions may require a more detailed specification of the legitimate interest.

[27] Compare also with decisions of the Greek DPA which considers consent not sufficient.

implement such technology and system) to prove the privacy-preserving aspects, in particular exclusion of re-use and of access, of the alternative way of storage.[28]

3.3 Best Practices for the *design and architecture* of a biometric IdM system

Privacy and data protection issues need to be addressed at the early stage of the design and the setting up of the architecture of the system.[29] In general, the architecture of an IT system will create *possibilities* for the system but will also *restrict* its abilities.

It shall hereby also be noted that discussions about privacy and data protection in the architecture and design of a system refer often to a more technical understanding of privacy. Privacy protecting concepts in an architecture from a more technical point of view and which are crucial include unlinkability, unobservability, anonymity and pseudonymity.[30] Control by the data subject is also important. To the extent an architecture could guarantee these privacy concepts in an IdM system, the privacy of the system will considerably be improved.

3.3.1 Best Practice N°2:User control over biometri c data by default

Privacy and data protection thought of as *the right to decide and to control* personal information is gaining increasing attention and support in various Member States of the Union. Because of the privacy risks upon the collection and the use of biometric data, more control by the data subject over the use of his or her biometric data is of particular importance.

The data subject does not obtain more control if he or she is merely informed of the use of his or her data, even if the data subject would retain the right to consent or not. The data subject may only retain control if he or she *has to cooperate* for the release and/or the use of the biometric data, for example by handing over the identity document, the smartcard or the token on which the biometric reference is stored, after which the comparison process can start.

It is for this reason strongly recommended that the collected biometric data are stored *locally on an object under the control* of the individual. The fact that only the data subject holds the biometric data, increases in addition the transparency over the use of the biometric data.

In exceptional cases, the controller may motive the central storage of the reference biometric data which should then only be used for verification purposes.[31] In that case, the data subject should preferably still be requested to cooperate for the release and use of the reference data, for example by providing a user name with secret code or key, upon which condition only the data may be released for the comparison process.

The control by the data subject further requires that he or she remains fully informed each time when his or her biometric data are used in a processing. Every use would in principle, in case of local storage, become apparent upon the need to request to submit the reference biometric data.

---

[28] See and compare also on such new developments, especially if match-on-card technology is used, European Security Research & Innovation Forum (ESRIF), Final Report, December 2009, p. 183.

[29] See also Legal-IST, Doc. No 11, *Privacy-Identity Management*, 4 November 2005.

[30] See A. Pfitzmann and M. Hansen, Anonymity, *Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology* (Version v.0.31 Febr. 15, 2008), available at http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf

[31] For example, because the central storage would be more convenient for the user ànd the biometric characteristic provided does not allow the use of the identification functionality (e.g., hand geometry). Compare, e.g., with the Unique Authorization n°AU-007 of 27 April 2006 for biometric systems based on hand geometry verification for access control, management of time and attendance and of the canteen in the workplace in France.

Collection and/or use of biometric data without the knowledge of the data subject is not acceptable. In addition, other measures are recommended as set out below.

Control by the data subject, however, *is not limited* to the *physical control* over the object on which the biometric characteristics are stored. Control also requires that there are *tools* for the data subject *to obtain information* about the process in which her or his characteristics are used for identity verification or authorization (output), and *to provide instructions* (input). This requires an appropriate user interface.

Motivation

The concept of user control over personal information is not established in the data protection legislation of most countries as such.[32] Nevertheless, the local storage of biometric data has been suggested for a while by some DPAs.[33] Other DPAs and the Article 29 Working Party are following this position and advise to store biometric data not centrally.[34] This is considered important for the future of privacy and data protection rights.[35]

However, a local storage requirement is not sufficient and additional guarantees for the processing of biometric data locally stored will remain required, for example, that no copies are kept in the enrolment database or that the data cannot be used in different contexts than those originally intended. This could be done by the transformation of the biometric data, whereby the data are linked to particular services for use by the IdM service provider (see *below*).

Effect

The processing of biometric data under the control of the data subject has additional privacy enhancing effects. The need for cooperation by the data subject *prevents* that the biometric data is being *used or re-used* (for other purposes) without the knowledge of the data subject. This is of especial importance because many biometric characteristics (including, for example, iris or vein patterns) can be captured on a distance or on the move without the knowledge of the data subject.

Cooperation by the data subject in combination with the local storage of the biometric reference data, further limits the risks of *attacks* on biometric central databases (for example, for identity theft purposes) and of *unauthorized access* to such data bases.

3.3.2 Best Practice N°3: Multiple identities and pseudonymity

Biometric data could be used in an IdM system as unique identifiers. Because unique identifiers present privacy risks, for example due to the possibility of linking various (trans)actions, sometimes across databases, it is best practice to avoid the use of biometric data as identifier if there is no legal basis for the use of biometric data as identifier. It is therefore recommended for a biometric IdM system to use *multiple* identities and identifiers. The use of multiple biometric identities for one

[32] Presently, the data subjects have information, access and correction rights, and the right to object under specific conditions. They also have the right to freely refuse consent.

[33] See for example, the At Face value report published by the Dutch DPA: R. Hes, T. Hooghiemstra and J. Borking, *At Face Value. On Biometrical Identification and Privacy,* Achtergrond Studies en Verkenningen 15, The Hague, Registratiekamer, September 1999, p. 52 ('At Face Value Report').

[34] For example, the DPAs of Greece and Belgium. See also the French DPA, the CNIL, which has warned since 2000 for the central storage of biometric data, especially fingerprint, and which thereupon developed a position on the use of biometric identifiers which shall in principle not be stored centrally but locally. Compare, however, with CNIL, Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 28 December 2007, 12 p.

[35] Article 29 Data Protection Working Party and the Working Party on Police and Justice, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of privacy*, 1 December 2009, WP 168, p. 14 : 'Biometric identifiers should be stored in devices under control of the data subjects (i.e. smart cards) rather than in external data bases'.

person will imply that privacy enhancing technologies shall be used to transform the original biometric data and to create multiple identities.

There are several aspects relating to the use of multiple identities. First of all, in order to assure the privacy rights of the individuals, the biometric identities shall be made irreversible and unlinkable across contexts. This is to be effectuated by technological means, as set out *below* in Best Practice N° 7. The possibility for a biometric IdM system to create multiple identities will in principle also imply the possibility that an identity may be revoked. This Best Practice N° 4 is discussed *below*. Thirdly, the identifiers for each of the multiple identities for the data subjects should preferably be a pseudonym. The term 'pseudonym' is used in IdM systems in general as a term to explain that not the real, 'civil identity' name is used, but another name or another identifier. Pseudonyms also allow data subjects to choose and to use a different name with each organisation. Pseudonyms allow service providers to create accounts for individual users, while they cannot determine the real identity of the data subjects.

The creation and the use of multiple identities and pseudonyms is a building element of user-controlled or user-centred IdM systems. In a fully user-centric biometric IdM system, there is more than one identity provider and service provider, all operating in the user's interest rather than in their own interest. The data subject would be enabled to select one amongst the various identity provider (for example, based upon the security and privacy policies and practices of a particular provider), while choosing (another) service provider for reasons of the services or goods. Furthermore, the data subject would in principle also be able to use his credentials with various service providers.[36]

Motivation

The Article 29 Working Party has clearly warned for the privacy and data protection risks of identifiers: '*The use of identifiers, whatever form they take, entails data protection risks. Full consideration should be given to all possible alternatives. If user identifiers are indispensable, the possibility of allowing the user to refresh the identifier should be considered'.* Multiple identities and accountability is also a requirement set forth in the Prime White paper for identity management systems in general and the OECD report on 'Personhood' and Digital Identity.

Some data protection legislations explicitly refer to the use of pseudonyms. The German Federal Data Protection Act, for example, states that *use is to be made* of the possibilities *for aliasing* ['*Pseudonymisierung*'] and *rendering persons anonymous*, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection' (stress added). [37] The need for the possibility to connect to a network with a pseudonym has been made explicit by the Article 29 Working Party as well: '*All possible efforts should be made to allow anonymous or pseudonymous use of online authentication systems*'.[38]

Legislation could give data subjects the right to use multiple pseudonymous biometric identities in biometric applications in the private sector, unless expressly forbidden.

Effect

The use of multiple identities based on the same biometric characteristics allows to avoid that the characteristics can be used as unique identifier, for example for linking information across various sources. The use of pseudonyms increases the privacy-enhancing effect. From a general, but also technical point of view, pseudonyms can not only be used for replacing a person's name or identity (person pseudonym), but also for a role (for example, for a role as customer) (role pseudonym) or for a relationship (for example, for the relation with different communication partners) (relationship pseudonym). The use of multiple identities in combination with pseudonymity will enhance the privacy and security to the benefit of the data subjects.

---

[36] OECD, Directorate on Science, Technology and Industry, *At a Crossroads : "Personhood" and Digital Identity in the Information Society,* STI Working Paper 2007/7, 29 February 2008, pp. 44-45, available on http://www.oecd.org/sti/ict/reports

[37] See Section 3 a) German Federal Data Protection Act.

[38] Article 29 Working Party, *Working Document on on-line authentication services*, WP 68, 29 January 2003, p.15., available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf

3.3.3 Best Practice N°4: Revocability of biometric identities and re-issuance

Biometric characteristics of a person are unique and persistent and can in principle not be changed in case of abuse. This given fact has always been one major concern for biometric IdM systems.

New techniques however make it possible to issue various identities based on the same characteristics, which allow to revoke such identities. TURBINE has also developed and tested a mechanism to issue revocable biometric identities. The process of generating multiple independent protected identities from the same biometric characteristics is referred to as 'diversification'.

It is therefore recommended for biometric IdM systems, once the identity provider and the service provider are determined and their roles specified, that biometric identities are issued which are revocable.[39] Furthermore, the IdM scheme should provide for the possibility to re-issue a protected biometric identity, in case a previously issued protected biometric identity would be compromised or lost (possibility to revoke).

The revocation may also prove to be useful in case a biometric identity leads to too many failures, or if the relationship between the data subject and the identity provider is terminated. The revocation could be at the demand of the data subject or of the identity/service provider. A revocation policy shall be agreed upon and contain the specifications of the procedure. The revocation procedure and policy should be fully transparent for the data subject.

Motivation

Identity theft and identity fraud are realistic security threats for IdM systems in general. These threats have even more severe consequences if the impostors make use of the data of the data subject, which the data subject cannot change (such as finger tips, iris, etc).

Various privacy advocates and some DPAs[40] have therefore also pointed to this requirement of revocable biometric identities.

Effect

The use of revocable biometric identities is an important privacy-enhancing aspect of biometric IdM systems. As long as there are no mechanisms[41] used to permit a data subject to revoke a biometric identity, the use of biometric data in an IdM system endangers the rights of data subjects whose characteristics have been (mis)used or stolen. The use of revocable biometric identifiers is essential for protecting the fundamental right to respect for privacy of the individuals upon the use of their unique human characteristics.

If technology enabling the revocation of biometric identifiers is applied, the use of such technology will *influence* to an important degree *the proportionality evaluation* of the use of the biometric data.

[39] This has been researched for some years now and several methods for such 'cancellable biometrics' have been proposed. See, for example, N. Ratha, J. Connell, and R. Bolle, 'Enhancing security and privacy in biometrics-based authentication systems' *IBM systems Journal*, vol. 40, 2001, pp. 614-634.

[40] See, for example, A. Cavoukian, A. Stoianov and F. Carter, 'Biometric Encryption: Technology for Strong Authentication, Security AND Privacy' in E. de Leeuw, Fischer-Hübner, S., Tseng, J., Borking, J. (eds.), *IFIP. Policies and Research in Identity Management*; Boston, Springer, 2008, pp. 57–77.

[41] For example, by the issuance of multiple biometric identifiers.

3.4 Best Practices for the *enrolment* for a biometric IdM system

3.4.1 Best Practice N°5: Credential and/or identi ty check

It is of crucial importance that the control of the credentials or of the identity of the individuals who enrol in biometric IdM systems is thorough and reliable. Such check is especially important in case the biometric identity is used for authenticating the civil identity (e.g., in national biometric ID cards, for issuing biometric passports, travel documents or other identity documents, in welfare schemes). If the wrong person becomes enrolled, all later use of the biometric system is compromised. The security of biometric IdM system is hence only trustworthy as long as the credential or identity check is reliable.

This check is not only important for IdM systems in the public sector[42], but also for biometric IdM systems in the private sector for which the credentials or identity of the individuals before enrolment are important (e.g., biometric payment scheme). Therefore, the *procedure(s)* for such credential check or identification, and in particular *which* documents shall be submitted and the *way* such documents shall be provided (in original, copy, etc), shall be agreed between the identity providers and the service providers and shall be documented. Policies and contractual arrangements should be further in place to ensure that the personnel and agents of the identity provider(s) follow these procedures.

For biometric IdM systems in which the identity is not relevant or necessary, but rather whether an individual is able to submit a credential in combination with a biometric identifier, the *procedure(s)* for linking the biometric identifiers with the credentials (for example, the evidence of age, the belonging to a particular profession, etc) shall be agreed and documented.

Motivation

A biometric IdM system which provides security at a given point is just a link in a security chain. Credentials or identity documents to be provided at enrolment are often less secured and therefore more likely to be subject to forgery and counterfeiting. Some clear agreements and procedures on these elements are therefore strongly advised in order to ensure the security aimed at with a biometric IdM system. The EDPS and some DPAs have pointed to this issue.

Effect

Biometric systems, which may involve risks for the rights of the data subjects, can only be effective if the procedure for enrolment has been carefully 'designed'. Without appropriate procedures for the credential or identity checks to be made, the biometric system will not be effective and should not be implemented.

3.4.2 Best Practice N°6 : Deletion of the samples and of the original templates

The conditions under which the local storage of biometric data enhances the privacy and data protection compliance of biometric applications include that (i) the original image of the biometric characteristic, (ii) all the forms of the image in between the extraction steps and (iii) the unprotected template shall not be stored but *always deleted* after the extraction process for enrolment or

[42] See, e.g., for the importance of this aspect for the issuance of biometric passports, EDPS, *Opinion of 26 March 2008 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004*, *O.J.* C 200, 6.08. 2008.

comparison. This should not only happen on the local device level (such as, e.g., on the biometric scanner or sensor) but also *from all other components* of the biometric system.

The data subject could also be informed of this deletion (see also Best Practice N°8).

The protected templates should also be deleted if there is no need anymore for processing thereof in compliance with existing data protection requirements.[43]

In case no protected templates would be used (see *below*), it is clear that at least the samples and all the forms of the image in between the extraction steps shall be deleted and that the local storage of the biometric template data is of crucial importance.

Motivation

EDPS and DPAs require in general that the controllers shall have a policy about the deletion of personal data after the processing. The term for which the data are kept is also often requested in notification forms. Such deletion strategy is even more important for biometric data processing.

Only if the original images and templates, captured during the biometric process, are deleted, the possible misuse of the image or template, such as the use of possible sensitive information contained in the image or template or the use of the biometric data as a unique identifier can be prevented.

Deletion of the data also prevents that they would be stored in a database, which permits to use the identification functionality.

The deletion of the biometric data which is not needed for the processing is also required according to the data minimisation principle.

Effect

The deletion of the biometric data which are not needed enhances the privacy preserving effect in that the data can no longer be used for other purposes, including the use of additional information contained in the biometric data.

[43] See and compare, e.g., Biometrics Institute Privacy Code, 2006, section F.11.4.

3.5 Best Practices for the *deployment* of a biometric IdM system

3.5.1 Best Practice N°7: The use of privacy-enhanc ing technologies

Transformation of the original biometric data

Because of the various risks of the use of biometric samples and of templates (e.g., the possibility that they contain information about the data subject's health[44]) it is best practice to transform the original biometric data (both biometric samples ànd the template) and to destroy the biometric samples ànd templates afterwards.

The transformation of the original data should render it possible to delete the original biometric data after the creation of identifiers. This should be done during enrolment, and thereafter, for every later comparison process.

The transformed information however will still refer to an identity of a given person - which is after all the goal of the use of the biometric IdM system - and the transformed information will hence still function as identifiers. For this reason, it is important that additional privacy-enhancing technologies are implemented in order to render these identifiers irreversible and unlinkable.

Unlinkable biometric identities

It is best practice that the digital representations of the biometric characteristics are processed with mathematical manipulations (encryption, etc.) *with different parameters for every biometric product, system or service* and *specific techniques* which guarantee low mutual information between templates derived from equal or very similar biometric data. This should avoid the combination of personal data of data subjects through the comparison of templates across databases and applications. The unlinkability also prevents that databases would be searched. These manipulations have as a result that the use of biometric data is limited to a specified context (context-specific use).[45]

Irreversible biometric identities

Captured biometric characteristics may include more information than what is needed for the comparison. Especially the biometric samples (previously referred to as the 'raw biometric data') may contain information which reveals racial or ethnic origin or data concerning health. The further processing of the data, especially of the biometric templates, limit the chances that such additional information is still contained therein. The transformation of the captured and processed information is therefore advised in transformed templates This requires however than it is not possible to reverse engineer the samples and the original templates from the transformed templates.

[44] M. Meints & M. Hansen, 'Additional and in some cases health related information in biometrics', in E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 83-86.

[45] See and compare also with the conclusions and recommendations of the Committee of experts on data protection (CJ-DP), *The introduction and use of personal identification numbers : the data protection issues*, Council of Europe, 1991, pp. 15-17, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Pins_1991_en.pdf

The use of the fore-mentioned kinds of privacy-enhancing techniques is sometimes referred to as the deployment of 'protected templates'.[46] There are presently standardization efforts going on in the Joint Technical Committee 1 of ISO/IEC, Subcommittee 27, in relation with protected templates.[47] The concept of 'protected template' of biometric characteristics refers essentially to the concept of protecting the biometric data and related identity by (1) the transformation and the generation of a secure reference to the biometric data by means of a robust one-way- function from which it is impossible to retrieve the original biometric information (transformation and irreversibility), (2) which reference does not permit cross matching between different databases (unlinkability), and (3) which is revocable and renewable (revocability).

Motivation

The concept of transformation of personal data is not established in the data protection legislation of most countries as such. The transformation of the original biometric data however has been suggested for a while.[48]

A recommendation nor a requirement of unlinkability of personal data is in many data protection legislations set forth in explicit terms.[49] General data protection legislation principles however require *purpose specification and purpose binding* for the collection and processing of personal data. It has been advocated to interprete these principles of purpose specification and finality, *as an obligation to prepare personal data for context-specific usage*. This could imply that it should be prevented that data could be linked for different purposes. Because of the increasing availability of biometric data over networks, it will become moreover increasingly difficult to enforce the purpose binding of personal data, unless technical measures are adopted.

The Article 29 Data Protection Working Party has stressed the *technical possibility* of linking data as a risk factor. It stated that it was necessary to scrutinize this from a data protection point of view, '*in particular concerning the technical possibility of sites sharing personal data of the user without his consent'*. [50] In the context of biometric data processing, it furthermore expressed its concern that biometric data could be used as a unique identifier and recommended that the use of biometric data for linking should be *avoided* as much as possible. [51]

In very specific cases, (unprecedented) legislation (in Ontario, Canada) referred to the irreversibility and the requirement that encrypted biometric data cannot be used as a unique identifier, capable of facilitating linkages to other information, combined with deletion of the original information.[52]

The unlinkability and irreversibility techniques shall be applied and could be recognized as 'best available techniques'[53] which render the use of biometric data more proportional with the risks for the data subjects.

---

[46] See J. Breebaart, C. Bush, J. Grave and E. Kindt, 'A reference architecture for biometric template protection based on pseudo identities', in A. Brömme (ed.), *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Bonn, Gesellschaft für Informatik, 2008, pp. 25-37.

[47] See J. Breebaart, B. Yang, I. Buhan-Dulman, Ch. Busch, 'Biometric Template Protection. The need for open standards' in *Datenschutz und Datensicherheit* 2009, pp. 299-304.

[48] See also Cavoukian, A., *Privacy and Biometrics*, Information and Privacy Commissioner, Ontario, Canada, 1999, p 5, available at https://www.pcpd.org.hk/english/infocentre/files/cakoukian-paper.doc www.ipc.on.ca

[49] The data protection legislation of only a few countries contain specific provisions relating to the linking of information, e.g., Slovenia.

[50] See Article 29 Working Party, *Working Document on on-line authentication services*, WP 68, 29 January 2003, p. 12.

[51] Article 29 Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, p.10.

[52] In particular, in Ontario, Canada, the Social Assistance Reform Act of 1997 (later revoked) and the Ontario Works Act of 1997 (Article 75).

[53] See also about the use of 'best available techniques' as one of the recommendations for privacy and data protection in the Union, ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-Induced challenges in Privacy & Data Protection in Europe*, M. Langheinrich and M. Roussopoulos (eds.), October 2008, pp. 9 and 35-36 available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf

Effect

Because biometric data are fit for use as unique identifiers, the irreversibility and the unlinkability of biometric templates is *privacy-enhancing* and privacy-compliant if there is no legal basis with specific conditions or motivations for such linkability.

Tuneable Trust

In function of the application, different trust levels may be required. By varying the amount of biometric information exposed by each individual, the concept of tuneable trust allows to control better the uncertainty / reliability of a biometric system.

Motivation

A higher accuracy is usually achieved by increasing the amount of biometric information measured from a data subject. Data subjects are entitled and controllers are obliged to process accurate and adequate personal data.

Effect

Tuneable trust does not only allow to meet in an improved way the requirement to process accurate and adequate personal data, but also to minimize data because no excessive information is accessed if this information is not necessary. It allows to adapt the amount of biometric data requested from each data subject for meeting a required level of trust for an application.

Anonymous verification

While biometric characteristics enable in essence that an individual is identified or that his or her identity is verified, it is also possible to use biometric data without the identity of the data subject being revealed. If there is no need for identification or verification of the identity, semi-anonymous or fully anonymous access control mechanisms should be put in place to manage and to verify the authorization of a given person to an area or place. These could be combined with the use of biometric characteristics if the controller has a legitimate interest to deploy biometric data to enhance the security.

Various scenarios and implementation methods exist. In some cases, it is sufficient that the service provider processes only biometric data to come to a decision, *without any other identity or pseudonym details* of the individuals concerned stored with the biometric data or separately (semi-anonymous verification). In other cases, the service provider may verify whether the anonymous user who accesses the service or place belongs to a *group* of authorized data subjects, hereby using biometric characteristics data which remain under the control of the data subject (e.g., on a token) (fully anonymous verification). To the extent it can be avoided to process identity or pseudonym details in direct relation with the biometric data (semi-anonymous verification), and in the cases where it is sufficient to perform the verification on the level of a group while the biometric characteristics data remain under the full control of the data subject (fully anonymous verification), such design and technology is recommended in view of data minimisation and anonymization objectives and in order to avoid risks of further misuse of biometric data.

Motivation

The anonymous use of biometric data[54] is in compliance with the data minimisation principle of Directive 95/46/EC. All data protection legislation of Member States require that no 'excessive data' shall be processed, while some legislations are very specific on this point.[55] Some DPAs have

[54] This should not be confused with to what some refer to as 'anonymous biometric data'. The latter is in our view strictly speaking *a contradictio in terminis*, since all biometric data refer and relate to an individual, whether directly identifiable or not.

since all biometric data relates to an individual, whether directly identifiable or not.

[55] The German Federal Data Protection Act, for example, explicitly states as a general principle that 'data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using *no* personal data *or as little* personal data *as possible (…)'* (Section 3 a).

explicitly stated that anonymous group verification is preferred when using biometric data.[56] This is also important in the evaluation of the proportionality of a system.

Effect

An anonymous biometric comparison system allows to use biometric characteristics for enabling an increased security while at the same time maintaining at the level of the service the anonymity or pseudonimity of the members of the group. Such anonymous verification system is demonstrated in TURBINE for access by pharmacists to an ehealth online forum, where anonymity is desirable, while at the same time assuring only access to pharmacists.

3.5.2 Best Practice N°8: Transparency and addition al information for the data subjects

Because of the complexity of biometric systems, *full transparency* about the processing of the personal data, especially towards the data subjects, shall be endeavoured.

This is especially the case when the informed consent is requested from data subjects for the legitimate processing of their personal data. Such consent can not validly be given if a system is not transparent. In case the controller relies on other legal grounds, transparency is equally a fundamental requirement. It results that the data subjects have to be *informed* of at least the most essential properties of the comparison system and the fall back procedures. In case the controller(s) rely on other bases for the legitimate processing, transparency is still needed.

In addition to the legal information which shall be provided according to current data protection legislation[57], it is for this reason recommended to inform the data subjects, of (i) the functioning of the system, in particular whether the verification or identification *functionality* is pursued and effectively deployed and where the biometric data are *stored*, (ii) the *error rates* of the particular system at the threshold set, and (iii) the procedure in case of failure of the system (fall back procedure) and in case of appeal by the data subject against the result of the comparison.[58] The notice could also inform the data subject about the deletion of copies of the biometric characteristics and any specific security measures taken. It is also recommended to inform the data subject of the name and contact details of the identity provider and of the service provider.

The additional information could take advantage of the possibility to be incorporated into a so-called 'multi-layered information notice'. Such notice essentially allows controllers to employ a simplified short notice in their user interface, as long as the latter is integrated in a multi-layered information structure, where more detailed information is available, and the total sum of the layers meets national requirements. There could be up to three layers of information: (i) the *short notice*, which provides the essential information (and, in view of the circumstances, any additional information necessary to ensure fair processing); (ii) the *condensed notice*, which includes all relevant information required under the Data Protection Directive; and (iii) the *full notice*, which

[56] CBPL, *Advice N°17/2008 of 9 April 2008 upon own initiative relating to the processing of biometric data for the authentication of persons*, n°77 ; See and compare also with the Biometrics In stitute Privacy Code which promotes anonymity (Article 8).

[57] The current information obligation includes *inter alia* the obligation to inform about the identity of the controller, the purposes, the recipients of the information and the access and correction right of the data subject as specified in the applicable national data protection legislation.

[58] See also CBPL, *Advice N°17/2008 of 9 April 2008 upon own initiative relating to the processing of biometric data for the authentication of persons*, n°79. The need for transparancy and agreement on FTE and FRR has also been recognized repeatedly in public sector applications, such as for the use of biometric passports. See, e.g., for the importance of this aspect for the issuance of biometric passports, EDPS, Opinion of 26 March 2008 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, *O.J.* C 200, 6.08. 2008.

includes all national legal requirements and specificities. To increase the visual presentation of some of the information, the use of icons[59], may also be considered.

This Best Practice N°8 also includes that biometric data shall *not be collected* from an individual *without his or her knowledge*.

Motivation

Under current data protection legislation, the consent by the data subject requires that the data subject has been informed about the system, that the data subject is able to choose freely whether to consent or not and that the consent is specific. In order to meet these conditions for consent, it is necessary that the data processing is transparent for data subjects in order to decide on whether they consent or not. Transparency, however, is also required if the data controller would rely on another legitimate interest for the *fair and lawful* processing of a system.

Such transparency can be created by informing the data subject of several steps in the processing of their data in an biometric IdM system. This should be done, not only before the start of the processing, but preferably also *during* the processing itself.[60] A multi-layered information notice was suggested by the Article 29 Working Party in an Opinion on harmonized information provisions in 2004 and controllers in IdM systems could take advantage of the various methods therein proposed. [61]

Effect

The increased transparency about the data processing will be beneficial for the specification of the purpose(s) of the biometric system. Information about the error rates, for example, will indicate how effective a given biometric data processing system may be for the purposes envisaged, for example for enhancing security or improving the efficiency (and fluency) of, for example, automated access, biometric payment methods, etc.

The data subject will further be able, based upon the information received, to *decide freely and in an informed way* to participate in the system.

3.5.3 Best Practice N°9: Specification of fall back procedures and of the procedure to appeal a comparison decision

The controller shall need to specify alternative procedures ('fall back procedure') in case the data subject cannot be enrolled (FTE), the biometric data cannot be acquired for further processing (FTA)[62] and/or if the data subject does not consent with the biometric data processing. These alternative procedures can be *different protocols* (e.g., the use of other fingers in a fingerprint access control system), but can also be *alternative access* procedures (e.g., the use of non-biometric access control means). A fall back procedure will also be required to control and review alleged false rejections (e.g., by determining the additional checks to be done by human intervention).

---

[59] See, for example, the suggestions made in this regard in the project PrimeLife. Other (standardization) work on icons for biometric systems is being done in ISO/IEC JTC 37 as well.

[60] Article 29 Data Protection Working Party and the Working Party on Police and Justice, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of privacy*, 1 December 2009, WP 168, p. 20 : 'Transparance : both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access/information should be enabled'.

[61] See Article 29 Data Protection Working Party, Opinion on More Harmonised Information Provisions, 25 November 2004.

[62] Increasing the number of attempts may already address various failures in a simple way. However, this will affect the security provided by the system. Moreover, it may not always solve the issue and additional fall back procedures will remain required.

Such alternative procedure shall provide to the data subjects the *same* access rights, *without significant delay* and *at no (extra) cost* for the data subject. In general, one shall take care that such alternative procedures shall in no way result in any discriminatory treatment of the data subjects.

Alternative procedures shall not only be determined in case of a *specific individual failure* affecting a particular data subject. Such procedures also need to be put in place for all data subjects in case of *general failure* of a biometric system due to a specific circumstances (e.g., failure of the whole biometric system due to hard- or software problem,…).

In case a data subject is not allowed by the biometric system, for example to pass a specific entrance gate, it shall be determined how the data subject may appeal the decision.[63] The appeal may involve the request for a further check by human intervention, but could also be a more formal procedure.

Motivation

Biometric systems use human characteristics, while considered universal and persistent, may vary from person to person which render biometric systems less accessible for some persons. Some persons will even not be able to enrol.

The need to establish alternative procedures could be compare with the need for a back up solution of a failing IT system in general. This is a general security measure, also mentioned in international IT standards (see ISO/IEC 27000 standards) and therefore qualified as 'good practice'. This 'good practice' is less straightforward from these standards in case of specific individual failure. The EDPS[64] and the national DPAs have repeatedly stressed the need of fall back procedures for biometric systems.

Effect

Fallback procedures constitute *essential safeguards* for the introduction of biometric IdM systems because they are neither fully accessible for all persons nor completely accurate.

At the same time, the fallback procedures shall *not decrease the security level* of the system *nor stigmatize the individuals* who are not able to provide their characteristics for processing. Fallback procedures shall effectuate that there is no discrimination between individuals in the request to provide biometric characteristics.

3.6 Additional Best Practice N°10: On the *organization, the security* and the *certification* of a biometric IdM system

3.6.1 Organizational and technical security measures shall address the specific risks of biometric data processing

In addition to the various design, enrolment and implementation best practices aspects which enhance the privacy and data protection rights of the data subjects, appropriate organizational measures are needed to back up these recommended practices. For example, in addition to the technology to revoke biometric identities, revocation schemes will have to be defined, organized and be set up for the revocation. In order to address the privacy concerns at the stage of the design of a biometric IdM system, it shall be organized that these concerns are discussed right from the start.

[63] Also note that in principle, automated individual decisions which produce legal effects or significantly affect the data subject and which are based on solely automated data processing are prohibited (Art. 15 (1) of the Directive 95/46/EC).

[64] While the EDPS has stated this especially for large-scale implementations in the public sector, such as VIS, this is nevertheless also relevant for biometric systems in the private sector.

The organisational measures shall in principle address the various steps of a biometric system. For enrolment, sufficiently *trained and qualified* staff shall assist in this procedure.[65] Clear agreements have to be made about the identity credentials that the data subject shall submit for the enrolment in the IdM system and any exemptions for enrolment, for example for children under a certain age or for elderly people. Access to any data in the system shall be *restricted* and reserved for duly *authorized* persons authenticated by one or multiple factors. A list of such persons has to be made and kept up-to-data.

Furthermore, the biometric data processing controller shall assess, analyze and address the specific *risks* of each component of the biometric system. This includes risks associated with the support medium of the data (e.g., a smart card), the biometric sensor(s) and the communication links between the various components. General measures for protecting biometric data are not sufficient.[66] The level of security needs to be *appropriate* to the risks presented by the biometric system. The controller shall hereby take *the state of the art in account*, as well as the *cost* of implementation of such state of the art measures.[67] The general data protection legislation further mandates the data controllers to take *the risks represented by the biometric processing* and *the specific nature of the biometric data into account.*

These risks shall be sufficiently *defined, documented* and appropriate security measures *implemented.* If, for example, the enrolment for a specific biometric IdM systems would require a thorough check of the identity and/or credentials, persons to perform these checks shall receive specific instructions and be trained. Furthermore, the systematic (self) auditing of security measures is recommended. In case of breach of the security of the biometric data whereby biometric data is or could reasonably be believed acquired by an unauthorized entity, such security breach shall be notified by the controller to the authorities and to the data subjects concerned.

If the controller relies on one or more processors, the controller shall choose a processor which provides sufficient guarantees that such measures shall be implemented and shall ensure the compliance with these measures. The controller shall therefore enter into a *written or equivalent contract with the processor*.

Motivation

The data protection legislation imposes upon the data controllers the obligation to implement appropriate technical and organizational measures to protect personal data against (i) accidental or unlawful *destruction*, (ii) accidental *loss*, (iii) *alteration*, (iv) unauthorized *disclosure or access*, in particular where the processing involves the transmission of data over a network, and against (v) all *other unlawful forms* of processing.[68] Some DPAs have issued guidelines for the controllers with more recommendations for the implementation of such measures, but these general guidelines do not sufficiently address the specific risks of biometric systems.[69]

In opinions on the implementation of specific biometric systems, the EDPS and the DPAs have made these recommendations more specific in view of the risks of biometric data processing (e.g., the risks for re-use of data can be prevented by restricting access and monitoring such access).

Effect

Appropriate organizational and technical security measures are essential to protect the data subject's privacy and data protection rights.

---

[65] See, e.g., the new Article 1 a introduced by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on biometric passports and travel documents.

[66] See, e.g., ISO19092: 2008 for a concise overview of infrastructure requirements (see also Annex 1).

[67] See also Art. 17 (1) § 2 of the Directive 95/46/EC.

[68] See also Art. 17 (1) of the Directive 95/46/EC.

[69] See, e.g., for Belgium, CBPL, *Reference measures for the security for every processing of personal data,* 4 p., available at http://www.privacycommission.be/nl/static/pdf/ referenciemaatregelen-vs-01.pdf

The European Court of Human Rights has stressed in its case law that insufficient security measures may imply a breach of one's right to privacy.[70]

Data subjects, suffering damages as a result of unlawful processing, are entitled to receive compensation from the controller(s) of biometric IdM processing systems.

3.6.2 Certification

Because the technical operation and effects of biometric products and systems are difficult to evaluate by non-technical persons, such biometric products and systems should be reviewed by experts, both IT-experts and legal experts. The certification should address the security aspects ànd data protection aspects. The evaluation could be done in two steps, based on the functional and technical specifications of the system in the design phase, and continued upon the practical implementation of the system.[71]

This would lead to the certification of the biometric products and systems relating to its privacy-enhancing characteristics and privacy-compliance. This should be done in a certification program which takes also the privacy regulations (e.g., with regard to the requirement of information to be provided to the data subject and transparency) in a consistent way into account.[72] Voluntary certification and self-certification of compliance could be the first steps towards such certification program.

Motivation

Various DPAs and the EDPS have stressed the opportunities that certification may offer.[73] The ENISA Ad Hoc Working Group on Privacy & Technology also reiterated the benefits of certification in its report on '*Technology-Induced challenges in Privacy & Data Protection in Europe'.*

Effect

Best practices in combination with certification could render the sometimes complex legal regulations more clear for the stakeholders and the data subjects concerned. Clear information and communication about the issues covered by certification (and the issues not covered) are indispensable. The combination of best practices and certification could also facilitate the application of selected legal principles.

[70] ECHR*, I. v. Finland*, application 20511/03, 17 July 2008.

[71] See and compare also with the Biometrics Institute Privacy Code which requires the auditing of biometric systems (Article 13).

[72] An example of a European wide certification scheme which provides a privacy trust mark for end-users is EuroPriSe. EuroPriSe is based on European privacy standards, which are outlined in the EurPriSe Criteria. See EuroPriSe, *EuroPriSe Criteria,* v.1.0, available at https://www.european-privacyseal.eu/criteria/EuroPriSe%20Criteria%20Catalogue%20 public%20version%201.0.pdf The certification scheme, however, is not specific for biometric (IdM) systems. Certification and data protection compliance has also been regulated in Switzerland.

[73] See, for example, the Independent Centre for Privacy Protection Schleswig-Holstein (ICCP/ULD), Germany, which leads the EuroPriSeconsortium. See also the CNIL, which joined the French governmental institute AFNOR, with the goal to be heard in domains such as biometrics (CNIL, *30 ans au service des libertés. 29e rapport d'activité,* p. 52).

4. Conclusions

The aforementioned TURBINE Best Practices suggested several guidelines which identity and service provider controllers of IdM systems should follow when implementing a biometric IdM system. The guidelines have been formulated in a limited number and in a concise way in order to allow the stakeholders to keep an overview of the most important privacy-enhancing requirements. They are based on one hand on previous work on the formulation of best practices for biometric data processing in other projects (e.g., BioVision) and on the other hand on TURBINE research and experience in relation with the implementation of the TURBINE technologies developed. Initial research ideas on best practices were also presented during the IFIP/PrimeLife summer school in 2009 and were published. They have also been submitted, reviewed and discussed with the Advisory Board team to TURBINE. The TURBINE Best Practices do not address all issues in relation with biometric data processing (e.g., spoofing), but focus on the most essential ones.

Privacy-enhancing technologies, such as for the irreversibility, the unlinkability and the revocation of biometric identities, and anonymous verification, developed and applied by TURBINE, have been given a clear role in these Best Practices. PETs have always been considered as necessary in preserving privacy of individuals in networks, and may play an important role in biometric systems.[74] These technologies will further develop but the functionalities that they pursue may remain the same.

The Best Practices require in addition a review of the compliance of a given biometric IdM system with the applicable national data protection legislation(s). Guidelines on the interpretation of the local data protection legislation with regard to the processing of biometric data for purposes of compliance have been issued by various DPAs now and compliance should be checked for each biometric IdM system, as well as special legal requirements for biometric data processing, such as, if needed, prior notification or authorization by the DPA.

[74] See EU Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final, 10 p.; see also R. Hes, T. F. M. Hooghiemstra and J.J. Borking, *At Face Value. On Biometrical Identification and Privacy,* Achtergrond Studies en Verkenningen 15, The Hague, Registratiekamer, September 1999, 74 p.

5. Selected Bibliography

Legislation and policy documents

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, pp. 31- 50

Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 142, 06.06.2009, pp. 1 – 4.

Ontario Works Act, 1997, Article 75, available at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_97o25a_e.htm

EU Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final, 10 p.

ISO/IEC JTC 1/SC 37, Standing Document 2 – Harmonized Biometric Vocabulary, version 12, N 3385, New York, ANSI, 16 September 2009, working draft text, 203 p.

ISO/IEC JTC 1/SC 37, *Text of Working Draft 24779- -2, Cross-jurisdictional and societal aspects of implementation of biometric technologies – Pictograms, icons and symbols for use with biometric systems - Part 2 : Fingerprint applications,* N 3363, New York, ANSI, 25 August 2009, working draft text, 24 p.

Opinions of the Article 29 Data Protection Working Party, the EDPS and DPAs

A. Türk, *Declaration for the European personal data protection day*, 28 January 2010, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_28_01_10_en.pdf

Article 29 Data Protection Working Party, *Opinion on More Harmonised Information Provisions*, WP 100, 25 November 2004, 9 p., available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/ wp100_en.pdf

Article 29 Data Protection Working Party, *Working Document on Biometrics*, WP 80, 1 August 2003, 11 p. available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf

Article 29 Data Protection Working Party, *Working Document on on-line authentication services*, WP 68, 29 January 2003, 15 p., available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf

Article 29 Data Protection Working Party and the Working Party on Police and Justice, *The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of* privacy, WP 168, 28 p.

Cavoukian, A., *Privacy and Biometrics*, Information and Privacy Commissioner, Ontario, Canada, 1999, 15 p., available at https://www.pcpd.org.hk/english/infocentre/files/cakoukian-paper.doc www.ipc.on.ca

Cavoukian, A., Stoianov, A. and Carter, F., 'Biometric Encryption: Technology for Strong Authentication, Security AND Privacy' in E. de Leeuw, Fischer-Hübner, S., Tseng, J., Borking, J. (eds.), *IFIP. Policies and Research in Identity Management*; Boston, Springer, 2008, pp. 57–77.

Cavoukian, A. and Stoianov, A., *Biometric encryption : a positive-sum technology that achieves strong authentication, security and privacy*, Privacy Commissioner Ontario, 2007, available at www.ipc.on.ca

CBPL, *Advice N°17/2008 of 9 April 2008 upon own initiati ve relating to the processing of biometric data for the authentication of persons*, 22 p.

CBPL, *Reference measures for the security for every processing of personal data,* 4 p., available at http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

CNIL, Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 28 December 2007, 12 p.

EDPS, Opinion of 26 March 2008 on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation No 2252/2004, *O.J.* C 200, 6.08. 2008.

EDPS, Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information Systems (SIS II) (COM (2005)230 final, COM (2005)236 final and COM(2005)237final, *O.J.* C 91, 19.04. 2006, pp. 38-56.

EDPS, Opinion of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas COM(2004)835final, *O.J.* C 181, 23.07. 2005, pp. 13-29.

Articles and reports

Biermann, H., Bromba, M., Busch, C., Hornung, G., Meints, M. and Quiring-Kock, G. (eds.) *White Paper zum Datenschutz in der Biometrie,* 2008, available at http://teletrust.de/fileadmin/files/ag6/Datenschutz-in-der-Biometrie-080521.pdf.

Bogdanowicz, M., and L. Beslay, L., *Cyber-security and the future of identity,* IPTS report, 2002

Breebaart, J., Yang, B., Buhan-Dulman, I., Busch, Ch. , 'Biometric Template Protection. The need for open standards' in *Datenschutz und Datensicherheit* 2009, pp. 299-304.

Breebaart, J., Bush, Ch., Grave, J. and Kindt, E., 'A reference architecture for biometric template protection based on pseudo identities', in A. Brömme (ed.), *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*, Bonn, Gesellschaft für Informatik, 2008, pp. 25-37.

CNIL, *21e rapport d'activité 2000*, Paris, CNIL, 2001.

Committee of experts on data protection (CJ-DP), *The introduction and use of personal identification numbers : the data protection issues*, Council of Europe, 1991, 20 p., available on http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Pins_1991_en.pdf

Consultative Committee of the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data [CETS No. 108] (T-PD), *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, Council of Europe, CM(2005)43, March 2005, 22 p., available at https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2005)43&Language=lanEnglish&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged

Dinant, J.-M., 'Chapter 5. The Concepts of Identity and Identifiability: Legal and Technical Deadlocks for Protecting Human Beings in the Information Society', in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, S. Nouwt (eds.), *Reinventing Data Protection,* Springer, 2009.

ENISA Ad Hoc Working Group on Privacy & Technology, *Technology-Induced challenges in Privacy & Data Protection in Europe*, M. Langheinrich and M. Roussopoulos (eds.), October 2008, 48 p. available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_privacy_wg_report.pdf

European Security Research & Innovation Forum (ESRIF), Final Report, December 2009, 324 p.

Goldstein, J., Angeletti, R., Holzbach, M., Konrad, D., Snijder, M., Rotter, P., (eds.), *Large-scale Biometrics Deployment in Europe : Identifying Challenges and Threats*, JRC Scientific and Technical Reports, European Commission JRC – IPTS, Seville, 2008, 135 p.

Grijpink, J., 'Two barriers to realizing the benefits of biometrics : a chain perspective on biometrics, and identity fraud as biometrics' real challenge', *Computer Law and Security Report* 2005, pp. 138-145 and pp. 249-256

Hes, R., Hooghiemstra,T. and Borking, J., *At Face Value. On Biometrical Identification and Privacy,* Achtergrond Studies en Verkenningen 15, The Hague, Registratiekamer, September 1999, 74 p.

Kindt, E. and Müller, L. (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, 130 p., available at http://www.fidis.net

Kindt, E. and Müller, L. (eds.), *D13.4. The privacy legal framework for biometrics*, Frankfurt, FIDIS, 2009, 134 p., available at http://www.fidis.net

Kindt, E., 'The use of privacy enhancing technologies for biometric systems analysed from a legal perspective' in M. Bezzi et al. (eds.), *Privacy and Identity*, IFIP International Federation for Information Processing AICT 320, 2010, pp. 134—145.

Korte, U., Merkle, J., Niesing, M., 'Datenschutzfreundliche Authentisierung mit Fingerabdrücken. Konzeption und Implementierung eines Template Protection Verfahrens – ein Erfahrungsbericht', *Datenschutz und Datensicherheit* 2009, pp. 289 – 294.

Legal-IST, Doc. No 11, *Privacy-Identity Management*, 4 November 2005.

Meints, M. and Hansen, M., 'Additional and in some cases health related information in biometrics', in E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 83-86.

Müller, L., 'Biometric system errors', in E. Kindt and L. Müller (eds.), *D.3.10. Biometrics in identity management*, Frankfurt, FIDIS, 2007, pp. 26-36.

OECD, Directorate on Science, Technology and Industry, *At a Crossroads : "Personhood" and Digital Identity in the Information Society,* STI Working Paper 2007/7, 29 February 2008, 51 p., available at http://www.oecd.org/sti/ict/reports

Organisation For Economic Co-Operation And Development, *Biometric-based Technologies*, 28 April 2004, 66 p.

Prime, *Prime White paper*, 2008, v.3.0, 19 p., available at https://www.prime-project.eu/prime_products/white paper/PRIME-Whitepaper-V3.pdf

Rossnagel, A., (ed.), *Allgegenwärtige Identifizierung ? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung*, Baden-Baden, Nomos, 2006, 132 p.

TURBINE, D.1.1.1, August 2008, 75 p.

Van Kralingen, R., Prins, C. and Grijpink, J., 'Het lichaam als sleutel', *National Programma Informatietechnologie en Recht*, 8, Alphen aan den Rijn/Diegem, Samsom BedrijfsInformatie Bv, 1997, 66 p.

Previous best practices initiatives :

Albrecht, A., *BioVision. Privacy Best Practices in Deployment of Biometric Systems,* BioVision, 28 August 2003, 49 p., available at http://www.eubiometricsforum.com/ (last visited on 19 September 2006)

Biometrics Institute, *Biometrics Institute Privacy Code*, 19 July 2006, approved by the Australian Privacy Commissioner, available at http://www.biometricsinstitute.org/displaycommon.cfm?an=1&sub articlenbr=8

BWG, *Biometric System Security Evaluation and Certification – MS09*, available at http://www.cesg.gov.uk/policy_technologies/biometrics/ms09.shtml

BWG, *Use of Biometrics for Identification and Authentication. Advice on Product Selection.* Issue 2.0, 22 March 2002, 36 p.

EuroPriSe, *EuroPriSe Criteria,* v.1.0, available at https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20Catalogue%20 public%20version%201.0.pdf

International Biometric Group, The BioPrivacy Application Impact Framework, 2001, available at http://www.bioprivacy.org/bioprivacy_main.htm

Initiative on Privacy Standardization in Europe (IPSE), *Initiative on Privacy Standardization in Europe*, Final report, CEN/ISSS, 13 February 2002, 89 p., available at http://www.cen.eu/CENORM/Sectors/Sectors/ISSS/Activity/ipsefinalreportwebversion.pdf

6. Annexes

6.1 Annex 1: Concise overview of general infrastructure requirements to counter administration, infrastructure and biometric overtness vulnerabilities as set forth in ISO19092: 2008

- Mechanisms to maintain the integrity of biometric data and authentication results between various components;
- Mechanisms to mutually authenticate the source and destination of biometric data or authentication results;
- Mechanisms to ensure the confidentiality of the biometric data between any two components;
- Mechanisms to ensure an enroller has the proper permissions (access control for the enrolment function) to enrol the enrolee;
- Mechanisms and procedures to ensure a binding of the biometric information to the enrolee, such that the biometric information captured during enrolment belongs to the enrolee;
- Tamper-resistant comparison subsystems, or comparison subsystems in a physical environment that provides a high level of security;
- Tamper-evident mechanisms that result in visual evidence that an attack has been attempted;
- Tamper-responsive mechanisms that detect unauthorized access and initiate countermeasures, such as placing the system into a security state; and
- Tamper resistant mechanisms that resist physical penetration.[75]

[75] Turbine, D1.1.1, August 2008, p. 30.

6.2 Annex 2: EDPS Opinion of 1 February 2011 on TURBINE

As part of the TURBINE project, partners requested the opinion of the EDPS on the developments made in TURBINE. The request for opinion was filed on July 2010 as a milestone of the project.

TURBINE partners received the opinion of the EDPS on 1 February 2011. The opinion is public and the text can be consulted on the website of the EDPS.[76] The opinion will be published in the Official Journal as well. It is the very first time that the EDPS issues an opinion on a European research project.

The EDPS analyzed several aspects of the project, including in particular the features of irreversibility and revocability of the biometric identification technology developed in TURBINE. The implementation of these two features contributes according to the EDPS significantly to privacy compliance by providing acceptable privacy compliant solutions.[77]

The TURBINE Best Practices were also submitted to the EDPS for his opinion.

The EDPS acknowledged the relevance of the Best Practices and stated that

> *'developing the best practices listed above will help to implement appropriate measures for any biometric Identity Management System conducted in compliance with the EU regulatory framework. Such a check list could indeed allow development of more privacy friendly systems, if they are taken into account from the start of projects'.*

With regard to the fallback procedures and the level of accuracy, the EDPS clarified that they have to be defined according to the precision of the system and monitored constantly in relation to the population using the system. The investment which needs to be made in the fallback procedures will be defined by the level of those rates. The EDPS stated that *setting the precise level of accuracy* expected from a biometric system is of *great importance* and recommended that this *should be established early in the system* and be *integral part of the Best Practices as well*.[78]

[76] EDPS, Opinion 1.02.2011 on a research project funded by the European Union under the 7th Framework Programme (FP 7) for Research and Technology Development (Turbine (TrUsted Revocable Biometric IdeNtitiEs), 14 p., also available at http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Consultation/OpinionsC/OC2011 ('EDPS, Opinion on Turbine, 2011')

[77] EDPS, Opinion on Turbine, 2011, §67 and §69.

[78] EDPS, Opinion on Turbine, 2011, §§ 34-37.

TURBINE partners agree with the recommendation of the EDPS.

They suggest that the TURBINE Best Practices, which were developed during the project, are now amended in BP N° 9 with this precision by the EDPS which was however received after the end of the TURBINE project and therefore not taken into account before.

BP N°9 of this document shall hence be entitled 'Ac curacy, fall back procedure and appeal' and shall be completed on p. 23 with the following paragraphs after respectively the third and fifth paragraph :

> "In addition, a precise level of accuracy expected from the biometric system shall be set *early*. Both the fallback procedures and the level of accuracy have to be defined according to the precision of the system and shall be *monitored constantly* during the operational use in relation to the population using the system."
>
> **Motivation**
>
> (…)
>
> "The setting of a *precise level of accuracy* is of *great importance.* Moreover*, t*he investment which needs to be made in the fallback procedures will be defined by the level of those rates."

Furthermore, the overview of the TURBINE Best Practices will hence be as follows :

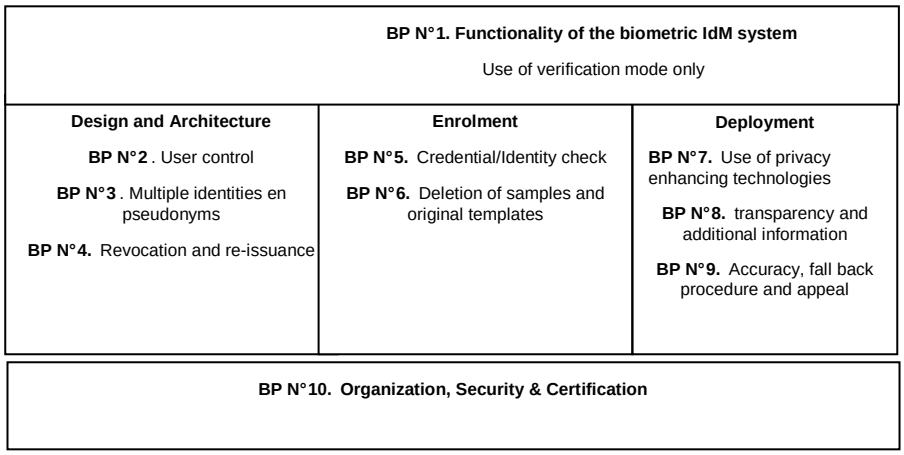

Figure 2: Overview of the suggested Turbine Best Practices for a biometric IdM system, including the suggestion of the EDPS about accuracy in BP N° 9

Furthermore, it may be noted that the EDPS commented that 'the project, although not mentioning *stricto sensu* the level of accuracy among its list of best practices, has taken into account his aspect in the research, by setting precise accuracy goals at the beginning of the project. Furthermore, through the research, this level of accuracy has been tested, verified and even improved as to allow that for the use of a biometric sytem in an operational environment, such precise levels of accuracy will be adopted'.[79]

[79] EDPS, Opinion on Turbine, 2011, §36.

6.3 Annex 3: Application of the TURBINE Best Practices to use cases

This Annex 3 demonstrates the application of the Best Practices developed above to two use cases. A first use case pertains to the use of biometric identifiers in an ehealth environment. The second use case demonstrates the Turbine Best Practices in the financial sector:

At the same time, these use cases discuss nor identify all rights and obligations under the Directive 95/46/EC as implemented in national law, while some may be mentioned however. It is therefore stressed that for each and every use case full respect shall be paid to existing national data protection legislation *in addition* to the application of the Best Practices set forth in this document.

Expert advise may be required to assess risks and compliance for each use case.

6.3.1.Turbine Best Practices in the ehealth sector

Use of biometric pseudo-identities for protecting and securing access to information concerning health (medical data)

Patients are entitled to the processing of information concerning their health with a *security level appropriate to the risks and the nature of the data.* This requires that potential vulnerabilities are adequately handled. One of these vulnerabilities is access by unauthorized persons, both from within and from outside the organisation. to their health data, for example maintained in a centralized file or kept in a hospital. Article 17 (1) of the Directive 95/46/EC as implemented in national data protection legislation imposes a general *obligation* to implement appropriate technical and organizational measures to protect health data. Security measures shall include *access and logging* control.[80] State of the art and reduced costs for biometric applications may result in a decision to implement biometric security measures to protect access by health professonials to health related data and others with a need. Biometric enhanced access control even becomes more urgent with increasing obligations to notify breaches of personal data protection. While data controllers could hence invoke legitimate interests and a legitimate aim, data subjects are entitled to safeguards limiting or excluding interference with their privacy and data protection rights. In case consent would be asked, alternative measures in case of refusal are to be provided as such consent shall remain free. For this reason, a regulation confirming the (substantial) (public) interest in enhanced security for accessing medical data records of patients, could be preferred.

To limit[81] interference with fundamental rights of the data subjects, Turbine Best Practices recommend to use biometric technology to only *verify* the identity of the individual authorized to have access and to store the biometric pseudo-identity on a *card*[82], kept under the control of the individual (BP N° 1 and 2). The biometric pseudo-id entity stored on the card allows to ensure that

[80] See ECtHR, *I. v. Finland*, no. 20511/03, 17 July 2008 where the European Court for Human Rights found a violation by Finland of the right to privacy (Article 8 ECHR) of a nurse, whose medical data (for treatment of HIV and processed in the same hospital as where she was employed) were not sufficiently secured and kept confidential against unauthorized access by her colleagues ; see and compare also with U.S. federal privacy requirement in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations which requires secure electronic access to patient's medical records to maintain data integrity and confidentiality.

[81] The safeguards proposed by the Turbine Best Practices are aimed at limiting interference as much as possible with the fundamental rights of the data subjects to privacy and data protection. Whether these safeguards recommended are sufficient to exclude any interference, will have to be determined by case to case.

[82] E.g., a Health Professional Card. This card could be a multipurpose card (since cards are also commonly used for other purposes in this environment), provided the storage of the biometric pseudo-identity/ies is/are sufficiently secured.

the card holder is 'valid', i.e. that the person is entitled to hold and to use the card. The identity of that individual having access shall however previously have been properly identified before enrolment (for example, review of the credentials of a health practitioner, of employment with and function within the hospital for personnel, ….) (BP N° 5). Turbine Best Practices further require that the identity provider processes the original biometric samples captured from the data subject ànd the template in such way that the digital representations of the biometric characteristics in the pseudo-identities are *irreversible and unlinkable*, i.e. irreversible to the original sample and template, specific for this purpose of access control to medical data in this particular environment and organisation, allowing to destroy the biometric samples ànd templates afterwards. (BP N° 6 and 7).

The stored biometric pseudo-identity on the card should not be linkable with other (similar) activities of health practitioners for which a biometric pseudo-identity would be needed[83], for example access to an online information forum reserved for particular professionals. Turbine Best Practices recommend hence that data subjects are entitled to multiple, unlinkable and irreversible biometric identities as pseudonyms (BP N° 3). These identities could be on the same card, and an appropriate user interface should allow the data subject to exercise control over the use of these identities. Such multiple identities also allow for adressing different levels of security and of authorization and access rights, while transactions cannot be linked.

In case of loss or theft of the card, the biometric pseudo-identity shall be revocable. In addition to the technology used, such revocation procedure shall be set up, as well as other organisational measures for security and for fall back in case of need shall be organised (BP N° 9 and 10). The individuals authenticated by their biometric characteristics for access to health related information of others shall receive all appropriate information as set forth in BP N° 8, including information about the safeguards deployed and the error rates.

Enhanced identity control of patients before treatment and for reimbursement

Another scenario for the use of biometric identities is the secure identification (control) of patients before treatment, for example by radiotherapy[84], as well to prevent impersonation in case of treatment for reimbursement of expenses by (private) health insurances.

The interests of the controller to apply enhanced security measures by biometric comparison shall outweight the interests of the patients to privacy and data protection, however. This balance could be effectuated by limiting or excluding the risks upon the deployment of biometric identitifiers as much as possible by deploying appropriate safeguards which limit these risks. Turbine Best Practices contain such safeguards in ten principles, covering the need of the specification of the controller's need (and the definition of the purposes), followed by the design, the enrolment and the actual deployment of the system. National data protection legislations, however, should be reviewed as well, as they may contain specific provisions on the rights of patients and social security. In case the government would become involved, for example for enrolling and issuing the biometric identities, legislation is needed stipulating the legitimate aims, the safeguards and motivating the necessity of the use of biometric data.

The application of Turbine Best Practices implies that the *identity* of the individual listed for treatment or authorized for treatment with reimbursement is *verified* only, without the need for central storage, but local storage of the biometric pseudo-identity on a *card*[85], kept under the control of the individual (BP N° 1 and 2). This requires that appropriate procedures have been determined and followed by the identity provider (for example, a hospital, or practitioner of the art of

[83] For example, for issuing prescriptions or ordering medicines. In case of the need for enhanced secured access to particular online information, BP N° 7 recommends anonymous verification of the identity. This was also demonstrated in the Generic Demonstrator of Turbine.

[84] See also and compare with the authorization of the French DPA for centralized storage of fingerprint for such purpose: CNIL, *La biométrie entre à l'hôpital pour identifier des patients traités par radiothérapie,* 15.04.2010, available at http://www.cnil.fr/la-cnil/actu-cnil/article/article/la-biometrie-entre-a-lhopital-pour-identifier-des-patients-traites-par-radio therapie-1/

[85] E.g., a (European) Health Insurance Card.

healing, ….) for properly identifying the patient (including medical coverage if applicable) before and during enrolment when the biometric pseudo-identities are issued (BP N° 5). The roles between the identity provider(s) and the service provider(s) shall be determined. Patients are according to the Turbine Best Practices entitled to the use of multiple biometric pseudo-identities, for example for treatment in different organisations, but also for different use, such as for health treatment and administrative purposes (in particular for reviewing and securing the entitlement for health treatment in particular reimbursement schemes). These biometric pseudo-identities should be revocable in case of theft or misuse of the identity or of the card, by applying privacy-enhancing techniques. These techniques shall meet in addition to revocability, the objectives of unlinkability and irreversibility, as identified in the Turbine Best Practices (BP N° 4 and 7). Pseudo-identities could also be renewed each time a new medical consultation is given to a patient.

Turbine Best Practices further require to delete the samples and unprotected templates after capture for every use (BP N° 6), which is also allo wed by using the recommended techniques. The patients shall receive all appropriate information as set forth in BP N° 8, including information abou t the safeguards deployed, place of storage, the error rates and of his or her right to appeal any decision of the biometric application. The controller shall deploy several other organisational measures for security and for determining and organizing fall back procedures in case of need (BP N° 9 and 10).

6.3.2. Turbine Best Practices in the financial sector

Another use case permitting to illustrate the application of the Turbine Best Practices is the deployment of biometric technologies for enhanced verification of the identity of banking customers, for example when using a payment card for a transaction whereby they instruct to debit their bank account, either at a point of sale or at an ATM for withdrawing money.

Banking and affiliated organisations may have a legitimate interest in enhancing the security of the use of banking cards, for example in case of increased fraud, as evidenced by facts and reports, where the traditional use of banking card with PIN and additional security measures (other than the use of biometric data) proves to be no longer sufficiently reliable, and upon the conditions the use of biometric identifiers is assessed to be appropriate and the only means to enhance the security. This legitimate interest and aim of the controller(s) shall however respect the rights of the banking customers to privacy and data protection, by limiting or excluding risks associated with the use of biometric identifiers. Consent of the banking customers with the collection and the use of the biometric identifiers may play a role, if their choice is informed and free, but only to the extent customers have viable alternative measures (which shall not result in increased costs or discrimination between banking customers) in case they would not consent. In addition, and in order not to override the interests of the data subjects, appropriate safeguards shall be taken to exclude the risks for interference with the fundamental rights of the data subjects. These appropriate safeguards shall ensure that fundamental rights are not interfered with and may lead to so called user-controlled banking applications.

Turbine Best Practices could guide the controllers in implementing such appropriate safeguards. In accordance with these Best Practices, banking customers are entitled to multiple, unlinkable and irreversible biometric identities as pseudonyms (BP N° 3). Such multiple biometric identities will enhance the privacy of customers when relying on several services of the banking organisation (for example, insurance services, banking services, investment services, …) without a need to link the use of these services by the same data subject. The irreversible pseudo-identities should guarantee that the biometric identities used cannot be reverse engineered to the original samples or template, and that the latter can be deleted. The pseudo-identities should further be issued only after a thorough identity check of the customer, which is often regulated by specific national legislation, requiring the proper identification in compliance with anti-money laundering legislation (BP N° 5). The pseudo-identities shall be used to *verify* (BP N° 1) the identity of the customer upon each use of the card issued and for accessing bank accounts or ATM, preventing the use of the same cards after skimming or shoulder surfing or theft of the card by thieves or impostors in combination with the PIN.

The architecture for such local verification of biometric identity, which shall preferably be reviewed and certified, should come in addition to existing authentication structures for pin verification value of card users in the banking sector, which shall remain in place as fall back or alternative measure in case the customer do not consent (BP N°9 and 10). The banking customer should with an easy interface have full control over the use of his or her biometric pseudo-identities for banking services, including for selecting a biometric pseudo-identity, allowing for anonymous but secure verification of membership of a loyalty program of the customer for taking up membership services to which he or she is personally entitled to (BP N° 2 and 7). It is for these last services not necessary to verify the identity of the customer, but only whether he or she is member of the group. The level of trust for this particular use could also be adapted (i.e., lowered) (BP N°7).

The banking customer should receive full and transparant information about the functioning of the use of the biometric pseudonymous identifiers, including about the (risks of) FRR (i.e., this should be reasonably low in view of the usuability of the services) and FAR (i.e. acceptance of impostors). This information should also be provided when interacting with the system, for example in multi-layered information notices (BP N° 8). In case the customer is no longer with the same banking organisation, the biometric identities shall be revoked and all personal data properly deleted, for which the controllers shall set up an appropriate procedure. More importantly, such revocation, including renewability and re-issuance of the biometric pseudo identities, should be possible in case of theft or misuse of the biometric data (BP N°4 and 6).

Finally, we hereby also like to refer to the proposed GlobalPlatform based architecture for multiple service providers as developed in Turbine public deliverable 1.2.1.[86] This architecture explaines the storage of several pseudonymous identifiers (Turbine's 'pseudo-identities') on one token, for use by several service providers.

[86] KUL, D.1.2.1. Services and schemes for multiple trusted identity, Turbine, February 2008, pp. 33-34, available at http://turbine-project.org/dowloads/TURBINE-KUL-D121-General_Scheme-R1.0.pdf