FIDIS

Future of Identity in the Information Society

Title:	"D3.10: Biometrics in identity management"
Author:	WP3
Editors:	Els Kindt (KU Leuven), Lorenz Müller (AXSionics AG)
Reviewers:	Mark Gasson (University of Reading, UK) Jozef Vyskoc (VAF, Slovakia)
Identifier:	D3.10
Type:	Deliverable
Version:	1.0
Date:	28 December 2007
Status:	Final report for submission to the Commission
Class:	Public
File:	

Summary

This deliverable discusses the deployment of biometrics for the management of identity in the public and private sector from a technical, legal, security and forensic point of view. It highlights some specific security and privacy aspects, including those from new demonstrations of user/capture and capture/extraction threats, but also stresses the advantages which biometrics offer. The research indicates that a fruitful debate about the risks and opportunities of biometrics requires the use of an agreed harmonised vocabulary and that discussion should focus on where the control over the biometric system is exercised and on the functionalities and purposes of the applications. The report proposes, in this context, five groups of biometric application models for future use. Although biometric references become increasingly part of various identity applications, there remain several research items which are not yet fully explored as illustrated and described, such as the question of health related information contained in biometric templates and the proportionality of the use of biometric data. The report also warns for biometric data becoming a primary key for the interoperability of systems. Finally, the document offers guidance in the deployment of biometrics, including by describing an approach on how to preserve privacy and to enhance security by the data subject retaining control over the biometric data.

The FIDIS *NoE receives research funding from the Community's Sixth Framework Program*

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	The Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	The Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.3	20.09.2006	• First draft of commented table of content (Lorenz Müller, Els Kindt)
0.4	15.11.2006	• Control models defined
0.5	01.02.2007	• Contributions collected
0.6	02.04.2007	• Preliminary integration of contributions I (Lorenz Müller)
0.61	15.05.2007	• Preliminary integration of contributions II (Els Kindt)
0.62	13.07.2007	• Final integration of contributions (Els Kindt, Lorenz Müller)
0.7	12.09.2007	• Final draft, ready for internal review (Els Kindt, Lorenz Müller)
0.8	05.10.2007	• Final draft sent to reviewers
0.9	19.11.2007	• Final draft with comments and integration of comments from reviewers (Mark Gasson, Jozef Vylstock, Els Kindt, Lorenz Müller)
1.0	28.12.2007	• Final version for submission to the Commission (Els Kindt, Lorenz Müller)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the contributors for the chapters of this document:

Chapter	*Contributor(s)*
1.Executive Summary	Els Kindt, KUL, Lorenz Müller, AXSionics
2. Introduction	Els Kindt, KUL (2.1, 2.2, 2.3) Lorenz Müller, AXSionics (2.2, 2.3)
3.Review of facts on biometrics	Lorenz Müller, AXSionics (3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.3.2, 3.3.3) Els Kindt, KUL (3.1.1, 3.2, 3.2.1, 3.2.2, 3.3.1, 3.3.2, 3.3.3) Paul De Hert, VUB & Annemarie Sprokkereef, TILT (3.2.3) Martin Meints & Marit Hansen, ICPP (3.3.2, 3.3.3)
4. Security and privacy aspects of biometrics	Lorenz Müller, AXSionics (4.1, 4.2.1, 4.2.2, 4.3.1, 4.4) Martin Meints & Marit Hansen, ICPP (4.3.2, 4.3.3, 4.4.2) Rikkert Zoun, NFI (4.4, 4.4.1) Zeno Geradts, NFI (4.4.2) Els Kindt, KUL (4, 4.2.1, 4.2.2, 4.3)
5. Advantages and needs of biometrics	Martin Meints & Marit Hansen, ICPP (5, 5.1) Els Kindt, KUL (5.1, 5.5) Lorenz Müller, AXSionics (5, 5.2) Vicky Andronikou, ICCS (5.3, concl. rem.) Zeno Geradts, NFI (5.4) Koen Simoens, KUL (5.2, 5.5)
6. Recommendations and guidelines	Lorenz Müller, AXSionics (6.3, 6.4) Els Kindt, KUL (6, 6.1, 6.4) Martin Meints & Marit Hansen, ICPP (6.4) Koen Simoens, KUL (6.2)
7. Conclusions	Els Kindt, KUL, Lorenz Müller, AXSionics, Martin Meints & Marit Hansen, ICPP
Abbreviations and Glossary	Els Kindt, KUL, Lorenz Müller, AXSionics.

Table of Contents

1 Executive Summary

This deliverable is part of the 3rd work package of FIDIS which focuses on high-tech oriented identity technologies. Biometrics is one of these technologies, and has been researched in combination with digital signatures and public key infrastructures (PKIs) in deliverable D3.2: 'A study on PKI and biometrics'. Another deliverable, D3.6: 'Study on ID Documents', concentrated on electronic ID documents, including machine readable travel documents such as the European e-passport, and contained an analysis of the security and privacy aspects of biometrics in combination with e-ID documents. This document builds further on these two reports. It discusses the use and implementation of biometrics from a technical, legal, security and forensic point of view in various applications and schemes in the public and private sphere. It contains also references to D6.1: 'Forensic Implications of Identity Management Systems'.

The report describes in detail the use of biometrics in an authentication process and hereby puts emphasis on the two different comparison functionalities of biometrics, i.e., verification and identification. These functionalities should be properly distinguished and it is shown that an effort for establishing accurate definitions for describing the complex biometric process, such as is presently ongoing in ISO/JTC 1 SC 37, is indispensable for a fruitful debate and understanding of the critical aspects of biometrics. The report further explains in technical detail the biometric capture and extraction process and aims to enhance the discussion about biometric systems by stressing various quality factors, in particular the system errors and failures in relation to both the verification and identification mode. In addition, the limitations of the current definition of quality factors like FAR (False Acceptance Rate) and FRR (False Rejection Rate) are discussed.

The aforementioned technical aspects of biometric systems are not taken into account in the legal treatment of biometrics. The Directive 95/46/EC on data protection does not expressly mention biometric systems as such and the criteria for the processing of biometric data are not clear. The Data Protection Authorities in the national member states retain as a result an important 'margin of appreciation' in allowing specific biometric applications. Analysis of several decisions of national DPA showed that this may even result in conflicting opinions on similar biometric systems. The report further shows, with reference to recent developments in the context of SIS II and the Prüm Treaty, that there is an indication that biometrics may eventually become a primary key within the framework of Justice and Home Affairs in the European Union without an appropriate regulation.

In order to facilitate the research and discussion about biometrics in identity management systems, and building upon previous attempts of classification, this report maps the differences in control, purposes, functionalities and regulation of biometric applications and suggest five types of biometric applications: a government controlled ID model (Type I), an access control model (Type II), a public-private (mixed) model (Type III), a convenience model (Type IV) and a surveillance model (Type V). Each type has different privacy and security concerns and the discussion about biometric applications could become more focused if a system could be classified in the appropriate model. Regulation could then specify which models require most attention and focus their recommendations and rules on a specific type.

The report further illustrates various privacy problems in relation to biometrics and these types, such as the difficulty to meet data quality principles or the fact that not only captured biometric samples but also the biometric templates may contain sensitive information about

someone's health, as no systematic research has been carried out so far with respect to remaining additional information in such templates. The report also includes some new demonstrations and analysis with regard to the user/capture and the capture/extraction threats with commercially available fingerprint scanners. The success of fingerprint spoofs vary from none to high for the tested devices and from the biometric scanners which do not provide for any data encryption, finger print images could be reconstructed.

The report highlights the benefits of biometrics as well, such as that biometrics remain a unique tool to link an individual to the digital world, as evidence in forensics or as a tool to provide enhanced privacy by requiring an additional authentication factor to prevent unlawful access.

It concludes with several recommendations, such as with regard to the template storage and biometric system architecture leading to the concept of encapsulated biometric. An encapsulated biometric system incorporates the full biometric processing in one tamper resistant device which is able to deliver trustworthy but non biometric credentials that proof that the recognition process of the enrolee has been completed successfully.

2 Introduction

2.1 Overview of the document

This report discusses the deployment of biometrics and the various schemes in which automated recognition of individuals based on behavioural and/or biological characteristics is currently used or could in the future be used in identity management systems. The deliverable summarises in chapter 3 several facts about the biometric technology which has been developing at a fast pace over the last decade. Attention is also given to the legal treatment of biometrics, although a thorough analysis of the legal aspects of biometrics will be made in another FIDIS deliverable.[1] In the same chapter, an overview of different types of models of control in biometric systems in combination with possible uses and owners of systems (subsection 3.3) is given and five types of biometric applications are suggested. Such an overview is useful to discuss biometrics in a more focused way because the great variety of applications in which biometrics could be used, from a political, organisational and technical point of view, often blurs the debate about the deployment of biometrics. The risks and advantages of biometrics will to a great extent depend on how, by whom and for what purposes the biometrics are used. Some control models will clearly involve more risks for the privacy of the individuals, while other models and schemes of deployment offer better possibilities to reconcile security and privacy. It is essential that these models and types are identified and that for each model appropriate safeguards are put in place, whether by adding additional security requirements and/or by additional regulation, whichever is most effective.

The document presents in chapter 4 and 5 in essence an evaluation of the strong and weak points of biometrics in relation to the models, with some recommendations. The report, however, does not aim to discuss in an exhaustive way all the security measures which need to be taken or a possible regulation of the use of biometrics. The report will continue by pointing out some critical issues about the use of biometric data which should be further researched, and will conclude with formulating some guidelines and recommendations for the further development and use of biometric technology in an attempt to realise more security while at the same time preserving privacy.

2.2 Review of previous FIDIS findings on biometrics

Biometric systems have been treated as secondary topic in previous FIDIS deliverables which had their main focus on other themes. This deliverable builds upon the findings relating to biometrics in these FIDIS deliverables, in particular D3.2 and D3.6. First of all, basic terminology and biometric methods were introduced in the FIDIS deliverable 3.2, ‘A Study on PKI and Biometrics’. This deliverable also analysed legal principles relevant for the use of biometrics and for the resulting technical and organisational privacy aspects. In the FIDIS deliverable 3.6, ‘Study on ID Documents’, the use of biometrics in the context of Machine Readable Travel Documents (MRTDs) has been analysed with respect to security and privacy. This work also included a description of ISO standards for biometric raw data and templates concerning machine readable travel documents. Readers of this document are hence advised to also consult D3.2 and D3.6 which can be downloaded from the FIDIS website.[2]

[1] See (planned) FIDIS Deliverable 13.4.

[2] www.fidis.net

Both of the aforementioned reports discussed biometrics in a rather specific context, i.e. the use of biometrics in a Public Key Infrastructure (PKI) and the inclusion of biometrics in MRTDs. The aim of this document is to continue and update the analysis made in the previous documents, and to study in depth certain specific aspects of biometrics, such as quality factors of biometrics (in particular biometric system errors) and the uncertainty about health related information contained in biometric systems. It also attempts to place biometrics and its use in a broader context, i.e. in the context of specific public and private applications, from government controlled ID applications to purely private convenience applications, proposing hereby a classification of biometric systems which is useful for further discussions.

This deliverable is also linked with the research on concepts of identity management done in FIDIS. Biometrics are often used for enhancing security and convenience of the authentication and authorisation of individuals, for example, to use a travel document, or to access a building. If we look at the overview of the types of identity management systems as developed in FIDIS deliverable 3.1 'Structured Overview on Prototypes and Concepts of Identity Management Systems', we could reasonably say that biometrics can play a role in all three types of systems. It is likely that biometrics would most often be used in a *Type 1 IMS for account management.* This type of identity management system is designed to enhance the authentication, the authorisation and the accountability of an individual. Behavioural biometrics, i.e. the use of behavioural characteristics in biometric systems which may or may not identify a person and which will not be discussed in depth in this deliverable[3] could probably also be used in a *Type 2 IMS for profiling of user data.* This type of identity management system analyses customer behaviour or supports personalised services to individuals. Finally, as the strict borders between the types of IMS are disappearing, it is correct to say that biometrics will also emerge in a *Type 3 IMS for user-controlled context-dependent role and pseudonym management*. In this type of identity management system, the use of biometrics may protect the access to personal identity assistants and therefore provide a valuable advantage for the individual who seeks privacy protection.

2.3 Biometrics in identity management and the authentication process: basic concepts and major distinctions

By way of introduction into chapter 3, some factors of the authentication process are hereunder recapitulated. It is hereby important to understand not only the basic concepts of the process but also the major distinctions in the functioning of a biometric system. In an *authentication* process, the authenticity of a claim of a person who seeks access to a place or a system is verified against previous information. This previous information may be given to that person, obtained about or obtained from that person. The *verification* of a claim can be done by various means, such as the control of the possession of a key or a token which is handed over to that person or the control of knowledge of an access code (user identifier and password). In general, however, there are three possible factors to authenticate a claim or a person (see figure 1): possession of a credential object, knowledge of a secret and/or a personal information, and an individual biometric feature in the form of a physiological or anatomical attribute or a distinctive behaviour. A biometric factor is fit to be used for verification but it is far more powerful as it enables checking of (mostly) unique biological characteristics submitted by an individual with previous biometric reference data. A biometric

[3] See for behavioural biometrics, M. Gasson, M. Meints, *et al.*, (eds.), *D.3.2. : A study on PKI and biometrics,* FIDIS, 4 July 2005, 82 - 90.

comparison processes the matching of selected features extracted from sets of information based on unique human characteristics. In the process, a decision is made about the probability that the characteristics which are compared belong to the same person. In a verification process, the biometric system recognises and decides that the individual (based on the submitted characteristics) is the same person as the one he claims to be (based on the previously submitted biometric characteristics by that same person). Because biometrics can in principle not be handed out or forgotten, it is believed that biometric recognition will play an increasing role in the authentication processes.

Figure 1: Biometric comparison is one of three possible factors to authenticate a person.

At the same time, the use of biometrics raises concerns. Biometrics mostly involve the use of physiological or behavioural characteristics (or a combination of both) which are *unique* for a specific human being. Biometric data, alone or in combination with other (personal) data, allow identification of a person. Biometrics can reveal directly or indirectly who a person is, even if information such as the name and the place where he/she lives is not stored with the biometric data. A facial image allows identification of a person. The use of a key or of an access code could in principle remain anonymous. A fingerprint image permits through comparison with the fingerprint of a present person or with the fingerprints in a database to identify the person in question. The use of a PIN does not necessarily identify a person. Therefore, biometrics are a very powerful tool, as the data also allow for the *identification* of human beings[4], sometimes even without their knowledge. Because of the identification capabilities, biometric information was initially mainly used for law enforcement purposes. This additional 'quality' of identification ability which is inherent to many biometric characteristics (e.g., fingerprint, iris, voice, etc), however, is now also, with much enthusiasm, investigated by governments for other purposes.[5]

[4] See also Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 8, in which the Article 29 Working Party has made the same observation about the special nature of biometric data as an example of personal data. Biometric data is particular as they not only contain information *about* an individual, but also can be used to establish a link to a person: '(…) As such, they can work as 'identifiers'. Indeed, because of their unique link to a specific individual, biometric data may be used to identify the individual. (…) '.

[5] See, for example, on the use of biometrics by the government (Germany), T. Weichert, 'Staatliche Identifizierung durch Biometrie', *Datenschutz Nachrichten* 2004, vol. 2, 9-19.

In the debate about the use of biometrics in identity management systems, the verification process of the authenticity of a claim has to be clearly distinguished from the identification process. *Identification and verification are in fact two completely different processes* and are also different functions performed by a biometric system. Biometric authentication by verification, in the sense of a process of establishing confidence in the truth of a claim (a claim is for example, "I am entitled to enter these premises" and "this entrance card has been issued to me"), is a verification of one submitted item of information against one given item of information and does not necessarily involve identification of that person. Authentication in this meaning of a one to one (1:1) biometric verification could also be effectuated with non-identification techniques, such as the testing of knowledge belonging to that person, (e.g., a pin code attached to the card) or location of that person, or verification of the possession of a particular item issued to that person, such as a smart card with biometrics, and verification that the biometrics stored on that card stem from the submitted biometrics. In other words, the identification ability of biometrics is in principle not necessary to be used in a 'simple' authentication process. However, upon the collection and the use of biometric characteristics, depending on the design and the use of a central database, both functions of identification and of verification often co-exist and the various schemes in which biometrics are used, often do not clearly indicate which functionality is used. This is also indicated in the overview of models and types stated *infra* in section 3.3.

The *identification ability* of biometrics, including the fact that once unique human characteristics (such as fingerprints) are compromised (e.g., stolen) it is not possible for the individual concerned to adopt new human characteristics, *brings on many concerns*. In the context of discussions about the protection of privacy and biometrics, the risks of function creep and non-respect for the data minimisation principle (amongst other things) are often mentioned. We believe that these concerns relate principally to the identification functionality of biometrics, which go beyond the authentication purposes for which the biometrics might be used in a particular application.

Because in an authentication process, it can also be verified that someone is the person he/she claims to be, the terms authentication, verification and identification and their meaning in the biometric comparison process are often used together or confused. This does not facilitate the debate about the deployment of biometrics. It is therefore very important to distinguish the two functionalities of the biometric comparison process in the discussions about its use and risks and crucial that due attention is paid to terminology and vocabulary. We will see below that during the standardisation activities on biometric vocabulary, the term *'authentication'*, which is still often used as a synonym for verification has become *depreciated* and that consensus grows that in discussions about the deployment of biometrics the term should be replaced by the term 'verification' (see *infra*, section 3.1). We should therefore speak in general of a biometric comparison which can be used in a verification or identification mode .

In this context, it is also important to be clear with the notion of 'identity', 'identification' and 'identifiability'. 'Identity' is in general often understood as referring to the identification details of a person, as registered at the time of birth by a civil servant in a population register (in civil law countries) and consisting of a set of information such as name, date and place of birth, address, name of mother/father etc about that person ('civil identity'). 'Identification' and 'identifiability' would then be understood as the possibility to link a person through his

biometric characteristics with this 'civil identity', as registered and known to the government. Private and commercial parties also know and use this 'official' information of persons in a variety of applications. It is primarily this meaning of identification that is by most people considered a risk in the discussion about biometrics. Practically speaking, this identification would require a database in which unique biometric characteristics are combined or linked with other identifying information about the 'civil' identity, such as name and address. Such a central register is exactly what several governments intend to establish, for example in the United Kingdom.

'Identity', however, could also be defined in other ways. In the context of identity management research, identity is sometimes defined as '*any subset of attributes of an individual which identifies this individual within any set of individuals*'.[6] According to this definition and understanding, there is no such thing as "the identity" of one person, and one person may have several 'identities'. 'Identifiability' is then 'the state of being identifiable within a set of subjects (…)'.[7] Taking into account this approach of identity, biometrics could also be used to identify an individual within a group of subjects, but without necessarily referring to the 'civil identity'. The identification ability of biometrics will then only be used to identify an individual within a group (one to many (1:N) comparison), without other information such as name. This does, however, not solve all problems as this would still require a central storage of the biometric data (but without name or a direct link to a database with names). First of all, biometrics could be deployed as unique identifiers and therefore could be easily linked with other information databases using or containing the same biometric identifier. Secondly, even if the possibility of using the biometric data as a unique identifier would be overcome, the collection and storage of biometric data in a central database will always mean that there remains a risk that the biometric information is sooner or later linked to other identity information which could ultimately identify a person (e.g., manual comparison). It has already been recognised that the collection of biometric information in large-scale databases[8], sometimes with not only a central control but with a control by several parties/governments without appropriate agreements (multilateral control, see also the models described *infra*, section 3.3 and Annex 2), is a major fear and risk.

For that reason, identification and the storage of biometric characteristics in central databases are two concepts that are linked to each other and that, in respect for the rights and freedoms of individuals, need to be considered with utmost care. The deployment of biometrics, however, does not necessarily require that the identification functionality and central storage are used. This deliverable aims to, in addition to giving a description of the risks and the advantages of identity recognition through biometric comparison, clarify in which models identification or verification is used. The models which are described in section 3.3 were developed because of an apparent need to have an overview of the use of biometrics in various applications.[9] The models are developed on the basis of a review of some existing

---

[6] A. Pfitzmann and M. Hansen, *Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v.0.23*, 25 August 2005, 20. The most recent version is v.30 of 26 November 2007 and is available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[7] *Ibid*., 20.

[8] See Article 29 Data Protection Working Party, *Working document on biometrics*, 1 August 2003 (WP 80).

[9] See also for example the attempt made by the National Consultative Ethics Committee For Health And Life Sciences in France in its recent *Opinion N° 98. Biometrics, identifying data and human rights*, 26 April 2007, 7.

suggestions (by AFNOR and BioVision) to classify biometric systems and on the basis of newly suggested consistent classification criteria which are in our view relevant. These classification criteria are (1) the way control is exercised (central, divided or multilateral), (2) the controller (public or private entity) and (3) the purpose(s) (combating identity fraud, securing online or offline access, mixed purposes of public and private entities, convenience purposes and surveillance) of the applications. Such 'grouping' of biometric applications on the basis of applications which are often cited or reported around these criteria should facilitate a common understanding of the risks and advantages and simplify a discussion about the use of biometrics. Medical biometric applications, however, have not been taken into consideration when defining the models, as such applications are evolving very fast in the e-health domain and require specific attention and review.

3 Facts and findings on biometric systems

3.1 Definitions and state of the art in biometrics

3.1.1 Definitions of biometric terms

The process of involving biometric characteristics in an authentication application is quite complex. A common vocabulary for the components and the functions of a biometric application is currently being discussed and developed which is useful as the terminology used is often very confusing. In Working Group 1 of Subcommittee 37 of the Joint Technical Committee 1 of the International Standardisation Organisation (ISO), work has been done on the harmonisation of terms that parties, whether users or developers, use in the field of biometrics. This process has lead to a public list of terms to be used in the field of biometrics.[10] This process is still ongoing. Other organisations have also suggested and published definitions for terms to be used in biometrics (such as the Biometrics Application Programming Interface standard (BioAPI) consortium). A compact and practical compilation can be found for example on the CESG-Homepage (National Technical Authority for Information Assurance, UK)[11] which has also been adopted by the Common Criteria Biometric Evaluation Methodology Working Group.[12] A few of the proposed terms of the Draft Harmonized Biometric Vocabulary and of the terms found on the CESG-homepage which are relevant for this report are mentioned in the glossary of this deliverable. Some important basic notions of biometrics are further discussed below.

The development of a vocabulary and common definitions for biometric systems is extremely important but also difficult because of the diverse understanding of common terms. From the current draft document of ISO, it should be noted that certain terminology is depreciated. For example, the terms 'positive identification' and 'authentication' are depreciated.[13] At this time, it is recommended that 'authentication' is used with care because it may create confusion as authentication has been used to indicate two completely different biometric functionalities, as explained in the previous chapter, i.e., it has been used to refer to not only the verification function (1:1) (one-to-one) of a biometric application but also to the identification function (1:N or N:1) (one-to-many or many-to-one).[14] While these two

---

[10] See Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 37, Biometrics. Standing Document 2 version 7, - Harmonized Biometric Vocabulary, 12 February 2007, a working document available at http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2299802/JTC001-SC37-N-1978.pdf?nodeid=6181365&vernum=1 (last visited on 29 June 2007) and version 8 of 22 August 2008 available at http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263033/2299739/JTC001-SC37-N-SD_2_version_8.pdf?nodeid=6714484&vernum=0 ((last visited on 30 August 2007) (hereinafter 'Draft Harmonized Biometric Vocabulary v. 2.7). An extract of the terms of a previous version is available at http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&ob jAction=browse&sort=name (last visited on 29 June 2007).

[11] UK Government's National Technical Authority for Information Assurance, available at http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=401

[12] Common Criteria Biometric Evaluation Methodology Working Group, Version 1.0, August 2002, available at http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

[13] See Draft Harmonized Biometric Vocabulary v. 2.7, p. 9 and v. 2.8, p. 9.

[14] Draft Harmonized Biometric Vocabulary v. 2.7, p.16, 3.5.2.

functionalities are completely different, including in terms of the place where the references should be stored, there grows a consensus that the appropriate terms for these functionalities should be used, i.e., *'identification' for an 1:N comparison and 'verification' for a 1:1 comparison*, and not the general term 'authentication'.

'Positive identification' is another example of a misleading term, as it refers in principle not to a 1:N comparison, but to a 1:1 verification comparison.[15]

It should be noted that the term 'identification' in this proposed ISO vocabulary is limited in its meaning as it (only) refers to a 1:N comparison of the submitted biometric sample against stored biometric reference templates to determine any comparison score or a N:1 comparison of a biometric reference template to multiple samples collected from individuals (mainly in forensic applications). In that sense, it only permits distinguishing a subject amongst a set of other subjects.[16] Identification is hence used not in the sense that it will necessarily also reveal the 'civil' identity of the subject (see above). This will only be possible if such other identifying information, such as for example name and birthday, are stored together with or could be linked to the biometric information. The identification function therefore does not necessarily refers to the 'civil' identity but it may do so. The proposed terminology was not always clear in that respect. The term 'verification' was defined in a previous draft of the Harmonized Biometric Vocabulary document as a *'one-to-one process of comparing a submitted biometric sample (…) against the biometric reference template (…) of a single enrolee (…) whose identity is being claimed, to determine whether it matches the enrolee's template'. Contrast with identification (…).*[17] Identity in this definition, however, was misleading as it is not necessarily 'civil' identity, but could be any other attribute of an individual which identifies him (e.g., being employee of company X who requests access to the premises). This was later clarified in the proposed vocabulary in the ongoing standardisation work by deleting the reference to 'identity' in the definition of verification. This will certainly help the public to distinguish the functions of verification and identification of biometrics properly.

It is therefore very important that this work on biometric vocabulary is continued in order to clear out misunderstanding of biometric applications and their functionalities. Agreed terminology should also where possible be used in any discussion on biometrics.

3.1.2 Reference model of a biometric system

In most cases a biometric system is embedded in the authentication process of an identity management system. Its result is used to decide if the individual that has delivered the biometric data shall be recognised by the identity management system. A biometric system may be used in two modes:

- **Verification mode**: An individual makes a(n identity) claim. The biometric system compares the captured biometric data sample with the biometric reference template

[15] See Draft Harmonized Biometric Vocabulary v. 2.7, p. 17, 3.5.9.

[16] See Draft Harmonized Biometric Vocabulary v. 2.8, p. 9, 3.2.4.1.2 defining 'biometric identification' as system function and the note mentioned with it: 'A biometric identification function may be used to verify a claim of enrolment in an enrolment database without a specified biometric reference identifier'.

[17] See Joint Technical Committee ISO/IEC JTC 1, Subcommittee SC 37, Biometric Vocabulary. N 460 Standing Document 2, 2004 (which was a previous version of the current working document), term 1.2.10.

that corresponds to the claim(ed identity). The outcome is the acceptance or the refusal of the (identity) claim.

- **Identification mode**: The biometric system compares the captured biometric data sample with all available biometric reference templates. All comparisons with a sufficient similarity to a stored reference template are selected and designate a candidate identity. The outcome is a list of identities that may belong to the individual. This list may contain zero, one or more entries. Individuals may be identified in this mode with or without their consent.

All biometric systems have some common main functional components in a typical processing chain. These components are (see *below*, figure 2):

- a storage entity with the biometric data samples (reference templates) of the enrolled individuals that is linked to or integrated in a database with the identity information of the corresponding individuals
- a sensor device and some pre-processing to capture the biometric data sample from an individual as input data
- a comparison process that evaluates the similarity between the reference templates and the captured data sample and that results in a similarity score and
- a decision function that decides if a data sample matches to a certain reference template.

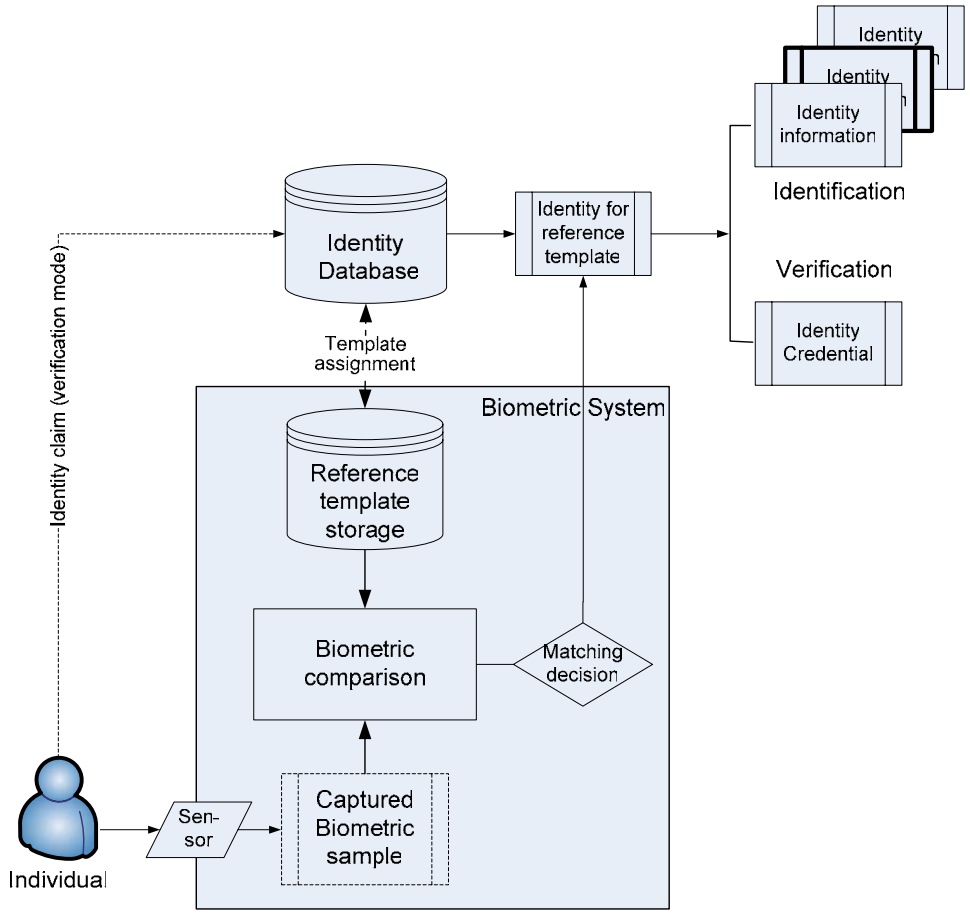

Figure 2: The main processing components of a biometric system

These components are described in a more detailed form by different standardisation organisations like the Common Criteria BEM Working group (CC-BEM) or the BioAPI Consortium (BioAPI). Although all use slightly different terminologies and description models, a common picture evolves for the description of a reference model of a biometric system.[18] The main functional components are hereunder described and are adopted from CC-BEM:

Delivery – Protocol that an individual follows (knowingly or unknowingly) to provide a signal of a biological and/or behavioural characteristic to the biometric application system

Capture – Acquisition of a biometric sample data from the original biometric characteristics of the individual with appropriate sensors (capture devices)

Extract – Conversion of the captured biometric sample data to an intermediate form that contains the concentrated distinguishing biometric property information of the biometric characteristics.

Create Template – Conversion of the intermediate data into an individual's template that can be stored (reference template) or that can be used as input (query template from sample data) for a comparison process that uses previously stored reference templates.

Compare – Comparison and matching of the query template with the information in a stored reference template.

Recognise – Mapping of the recognised query templates on the identity data of the individuals that are stored in the system (identification mode) or acceptance of an identity claim of a specific individual and delivery of a corresponding identity credential (verification mode).

All biometric systems run in two separate processing phases. For each individual that shall be recognised by a biometric system first an initialisation, called enrolment, takes place. In this processing phase the individual subject provides samples of a biometric characteristic to establish a new so called reference template. After the enrolment, the subject is known by the biometric system. In the subsequent query phase, the subject provides a new sample called query template that is processed and compared with the saved reference templates of all enrolled subjects (identification) or with the saved template of a specified subject (verification). The output of the system may be a simple yes/no, or an identity credential with identity information about the subject for a system that operates in the verification mode, or a list of identity data that correspond to the best matches (comparison scores) for a system running in an identification mode.

A schematic model of all processing steps in a biometric system with inputs and outputs is shown in figure 3. The red track represents the enrolment mode and the green track the query phase processing. The two different recognition modes (verification of a biometric sample with claimed identity; identification through a mapping of a biometric sample to potential

[18] See also R. Veldhuis, *The Biometric Experience - From pattern recognition to biometrics*, presentation at the 2nd Smart University, 21 September 2006, Sophia Antipolis, France.

candidate reference templates) are distinguished by the additional 'identity claim' input in the recognition step.

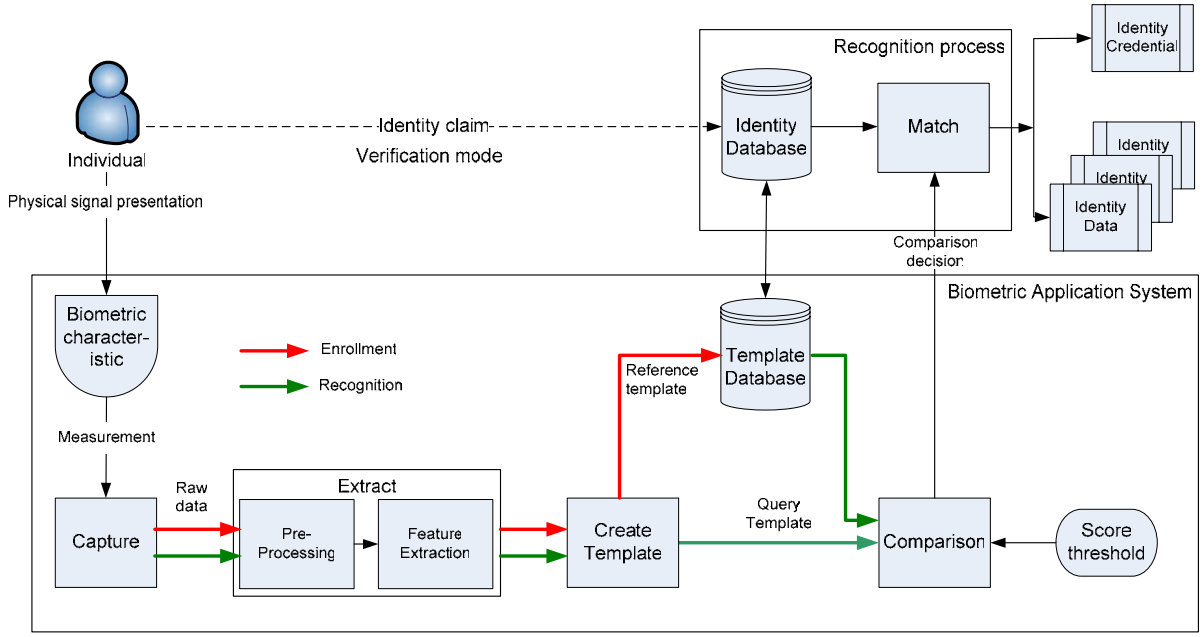

Figure 3: Schematic representation of the processing steps of a biometric system. The processing for the two phases (enrolment, comparison) follow two different flow paths.

The reference diagram presents a simplified logical model of a general biometric application system. The biometric data inside the functional chain may be formatted and tagged in a standardised way generically termed as a Biometric Identification Record (BIR) (BioAPI). A real implementation could be complicated by additional factors such as the following:

a) The requirement for confidentiality and integrity of the biometric and user identity data and of the transmission paths between components and involved systems. These paths may be protected by cryptographic mechanisms or other means, e.g. physical access control. Unique session keys may also be used to counter replay attacks.
b) The system may be distributed over multiple locations, such as in a client server architecture.
c) The system may be under the control of different instances such as the user, the operator, a trusted third party or a governmental organisation. Such instances may control different parts of the processing chain in various combinations (see discussion below about the different control types and models, such as central control, divided control with trust and multilateral control).

Delivery

The delivery protocol includes all organisational and technical support procedures and all explicit or implicit action steps to enable the biometric capture process. Actions are needed to guarantee that only intended subjects are enrolled in the system and that the deposited biometric characteristic belongs to the subject that is supposed to deliver the physical signal. Part of the delivery setup is dedicated to support the measuring process of the capture device through appropriate supply of technical and formal user guidance. For example, in a

fingerprint recognition system the delivery process has to provide the centre part of the fingerprint onto the capture device to ensure the maximum number of characteristic features of the print. For facial recognition systems, some require the subject to be in a standard position directly facing the capture device. For other devices, other criteria and procedures for the delivery must be clearly defined to ensure a standard, repeatable capture process.

Capture
This component includes both enrolment capture and recognition capture for comparison. It is defined as the automatic capture or measurement of the physiological or behavioural characteristic(s) of an individual. This component may include processes that enhance the quality of the acquired sample, such as user interface (UI) feedback or using a number of acquisitions to produce the sample. Each capture device type will have certain criteria and procedures defined for a valid delivery process, both for enrolment and for recognition data samples. The capture process includes two steps: the presentation and the attempt. Presentation means that the physical signal is delivered to the capture device. Attempt means that the capture device could record and evaluate the physical signal to generate a raw data sample. The output of the *capture* component is the raw data *biometric sample* ready for the processing in the extraction step.

Extract
This component includes two processing steps. The pre-processing enhances the quality, masks the usable sectors of the biometric sample data, expands and transforms the raw sample data in an appropriate way to allow the subsequent feature extraction step. The feature extraction procedures identify and preserve the distinct and repeatable biometric features from the raw data sample. This component is critical from a security evaluation point of view, since the level of uniqueness inherent in a template will influence the False Match Rate of the system.
The *extract* component is generally a proprietary algorithm. Inherent in this algorithm is quality control, wherein through some mechanism, the sample is rated for quality. If the quality is not acceptable, the *capture* process may be repeated. A failure in one of the two capture or extract steps contribute to the *failure to acquire* (FTA) rate. The FTA rate is the relative frequency that either the capture or the extract process could not complete its task in a sufficient quality.
Quality standards of the captured biometric are expected to be high during enrolment, since this forms the basis against which all further biometric comparisons are made. Repeated attempts may be required during enrolment to have the best biometric samples as reference.
The output of the extraction component is the *biometric features* that serve as building elements for the biometric template.

In figure 4, the change of the transformation of the biometric data through these first three processing steps are illustrated for a fingerprint recognition system. The delivery protocol provides the right biometric characteristics of an individual fingerprint, the capture step provides the captured biometric data of the measurement process and the extraction runs several processing steps to mask useful regions of the captured data, to enhance the quality and to extract the features which will be used in the subsequent template creation step.

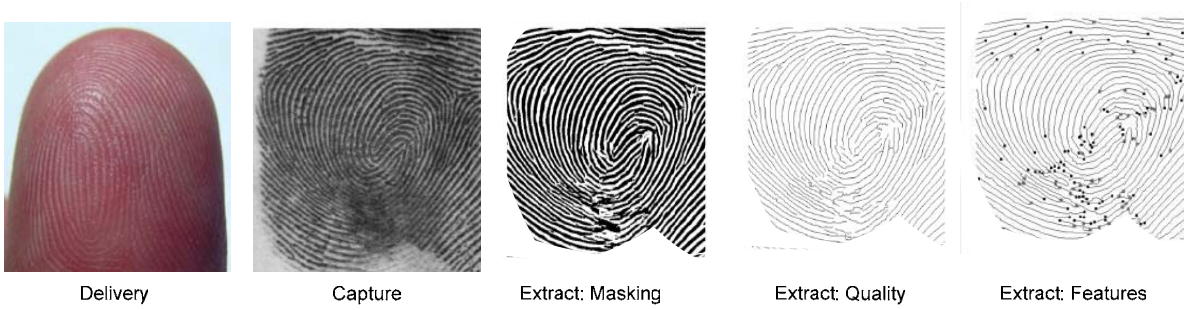

Figure 4: Illustration of the first three processing steps in a fingerprint recognition system (pictures from BSI-Bericht: Evaluierung biometrischer Systeme, 2005).

Create Template

This component creates the biometric template from the output of the extraction process. It may include meta-information about the format and the type of the biometric data, encryption of the biometric data, or digital signing of the biometric identification record (BIR) (See the BioAPI and CBEFF standards documents. In the enrolment phase, the output of the create template component is the reference template. During a biometric identification or verification process, the output is the so called sample or query template used for the comparison step. Normally, the reference and the query templates contain a reduced set of distinctive feature data relative to the recorded raw sample data. In general, it is not possible to reconstruct the original biometric raw data sample from the template data. However, the huge data reduction makes templates vulnerable to attacks of impostors who try to find other biometric raw data sets that lead to approximately similar templates.

Figure 5 *below* shows the representation of the extracted features within a fingerprint recognition system. On the left side, one sees the extracted features (in this case so called minutia points represented as red points) overlaid on the quality enhanced fingerprint picture. On the right side, these points are represented in their digital form as a list of point data with coordinates, local ridge direction, quality and type information. This list represents the biometric reference template for the specific fingerprint recognition system and illustrates the huge data reduction of a typical feature extraction step.

min_T.txt

```
 1
 2  33 Minutiae Detected
 3
 4     0 :   18,   84 : 13 :  0.12 :BIF
 5     1 :   22,   41 : 16 :  0.13 :RIG
 6     2 :   25,  127 : 26 :  0.28 :BIF
 7     3 :   27,   67 : 29 :  0.58 :RIG
 8     4 :   39,   26 : 17 :  0.12 :RIG
 9     5 :   45,  157 : 25 :  0.12 :BIF
10     6 :   52,   40 : 16 :  0.29 :RIG
11     7 :   54,   28 :  2 :  0.29 :RIG
12     8 :   55,   63 : 29 :  0.30 :RIG
13     9 :   61,   80 : 27 :  0.30 :RIG
14    10 :   65,  177 : 23 :  0.12 :BIF
15    11 :   78,   41 : 14 :  0.13 :RIG
16    12 :   80,   73 : 25 :  0.29 :RIG
17    13 :   82,   37 : 11 :  0.29 :BIF
18    14 :   82,  102 : 23 :  0.29 :BIF
19    15 :   83,   65 : 29 :  0.12 :BIF
20    16 :   83,   76 : 26 :  0.29 :BIF
21    17 :  105,  152 : 21 :  0.62 :RIG
22    18 :  107,   25 : 28 :  0.31 :RIG
23    19 :  110,   83 : 19 :  0.29 :RIG
24    20 :  110,  108 : 20 :  0.29 :RIG
25    21 :  113,   41 : 14 :  0.58 :BIF
26    22 :  132,  161 : 20 :  0.60 :BIF
27    23 :  136,  104 : 18 :  0.59 :RIG
28    24 :  145,  168 :  4 :  0.60 :RIG
29    25 :  156,   71 : 16 :  0.59 :BIF
30    26 :  171,  160 : 19 :  0.57 :RIG
31    27 :  173,  184 : 19 :  0.12 :RIG
32    28 :  175,  210 :  4 :  0.06 :RIG
33    29 :  175,  212 :  4 :  0.06 :BIF
34    30 :  214,   98 : 16 :  0.58 :BIF
35    31 :  249,   77 :  0 :  0.59 :BIF
36    32 :  273,  179 :  1 :  0.06 :RIG
37
```

Figure 5: Illustration of the feature extraction step of a fingerprint recognition system. On the left side the extracted features (in this case so called minutia points) are overlaid as red points on the quality enhanced fingerprint picture. On the right side these points are listed as feature vector. This list represents the biometric reference template.

Interoperability between different biometric systems that look at the same biometrics may be achieved after the template creation step. The template may be represented in a standardised form that allows the further processing by another biometric system that uses the same feature vector representation conventions. Such a standard form including the according metadata for interoperability, called Biometric Identification Record (BIR), has been defined in the BIOAPI standard. The structure of a BIR record is shown in figure 6 *below*. The expanded header includes the additional information that allows the use of the templates across different systems.

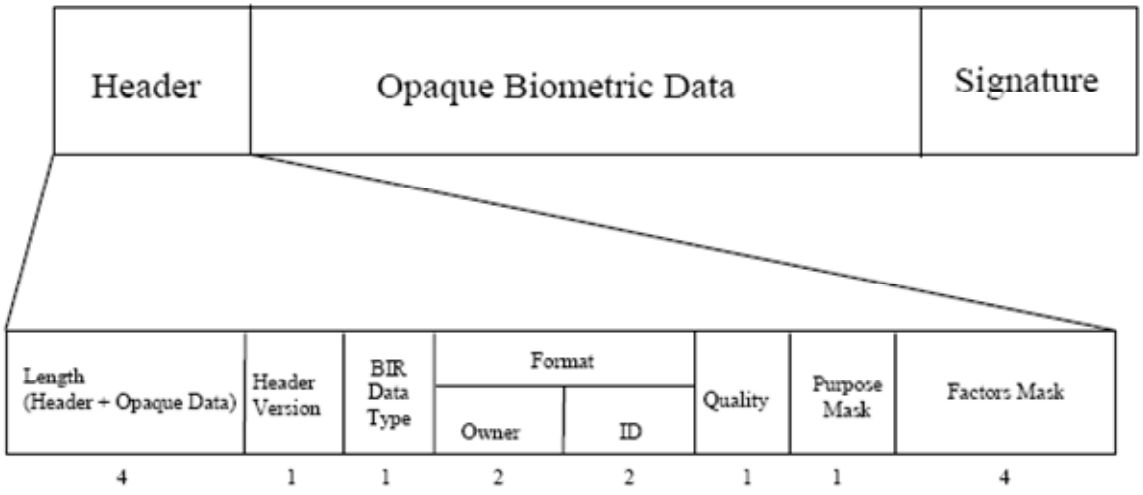

Figure 6: Schematic representation of the Biometric Identification Record (BIR) defined in the BIOAPI standard with the expanded header that contains the meta-information to use the biometric data across different systems.

Compare

This component compares the biometric information extracted from the sample (query template) with the biometric information in the reference template. It will typically result in a matching score which is a measure of the correspondence of the two templates.

The comparison may be against a single template (for *verification*), or against a list of candidate templates (for *identification*). The distribution of score parameters coming from comparisons of templates from the same biometric characteristics and the corresponding score parameter distribution coming from comparisons between templates from different characteristics (same or different individuals) defines the separation capability of a biometric system. In the ideal case, the two distributions do not have any overlap region. In reality, most of the biometric systems deliver score parameter distributions for corresponding and non corresponding templates that have a more or less important overlap region. The two distributions then will be separated by the so called score threshold value. The choice of this value determines the security (discrimination against casual impostors) and the conveniences (rejection of enrolee) of the specific biometric system.

Recognise

The recognition step typically includes a comparison of a matching score with a predefined threshold value. The comparison may be against a single template (for *verification*), or against a list of candidate templates (for *identification*). The output is a decision about acceptance or rejection of a claimant (verification mode) or a list of candidates (identification mode).

The threshold may be configurable by the administrator, or it may be fixed by the biometric system. Clearly, the security assurances relating to the setting of this value, the protective means within the biometric system to safeguard the threshold setting, and the internal decision process to decide a match are some of the most critical components of a biometric system and their vulnerabilities should be carefully assessed.

When the biometric verification process is successful, identity credentials and other data may be released from the identity database or the BIR. The decision whether to accept or reject the

subject as an authorised individual may need further evidence, e.g. a username, PIN or token. For multimodal biometric systems, decisions may depend on a compound score valuation based on the results of the comparison process for more than one biometric characteristic.

3.1.3 Quality factors of biometric systems

Several physiological and/or behavioural characteristics are apt to serve as a biometric identifier to recognise a human subject. Such identifying characteristics however have to fulfil some mandatory and some desirable qualities.

Mandatory qualities of a biometric characteristic:

- Universality - each individual has the biometric characteristic and can become a biometric capture subject
- Distinctiveness – any two individuals have sufficiently distinct biometric characteristic to be separable by suitable extracted biometric features
- Permanence – the biometric characteristic must be sufficiently invariant over a longer time period
- Collect ability – the biometric characteristic can be measured through the evaluation of emitted physical signals

Desired qualities of a biometric characteristic:

- Performance – the measurement of the biometric characteristic is robust, fast, accurate and efficient
- Acceptance – the delivery of the biometric characteristic is well accepted by the individuals which are biometric capture subjects
- Reliability – the biometric characteristic is not easy to forge and the delivery not easy to circumvent by fooling the system

For practical implementations, the following additional considerations have to be taken into account:

- The size of the population that has to be enrolled in the biometric system
- The biometric application mode, identification or verification
- The control scheme of the biometric system components (see below, section 3.3)
- The environment for the different processing steps (delivery, capture, extraction, template creation and comparison and match)
- The purpose of the biometric system relative to the security policy

- The proportionality of the recognition and data collecting process relative to the intended transaction
- The organisational integration in the superordinated identity management system
- The ergonomic integration of the biometric delivery process in the authentication protocol of the authorised users to find long term acceptance of the user
- The costs and the requirements on the infrastructure

3.1.4 Biometric system errors

Any biometric processing system utilises a physical measurement step which is intrinsically error prone. The systematic and statistical errors of the measurement and the algorithms of the biometric extraction and comparison processes define the limits of application of the biometric system and the separation capability between different individuals. Each biometric template measurement of an individual represents a point in the phase space of the biometric feature vectors. The separation capability of a biometric system depends on the distribution of these points in the feature phase space. If points representing templates from one individual are clustered in a narrow region that is typically far away from all other clusters of different individuals the separation capability of the system is high and the error rates are low. On the contrary, if the clusters are large and overlapping, the separation capability is low and there are errors of the first (false non recognition) and second kind (false recognition). There are various reasons for such an overlapping of template clusters in the feature vector space. It is possible that the biometric identifier characteristic is not very distinctive or has a natural variation from measurement to measurement, e.g. voice or planar signatures are examples of such biometric identifiers with low separation capability. It is also possible that the measurement and feature extracting processes are poor or oversimplified and reduce a high dimensional feature vector to a few components with a much poorer separation capability. Early commercial fingerprint and many face recognition systems are examples of such oversimplified systems. A third reason for system deterioration comes from the scaling of centralised systems to large populations. If a central database collects so many reference templates that the cluster region of each individual heavily overlaps with the regions of other individuals the system will no more work in the identification mode and becomes susceptible to impostor attacks even in the verification mode.

Figure 7 *below* illustrates this problem. The representation of 3-D feature vector phase space for a biometric system is filled on the left side with the points of the reference templates of a given population. Each point represents a measured reference template of an individual. On the right side the lines represent the measured distance of the feature vectors between the reference templates and a corresponding query template (one endpoint represents the reference template, the other endpoint represents the query template in the same phase space). The lengths of the straight lines are an indicator of the typical cluster size of the feature vectors distribution from one biometric characteristic of an individual in the population. It is clear that this example would not lead to a good biometric classifier as the clusters are heavily overlapping between individuals. The specific system comes from an oversimplified fingerprint recognition system and it was selected for the illustration of the scaling problem.

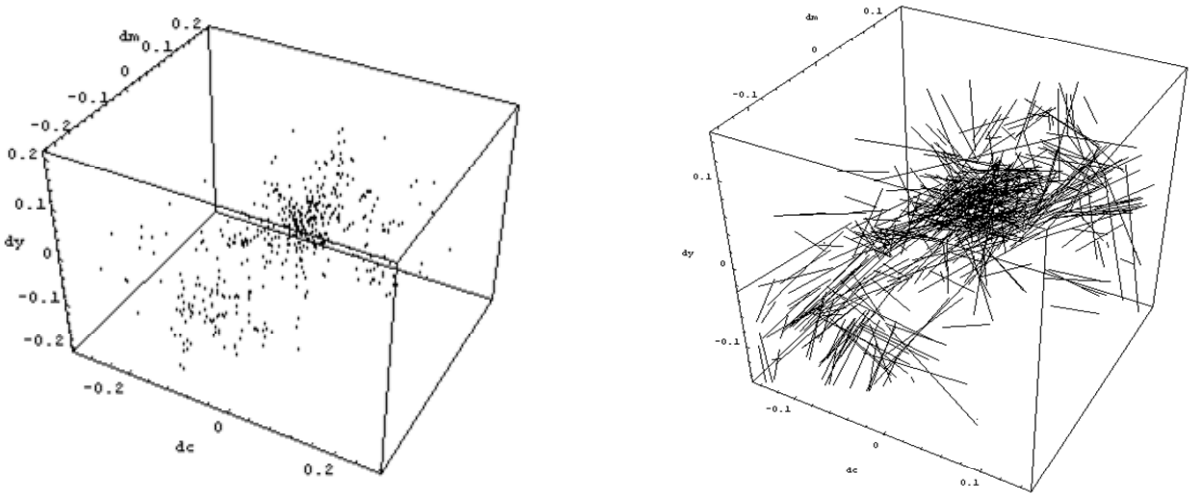

Figure 7: Distribution of reference feature vector points in a 3-D feature phase space (left side) and connection lines between the reference and a set of corresponding query vectors (right side). The length of the lines are indicators for the typical cluster size of feature vectors of one subject in the phase space. The example shows a biometric system with insufficient separation capability for the chosen population.

The scaling problem becomes especially serious in applications with non cooperative individuals where the system should provide the evidence of false identity claims or attempts of individuals for multiple enrolments under different identities. The scaling problem can be solved by an appropriate conceptual architecture of the biometric system. It is evident that the overlap problem can be reduced by the reduction of the number of reference templates that have to be recognised. In the ideal case, the biometric system has only to recognise query templates coming from one single individual and therefore only one reference template has been stored in the template storage. The acceptance region in the feature space around the point defined by the single stored reference template can then be tuned in an optimal way to this reduced problem. This architecture is realised within the concept of the so called encapsulated biometrics where each individual carries a personal identity assistant device which has a full biometric system integrated in it. Such a system will be presented in planned FIDIS D3.14.

The multiple enrolment problem can be reduced by the use of multimodal biometrics. If the system detects an overlap of newly delivered reference templates of different and independent biometric characteristics with already registered reference templates of one single enrolee, it is very likely that the new claimed identities is claimed by the same person that already has enrolled under a different identity.

Biometric system failures

In addition to the system errors with false results of the recognition process, there are system failures where the biometric system is unable to process the biometric data. If such a failure happens in the initial, enrolment, mode, we speak of a failure to enrol (FTE), if such a failure happens in a query process we speak of failure to acquire (FTA) or failure to capture (FTC).

For a clear definition of theses failure notions, we have to break down the biometric processing in three hierarchical steps:

- Presentation
  A presentation is the interaction of an individual with the capture component of the biometric system. One or more presentations may be necessary or permitted to constitute an attempt to deposit a template. In a typical decision policy, failure to acquire the biometric data sufficient to constitute an attempt after a certain number of presentations represents a failed attempt.
- Attempt
  An attempt is the presentation of a biometric identifier and the capture of the biometric data for the preprocessing, feature extraction and template generation step. One or more attempts may be necessary or permitted to constitute a biometric transaction, depending on whether the system requires or allows multiple sample templates of a biometric identifier characteristic. In a typical decision policy, an inability to enrol or match a template subsequent to a certain number of attempts constitutes a failed transaction.
- Transaction
  A transaction is the successful completion of a biometric processing step either in the enrolment or in the query mode. A biometric recognition may consist of one or several biometric transactions using a certain biometric identifier characteristic. The inability to complete a biometric transaction leads to the two following failure types:

  - FTE – Failure to enrol

    The FTE is defined as the probability that an individual attempting to enrol in the biometric system is unable to succeed. Inability means that the individual exhausted the maximum number of presentations and/or attempts without succeeding to realise the requested number of transactions for a successful definition of a valid reference template.

  - FTA (FTC, FTM) – Failure To Acquire (Failure To Capture or Failure to Match)

    The FTA (FTC, FTM) is defined as the probability that an individual attempting to pass a recognition step in the biometric system is unable to deliver a query template for the regular running of the comparison step. Inability means that the individual exhausted the maximum number of presentations and/or attempts without succeeding to realise the requested number of transactions for a successful definition of a query template with sufficient distinctive features to run a comparison step (FTC) or that the comparison step fails for some reason without delivering a correct matching score (FTM).

The two failure rates are not necessary equal and for each individual there are specific failure rates:

$$FTE(i) = \frac{\#\ failed\ enrol\ transactions}{\#\ all\ enrol\ transactions}; \quad FTA(i) = \frac{\#\ failed\ query\ transactions}{\#\ all\ query\ transactions}$$

The corresponding values over a population are the averages over the individual values for FTE and FTA over the population in question. The failure rates are in principle not dependent on the operation mode. An identification process as well as a verification process both need valid reference and query templates. However, the design of a verification and an identification system may lead to different definitions of what a valid template is, which in turn influences the failure rates.

Statistical measurement errors

A typical response of a biometric system in a template comparison step is a so called matching score S, which is a measure of the correspondence between the two templates. The matching score is compared with a recognition threshold T to decide if two templates originate from the same biometric characteristic or not. If S >= T (assuming an ascending matching score with a better correspondence between the two templates) the templates are considered as matching templates, if S < T the two templates are considered as non matching templates. It is clear that the choice of the threshold T is critical for the rate of false non matching of two templates coming from the same biometric characteristic (error of the first kind I) or the rate of false matching of two templates that come from different biometric characteristics (error of the second kind II). Expressing this in a more formal way with the stored reference template R and the acquired query template Q, the null and the alternate hypothesis are:

- $H_0 : Q = R$ query template does come from the same biometric characteristic as the reference template
- $H_1 : Q \neq R$ query template does not come from the same biometric characteristic as the reference template

And accordingly the associated decisions are

- D_0 : query template does come from the same biometric characteristic (same person) than the reference template
- D_1 : query template does not come from the same biometric characteristic than the reference template

The errors are of type I when the decision D_1 is taken when H_0 is true and of type II when the decision is D_0 when H_1 is true.

Figure 8 *below* shows typical distributions of the score parameters of comparisons between reference and query templates coming from the same biometric characteristic of the same subject (green distribution) and such coming from different subjects (red line) The green field to the left of the threshold value T represents the total False Non Match Rate (FNMR) due to errors of the first kind and the red field to the right of the threshold value represents the total False Match Rate (FMR) due to errors of the second kind. The two points (ZFR, ZFA) on the score parameter axis design the critical score parameters below which the FNMR becomes zero (ZFR) and above which the FMR becomes zero (ZFA).

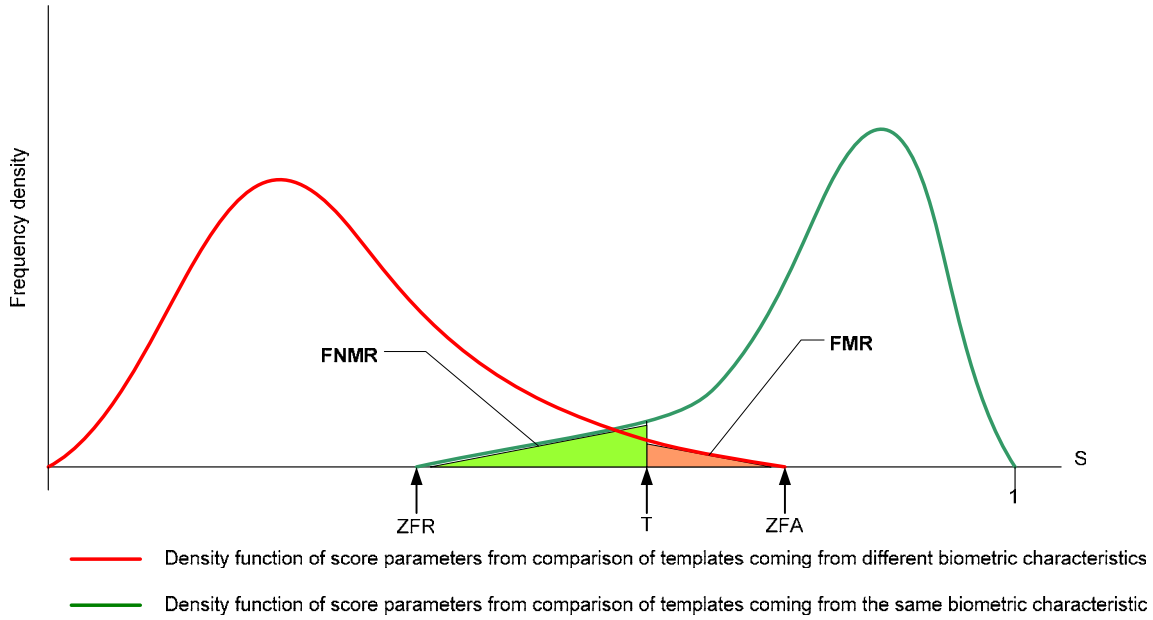

Figure 8: Typical distributions of the score parameters of comparison between templates coming from the same biometric characteristic of a subject (green line) and such coming from biometric characteristics of different subjects (red line).

The matching process delivers a matching score S= S(Q,R) which we assume to be normalised to the interval [0,1] with a perfect match for the value S=1. This leads to the following error notions which are slightly different for the verification and the identification mode.

Errors in the verification mode

FMR – False Match Rate

$$FMR(T) = \int_{T}^{1} p(S \mid H_1 \, is \, true)\, dS$$

Total probability that the calculated matching score exceeds the threshold value T although the two templates do not come from the same biometrics.

FNMR – False Non Match Rate

$$FNMR(T) = \int_{0}^{T} p(S \mid H_0 \, is \, true)\, dS$$

Total probability that the calculated matching score is below the threshold value T although the two templates come from the same biometrics.

Zero FMR

$$ZeroFMR = \int_{ZFA}^{1} p(S \mid H_1 \, is \, true)\, dS = 0;$$

$$FNMR(ZFA) = \int_{0}^{ZFA} p(S \mid H_0 \, is \, true)\, dS$$

FNMR(ZFA) is the lowest FNMR Thus it defines the lowest threshold value T=ZFA so that the FMR is still zero. This value is a measure of the total rate of 'inconvenience' when one would achieve a 100 % rejection of impostors.

Zero FNMR

$$ZeroFNMR = \int_{0}^{ZFR} p(S \mid H_0 \, is \, true)\, dS = 0;$$

$$FMR(ZFR) = \int_{ZFR}^{1} p(S \mid H_1 \, is \, true)\, dS$$

FMR(ZFR) is the lowest FMR that can be achieved without accepting false negative matches. Thus it defines the highest threshold value ZFR so that the FNMR is still zero. This value is a measure of the total rate of 'insecurity' when one would achieve a 100 % acceptance of authorised individuals.

EER- Equal Error Rate

$$EER = \int_{T_e}^{1} p(S \mid H_1 \, is \, true)\, dS = \int_{0}^{T_e} p(S \mid H_0 \, is \, true)\, dS$$

The equal error rate is defined as the error rate at the specific threshold value T_e where FMR=FNMR. The EER is a measure for the quality of biometric system that operates in a typical commercial or civilian environment. For highest security or for forensic applications where the FMR or the FNMR are the dominant criterion the EER may not be a good quality indicator.

FAR – False acceptance Rate

The false acceptance rate is closely related to the FMR. It is defined as potentially successful impostor acceptance rate when the impostor uses his own biometric characteristics to try to be accepted as another subject. If a system requests several matches N to accept a biometric verification the value of FAR may be substantially different from the FMR.

$$FAR(T) = (1 - FTA) \cdot (1 - FTE) \cdot FMR(T)^N$$

In most civil application cases N=1 and the rates are only calculated relative to enrolled persons. In addition, the amount of allowed presentations and attempts to create a valid template are sufficiently high to reduce the FTA rate to a very low value. Therefore:

$$FAR(T) = (1 - FTA(T)) \cdot FMR(T) \approx FMR(T)$$

is a good approximation which is widely used in the literature and in the biometric community.

FRR – False Rejection Rate

On the other side, also the false rejection rate is closely related to the FNMR. It is defined as the rate of rejection of (in principle) authorised persons relative to the total number of recognition processes of persons. If a system requests several successful matches N to accept a biometric verification, the value of FRR may increase relative to the FNMR.

$$FRR(T) = FTE + (1 - FTE) \cdot FTA + (1 - FTE) \cdot (1 - FTA) \cdot (1 - [1 - FNMR(T)]^N)$$

In most civil application cases N=1 and the rates are only calculated relative to enrolled persons. In addition, the amount of allowed presentations and attempts to create a valid template is sufficiently high to reduce the FTA rate to a very low value. Therefore:

$$FRR(T) = (1 - FTA) \cdot FNMR(T) \approx FNMR(T)$$

is a good approximation which is widely used in the literature and in the biometric community.

The approximations for FAR and FRR are further justified by the fact that the values of FMR(T) and FNMR(T) are approximated calculations over the biometric variability of the identifiers within a population. Exact definitions would need to calculate the values of p(S) for each biometrics and for each individual in function of the time and location within the feature phase space of the templates, which is infeasible in practice (see also figure 10 *below*). However, one has to be aware of this fact when error rates are calculated on a limited population sample and when such rates are applied for predictions on the behaviour of a biometric system within other populations. There are dependencies of such values from relative position of the considered templates in the feature phase space[19] but also from the age, ethnic characteristics, profession and health conditions.

Relations between error parameters in the verification mode

It is often not clear for what purpose a biometric system will be implemented. Depending on the specific application, the biometric system should provide high security with low FAR or high availability with low FRR. To characterise a biometric system, the interdependence of the two parameters can be best represented by the so called Receiver Operating Characteristic curve:

ROC curve – Receiver Operation Characteristic

The ROC curve shows the FNMR (FRR) in function of the FMR (FAR). The plot is most often represented in a double logarithmic diagram. Sometimes the vertical axis shows the transformed value (1-FNMR) instead of the FNMR.

[19] In all such performance evaluation of biometric systems, one implicitly assumes that the evaluated population sample is a representative sample for all populations which may be a dangerous oversimplification.

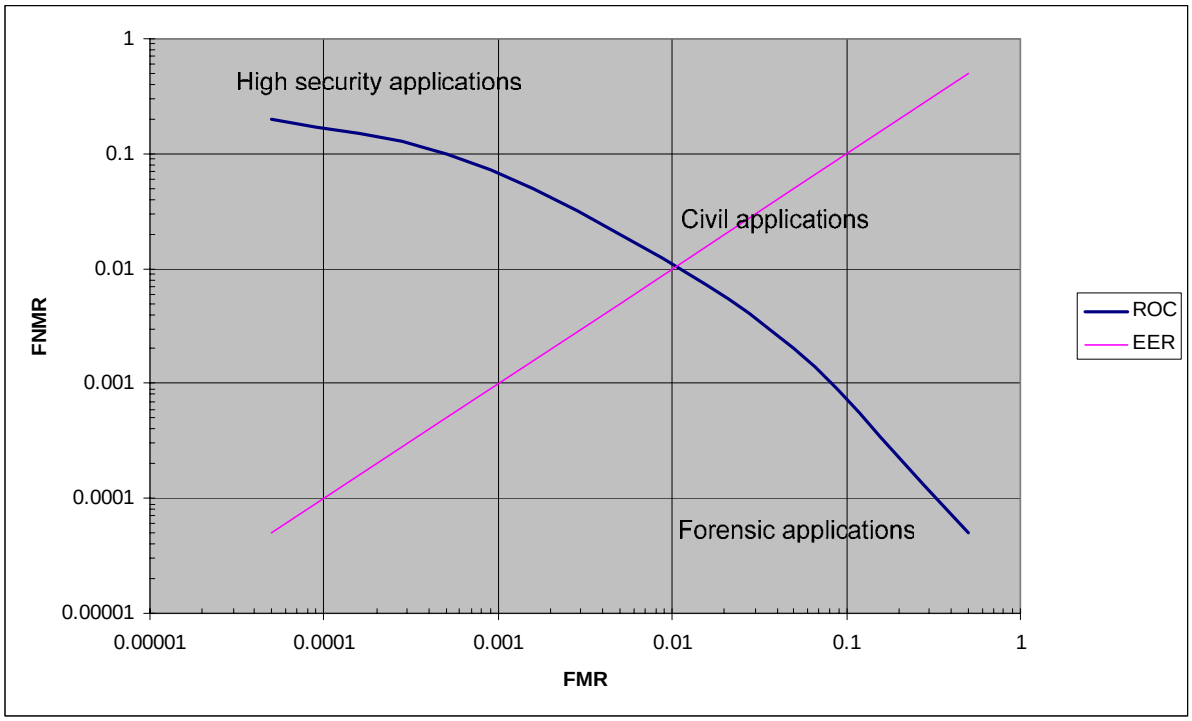

Figure 9: Typical ROC curve on a double logarithmic diagram. Alternative representations may show (1-FNMR) or the direction of the axis flipped. The ROC curve is the characteristic quality curve of a biometric system.

Errors in the identification mode

The main difference of the identification mode relative to the verification mode arises from the matching step. Instead of a clearly defined reference template R claimed by the individual that requested a verification of his biometrics, the comparison step has to use all possible reference templates R_i to calculate all matching scores $S_i(Q,R_i)$ over the full database. The result in general is not a clear match but a ranking list of reference templates with the matching scores over the threshold value $\{S_i,\ldots S_{i'})>T$. It is clear that the size of this list and the probability of an error rises with the size N of the entries in the database of reference templates. The decision rule becomes more complex as it is not clear which one within the list of reference templates with matching scores over the threshold belongs to the individual that has presented the query template. The notions of FMR and FNMR can only be extended to the identification mode in a more or less straightforward way if the FMR<<(1/N). For a given biometric system with defined ROC characteristics this constraint clearly limits the potential size of the enrolled population. The error notions become slightly more complicated as one has to distinguish between the following cases for a given query template Q and N reference templates (R_1…..R_N):

A. All comparisons of Q with any R_i give matching scores $S_i(Q, R_i)<T$; this means that the individual which delivered the biometric sample Q is either not enrolled in the database or that the comparison of query template with the right reference template R_q falls under the FNMR(T). Assuming that the individual was enrolled the probability that this happens is the probability that all (N-1) non corresponding templates do correctly not match and that the single corresponding template does falsely not match

$$P(A) = (1 - FMR(T))^{N-1} \cdot FNMR(T)$$

B. All comparisons of Q with any R_i except with R_q give matching scores $S_i(Q, R_i)<T$ and $S_q(Q, R_q)>T$; this means that for this case the identification mode worked correctly. The chance that this happens is:

$$P(B) = (1 - FMR(T))^{N-1} \cdot (1 - FNMR(T))$$

C. The comparisons of Q with the R_i give k matching scores $S_i(Q, R_i)<T$ and (N-k)>1 matching scores $S_j(Q, R_j)>T$ with $S_q(Q, R_q)>T$ also one of the accepted templates; this means that for this case the identification mode delivers a set of candidates in which the right candidate is still present. The chance that this happens is:

$$P(C) = \binom{N-1}{k} (1 - FMR(T))^{k} \cdot FMR(T)^{(N-1-k)} \cdot (1 - FNMR(T))$$

D. The comparisons of Q with the R_i give k>0 matching scores $S_i(Q, R_i)<T$ and (N-k) matching scores $S_j(Q, R_j)>T$ with $S_q(Q, R_q)<T$ not one of the accepted templates; this means that for this case the identification mode delivers a set of candidates in which the right candidate is not present any more. The chance that this happens is:

$$P(D) = \binom{N-1}{k-1} (1 - FMR(T))^{k-1} \cdot FMR(T)^{(N-k)} \cdot FNMR(T)$$

The first terms in the expressions C and D are the binomial coefficients. It is clear that mathematically case A is a special case of case D with k=N and case B is a special case of case C with k=N-1. Interpreting all events that fall under case B and C as a correct match and all events falling under A or D as a false non match allows definition of the FNMR for the identification mode.

$$FNMR_{Id}(T) = FNMR(T) \cdot \sum_{k=1}^{N} \binom{N-1}{k-1} (1 - FMR(T))^{k-1} \cdot FMR(T)^{(N-k)} = FNMR(T)$$

The FNMR does not change relative to the verification mode as only one reference template is implied in the calculation of the matching score that could lead to false rejection.

In the same sense we can interpret all events that fall under case D with exception of case A as a false match event which gives us a clue for the determination of the false matching rate in the identification mode for instance in forensic application with a subsequent human controlled evaluation of the remaining candidates:

$$FMR_{ID}^{c}(T) = FNMR(T) \cdot \sum_{k=1}^{N-1} \binom{N-1}{k-1} (1 - FMR(T))^{k-1} \cdot FMR(T)^{(N-k)} = FNMR(T) \cdot (1 - \left[1 - FMR(T)\right]^{(N-1)})$$

In applications with an automated identification however all cases with false matches have to be considered as a false match event and therefore contribute to the FMR (case C and D excluding A and B).

$$FMR_{ID}(T) = 1 - [1 - FMR(T)]^{N-1} \approx 1 - [1 - FMR(T)]^{N}$$

It is evident that even with a very small FMR(T) this value rises rapidly to unacceptable values when the size N of the database grows. This problem is known as the scaling problem. Therefore useful applications of biometric systems in the identification mode with centralised processing against a large database are limited more or less for forensic purposes. The identification mode however may be very useful in distributed architectures with local small numbers of reference templates coming from a few or even just one person. The identification mode is best suited for personal biometric tokens that recognise only templates from the authorised user. In this case, the biometric processing and the threshold for the matching decision may even be adapted to the individual user. In such architectures, the identification mode is equivalent to the verification mode but it omits the additional step that the individual has to claim his identity. This claim is intrinsically realised and the system becomes more convenient for the individual user.

Interpretation of the estimated errors

It is necessary to make a restriction remark concerning all above formulas. They are perfectly valid only in the ideal case where FMR(T) and FNMR(T) are not dependant from the position of the compared templates in the feature vector phase space. For all other practical cases they are only more or less good estimators. An exact calculation of the real values would lead to rather infeasible integrations over the probability density functions of the feature vector distributions in the feature vector phase space. Such a discussion is clearly beyond this report.

But the following example, represented in figure 10 *below*, illustrates the problem. In figure 10, we see a (dimensionally reduced) distribution of feature vectors of reference templates in a 2D phase space. We consider 4 locations of a possible reference template feature vector with their acceptance range defined by the threshold value T (indicated by the red circles around the template point) and the corresponding location and acceptance range of query templates (denoted by green and purple circles).

- Case A: The reference and the query template are too far away from each other to match, but both lie in a region of the phase space with low density of feature vectors. Thus the result of the comparison process is a no match (Type A of the above explained cases). The FMR(T) at this location is very low.

- Case B: The reference and the query template are within the acceptance range from each other to match and both lie in a region of the phase space with low density of feature vectors. Thus the result of the comparison process is a single match with the right reference template (Type B of the above cases). The FMR(T) at this location is very low.

- Case C: The reference and the query template are within the acceptance range from each other to match, but both lie in a region of the phase space with high density of feature vectors. Thus the result of the comparison process is a multiple match with many reference templates including the right one (Type C of the above cases). The FMR(T) at this location is much higher than the average FMR(T).

- Case D: The reference and the query template are too far away from each other to match, and both lie in a region of the phase space with high density of feature vectors. Thus the result of the comparison process is a multiple match with many

reference templates but missing the right one (Type D of the above cases). The FMR(T) at this location is much higher than the average FMR(T).

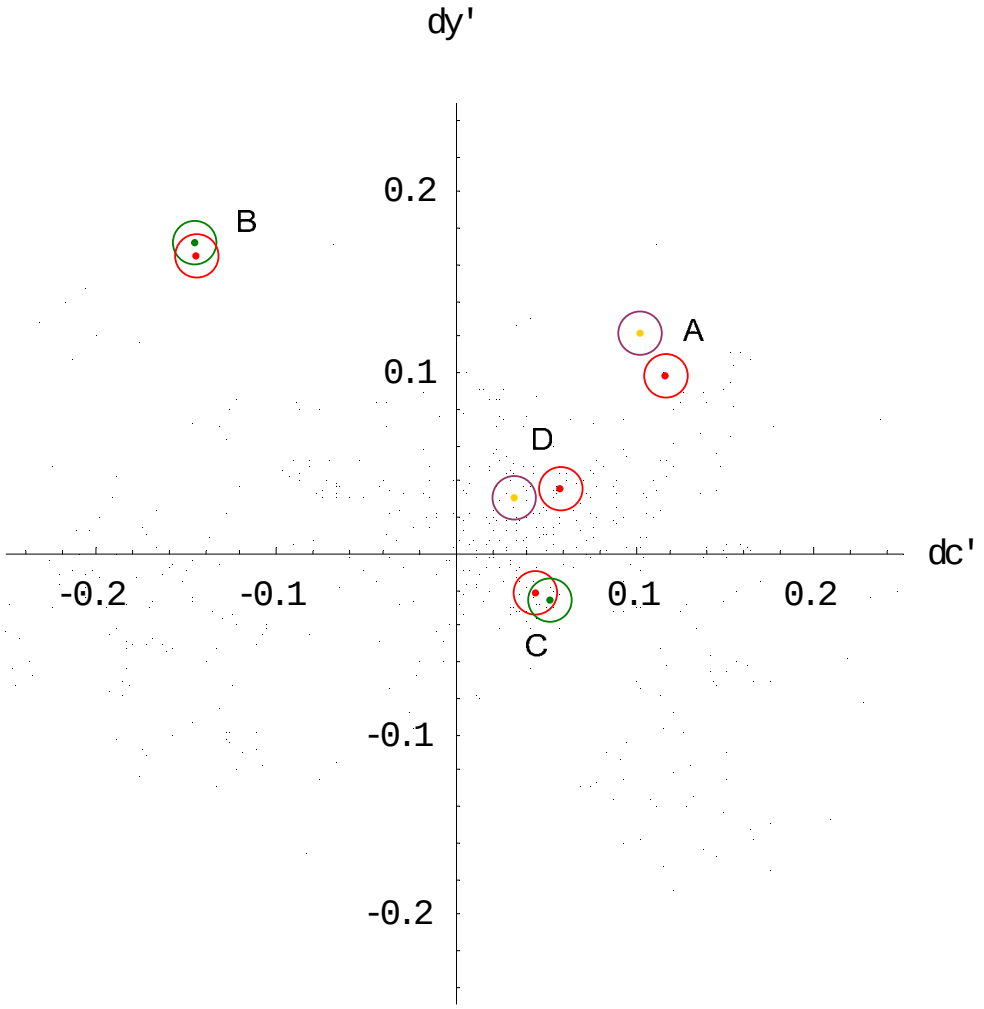

Figure 10: Distribution of feature reference vectors in a 2D phase space with the same acceptance range but in regions with different population densities.

The examples show that the FMR(T) is not necessarily a constant value for all types of biometric samples in the same system but depends also on the location of the feature vectors in their phase space. The performance of identification systems with large centralised databases may be especially biased by such effects.

It is possible to obtain a homogeneous distribution of the feature vectors with a topology conserving transformation of the phase space inserting a so called self-organising topological map[20] between the feature extracting and the comparison component. Such a map reorganises the feature vectors in a homogeneous way over a non-linear transformed phase space. However this neuronal network technique works only with a large and representative sample of training vectors. It is therefore rarely applied.

[20] T. Kohonen, *Self-Organising Maps*, Springer Series in Information Sciences (ISBN 3-540-58600-8).

3.1.5 Valuation of a biometric system in identity management

Biometric recognition of individuals is a valuable method to establish a strong link between a person and a specific identity within a set of identities. It has the advantage that a manipulation of this link is substantially more difficult for the concerned individual but also for potential impostors. This includes the fact that it becomes more difficult for an individual to hide an identity or to usurp new identities. On the other hand, biometric links between an individual and an identity are difficult to determine even if there are good and legal reasons to do so. Most of the biometric characteristics are stable for a long time in the lifespan of an individual, much longer than typical business relationships. Therefore a widespread use of biometric applications for identity management in civil or business purposes may harm the right of privacy of persons.

Another important point which has been outlined above is the fact that biometric techniques always include a measurement process of a physical parameter. As all physical measurements, such a process is intrinsically error-prone and it can lead to false results in the identity verification mode but especially in the identification mode. It is therefore necessary that backup mechanisms and legal restrictions protect individuals that are wrongly authenticated or abusively profiled, from severe consequences.

3.2 Legal treatment and regulations of biometrics

In FIDIS deliverable 3.2. 'Study on PKI and biometrics', it was explained that the Directive 95/46/EC[21] (hereinafter the 'Privacy Directive 95/46/EC') constitutes the general legal framework for the processing of personal data and that, although the Privacy Directive 95/46/EC does not mention biometric data as such, its legal provisions and principles also apply to the processing of biometric data.[22] Although some have tried to argue that the Privacy Directive 95/46/EC does not apply in specific processing circumstances of biometric data, one has to acknowledge that biometric systems *per se* relate to identified or identifiable persons as they use personal characteristics and aim to identify the person to whom these characteristics belong or aim to verify that these belong to the same person.

In August 2003, the Article 29 Data Protection Working Party (hereinafter the 'Article 29 Working Party') established by the Privacy Directive 95/46/EC has provided specific guidelines for the processing of biometric data in a working document on biometrics.[23] These guidelines are highly relevant for biometric identity management systems in general, whether used in the public sphere or for private commercial purposes. These guidelines will not be repeated in this deliverable as they were discussed in the aforementioned deliverable. The Article 29 Working Party has in the meantime further reflected on the meaning of biometric

[21] 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, of 23 November 1995, 31 also available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (part 1) and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf (part 2).

[22] See for the application of the Privacy Directive 95/46/EC to biometrics, M. Gasson, M. Meints *et al.* (eds.), *o.c.* at footnote 3, 101 et seq.

[23] For a discussion of the guidelines of the Article 29 Working Party, *ibid*., 101 et seq.

data in an opinion of 2007 on the concept of personal data.[24] In this opinion, the functionality of biometric data as to establish a link with an individual and to function as identifiers was stressed (see also the discussion *above*, section 2.3).[25]

Furthermore, the use of biometrics in applications controlled by the government, such as in passports and travel documents and in large scale applications in Europe such as the Visa Information System (VIS) and the second generation Schengen Information System (SIS II), has received a lot of attention and was subject to some debate when in several opinions the Article 29 Working Party and the European Data Protection Supervisor (hereinafter the 'EDPS') pointed to the risks of the implementation of biometrics in these applications.[26] Several countries planned or started to issue biometric passports in furtherance of the Council Regulation (EC) No 2252/2004 of 13 December 2004.[27] The regulations and the legal aspects of the use of biometrics in ID documents and passports have been analysed in detail in FIDIS deliverable 3.6. 'Study on ID Documents' of 2006. The present deliverable will therefore not focus on the legal aspects of the use of biometrics for these purposes by governments in ID documents.[28]

In the meantime, the national Data Protection Agencies (hereinafter the 'DPAs') of the Member States have been active in the interpretation of the data protection legislation applied to biometrics for use in the private sector. In most countries, the data protection legislation does not explicitly mention biometrics. The legal provisions which the DPAs apply, however, are in principle the national data protection laws, which have implemented the Privacy Directive 95/46/EC. National DPAs may in principle issue opinions and general recommendations with regard to the processing of biometrics. While recommendations of DPAs have strictly not the force of law, controllers often tend to follow the recommendations issued by DPAs on specific matters.

Presently, the DPAs review the processing of biometric data in many cases upon request for a preliminary opinion by the data controller or sometimes upon notification of the processing. The DPAs, however, have many more important competences. These competences according to the Privacy Directive 95/46/EC include endowment with investigative powers, such as access to the (biometric) data processed by a controller and powers to collect all the information necessary, powers of intervention, including the competence to order the erasure of data or imposing temporary or definitive bans on the use of (biometric) data, and the power to engage in legal proceedings against controllers if they do not respect the data protection provisions.[29] The DPAs can also hear claims of an individual who states that his/her rights

---

[24] Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 26 p.

[25] *Ibid*., 8.

[26] For an overview and discussion of these opinions, see P. De Hert and W. Schreurs, "Machine-Readable Identity Documents with Biometrical Data in the EU Legal Framework (Chapters 4.1 through Chapter 4.1.5)" in M. Meints and M. Hansen (eds.), *D.3.6 Study on ID Documents, FIDIS*, 2006, (39)

[27] Council Regulation (EC) No 2252/2004 of 13 December 2004 for security features and biometrics in passports and travel documents issued by Member States, *O.J.* L 385, 29 December 2004.

[28] See M. Meints and M. Hansen (eds.), *o.c.* cited *above* at footnote 26, 39-69.

[29] See Article 28.3 of Privacy Directive 95/46/EC. The DPAs, however, are often confronted with too limited resources to engage in these tasks, especially for biometric identity management systems, which deployment has

and freedoms with regard to the processing of personal data are infringed or bring violations to the attention of the judicial authorities.[30]

Appeal against the decisions of the DPAs is in principle possible before the national courts of the country where the DPA is established in conformity with the existing procedure for appeal against such (administrative) decisions in that country. In the United Kingdom, a specialist Tribunal (the 'Information Tribunal', formerly the 'Data Protection Tribunal') is set up to determine appeals against notices and decisions served by the Information Commissioner.

In section 3.2.1 *below*, we will first briefly touch upon some ongoing work relating to standards in the field of biometrics. In section 3.2.2, the situation of biometric applications (other than its use in ID documents) in some countries, including some opinions of DPAs, will be discussed. This review will show that the proportionality principle is a leading principle in the evaluation of biometric systems. This concept will be further addressed in section 4.2 *below*.

3.2.1 Standards and regulations

The work on standardisation of biometric technology is ongoing. The efforts are made in national bodies, such as the 'Deutches Institut für Normung' (DIN) in Germany, the Biometric Working Group (BWG)[31] in the United Kingdom, in the United States, the National Institute of Standards and Technology (NIST), the American National Standards Institute (ANSI)[32] and the InterNational Committee for Information Technology (INCITS). Efforts are also made in international organisations, such as the European Committee for Standardisation (CEN)[33] in collaboration with the Information Society Standardisation System (ISSS) and ICAO, ILO (two UN related organisations) and ISO. The work of ISO in cooperation with the International Electro-technical Commission (IEC)[34] in the field of biometrics is important. Subcommittee 37 of the Joint Technical committee 1[35] of ISO/IEC focuses on the standardisation of biometrics. The group was set up in December 2002 and consists of 6 Working groups.[36] Working Group 1 works on a Harmonized Biometric

---

considerably increased in 2006 and 2007. See in this context, the press release of the French DPA of 1 June 2007, available at http://www.cnil.fr/index.php?id=2230&news[uid]=470&cHash=7cc69e6c38.

[30] The powers which are granted to the DPAs are implemented in the nationals laws of the Member States. From Member State to Member State, these powers vary, as summarized in the First report on the implementation of the Privacy Directive 95/46/EC of the European Commission.

[31] See www.cesg.gov.uk. The UK BWG supports the UK government in its current and future use of biometrics for personal identification and authentication. BWG is managed by CESG. CESG is the UK Government's National Technical Authority for Information Assurance.

[32] See www.ansi.org.

[33] See www.cenorm.be. CEN is the European Committee for Standardisation, which draws up voluntary technical specifications to help achieve the Single Market in Europe. The CEN/ISSS Biometrics Focus Group held its first meeting in Brussels, Belgium in June, 2004 and will address biometric interoperability for travel by European citizens in- and outside the EU and EFTA, travel within the EU by non-EU residents, cross-jurisdictional e-government services, and access control by multinational organisations.

[34] See http://www.iec.ch.

[35] JTC 1 of ISO/IEC is responsible for the international standardisation in the field of Information Technology.

[36] For the website of the group, see http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=5537 (last visited on 13 July 2007).

Vocabulary.[37] Group 2 works on Biometric Technical Interfaces. The BioAPI is one of the standards on which that group has worked. Group 3 standardises the Biometric Data Interchange Formats. This group has also been very active. It aims at standardising the content, meaning, and representation of biometric data formats which are specific for a particular biometric technology. The standards issued in 2005 for the biometric data interchange formats for fingerprint image (ISO/IEC IS 19794-4) and face image (ISO/IEC IS 19794-5) are best known. Group 4 works on a Biometric Functional Architecture and Related Profiles. Group 5 concentrates on Biometric Testing and Reporting and Group 6 on the Cross-Jurisdictional and Societal Aspects. Some time ago, Group 6 started its work on the cross-jurisdictional and societal aspects of the implementation of biometric technologies. In a first part, a guide is drafted to the 'accessibility, privacy, and health and safety issues in the deployment of biometric systems for commercial application'. In a second part, there is a technical report relating to the practical application to specific contexts being prepared. A working draft study has been initiated.[38] The work of Subcommittee 37 is also relevant for other standardization work within ISO, such as the work of the Subcommittees 17 (Personal Identification Cards) and 27 (Security) of the Joint Technical committee 1 of ISO/IEC. This group 27 is also engaged to some extent in standardisation related to biometrics. Parties which have an interest in the field of biometrics should take a closer look to the (draft)documents issued by these organisations and follow closely the standardization work which is presently going on in all of these groups.

3.2.2 Situation in some selected countries

As stated *above* in the introduction to this section, we will discuss hereunder briefly the present situation with regard to the legal treatment of biometric systems in some selected countries in the EU. Overall, if one takes a look at the results of the application of the present legal framework upon biometric applications, it appears that Member States, and more in particular the national DPAs, have a considerably large 'margin of appreciation' in pronouncing whether specific biometric systems are in conformity or not with the Directive 95/46/EC and the legal provisions of their countries.

The pronouncements of the DPAs on the use of biometrics, to which we will refer below, relate primarily to the situations where the controller has requested a preliminary opinion on the deployment of a biometric application. In France, it has become mandatory since 2004 to request such opinion, which is *de facto* an authorisation to be obtained, before the start of the processing of biometric data.[39] France is hereby one of the few countries that has acted proactively to the emerging trend of the use of biometric data by imposing such prior authorisation.

The 'margin of appreciation' is a concept deferring to a legislator, an administrative or judicial body or another authority, the possibility to have varying views on matters and to appreciate these in different ways, for example, with regard to the choice of the use of means or to what extent a restriction upon the fundamental right to privacy by the deployment of

[37] See also *above*, section 3.1.

[38] For the draft document, see http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2299802/JTC001-SC37-N-2261.pdf?nodeid=6715191&vernum=0.

[39] Later on, in 2006, the CNIL has issued some 'unique authorisations' which permit controllers, if they comply with all requirements, to file a declaration of conformity (see also *below*).

biometrics is 'necessary'. The concept will be further explained in section 4.2.2. The 'margin of appreciation' of the DPAs is considerable as will be shown below, and may even lead to conflicting opinions in different Member States on very similar biometric applications.

In biometrics, such margin of appreciation of the national DPAs is in our view enhanced because the national data protection laws contain in most countries no specific provisions or criteria on the processing of biometric data. Hence, the DPAs applying the general national data protection laws effective in their country use different criteria which results in diverging views.

We will limit the description of the legal treatment of biometrics to some selected countries of the European Union, in particular Belgium, the Netherlands, France and the United Kingdom.

Belgium

In Belgium, the general data protection law of 8th December 1992, as modified, (hereinafter the 'Data Protection Act') is in principle applicable to the collection and processing of biometric data. The Data Protection Act, however, does not contain specific provisions which mention biometric data as such.

In the annual report of 2005 of the national Data Protection Authority (DPA), the DPA discusses the use of biometric data in the context of a request for an opinion about an access control system. The DPA also refers to biometrics in relation with the developments in Europe with regard to the installation of a visum information system (VIS), the new passports and travel documents and the second generation of the Schengen information system (SIS II).

The Belgian DPA stated in this report, which discusses an opinion that was rendered by the DPA in 2005, that an access control system for a dancing club permitting the identification of the customers by collecting and storing fingerprints in a data base was excessive.[40] The DPA stated that 'the fingerprints have to be considered 'biometric data' and have to be used in a careful way'. It further stated that 'the processing of such data shall be evaluated by the usually applicable texts, taking into account the higher risk of breaching the privacy that this method in some cases entails'. The DPA stressed that 'in view of what has been said above, [ ] *the evaluation of the proportionality* of the use of such data taking into account the envisaged purpose [shall] be decisive'[emphasis added].[41] The DPA further reasoned that fingerprints shall only be used if this is 'absolutely necessary' for the control of the identity. The dancing club argued that young people were not always carrying an identity card and that therefore the use of fingerprints was necessary. The DPA reminded that in Belgium there is a legal obligation to carry an identity card, and that the dancing club could therefore require carrying and showing of such a card. The DPA stated that, in addition, the dancing owner had the possibility to introduce a 'membership card' with a picture ID, which would also permit to control the identity at the entrance. Such membership card would render the use of more extreme means such as the use of biometric data, superfluous.[42]

---

[40] Commissie Voor De Bescherming Van De Persoonlijke Levenssfeer, *Verslag over de werkzaamheden 2005*, 2005, 82 - 83.

[41] *Ibid*., 83.

[42] See and compare this with a decision of the DPA in the Netherlands on a similar system *below.*

The discussion of the opinion in the annual report shows that the proportionality principle to which the DPA refers is a main criterion which the DPA applies in its decision on the use of biometrics. The DPA hereby referred to Article 4, §1, 4° of the Belgian Data Protection Act which requires that the data shall be 'adequate, relevant, useful and not excessive (…) taking into account the purposes for which they are collected or processed'.[43] The importance and the meaning of this principle will be further discussed below.[44]

In the same report, the DPA explicitly referred to several opinions of the Article 29 Data Protection Working Party in which biometric data was discussed. With regard to the data in VIS, the DPA repeated the concern of the Article 29 Data Protection Working Party for additional guarantees for the processing of biometric data. In connection with the passports and travel documents, the DPA stressed that the use of biometric data in these documents entail several ethical, legal and technical questions. For SIS II, the DPA pointed again to the position of the Article 29 Data Protection Working Party and that the *proportionality principle* should be the guiding principle for adding new functionalities to the system, such as the introduction of biometric data. The use of biometric data for purposes of identity control shall be strictly limited to situations, provided for by law, where such use is absolutely necessary (including in the interest of the data subject) and accompanied with appropriate safeguards.[45]

France

In France, the general data protection law N° 78-17 of 6th January 1978, as modified, (hereinafter the 'Act N° 78-17') mentions explicitly biometric data.[46] The Act N° 78-17 requires since a modification of the Act in 2004 that the automated processing of biometric data for identity control must receive the prior authorisation of the DPA (Article 25, I, 8°). Referring to the wording of this Article 25, it is not entirely clear from the text whether the use of biometric data for verification purposes (1:1) would also fall under this article. If this would not have been the intention of the legislator, the use of biometric data for verification would then only be subject to the requirement of notification ('déclaration') prior to the start of the processing. [47] The DPA however seems to take a different position (see *below*).

The DPA may also issue an 'unique authorisation' ('*decision unique*') for the data processing which include biometric data and which have a same purpose, contain the same categories of personal data and have the same (categories of) receivers as set forth in the unique authorisation which the DPA proclaims (Article 25, II). If a controller esteems that the data processing of the biometric data meets these criteria, he shall send a 'letter of conformity' to

[43] This article is an implementation in the National Data Protection Act of Article 6 of the Directive 95/46/EC that requires that '(…) personal data must be (..) collected for specified, explicit and legitimate purposes (…)' and that the data shall be 'adequate, relevant and not excessive (..)'.

[44] See *infra*, section 4.2.

[45] See *supra* at footnote 40, at 88.

[46] For the text of the Act N° 78-17', see the website of the DPA, at http://www.cnil.fr/index.php?id=300.

[47] This is deduced from Article 27, I, 2° of the Act N° 78-17 which explicitly mentions the use of biometrics for 'authentication' as distinguished from the use of biometric data for identity control purposes.

the DPA stating that the data processing complies with the description in the unique authorisation.

The processing of biometric data necessary for the 'authentication' or the identity control for the government needs to be authorised by an ordinance in execution of the law after the DPA has rendered its opinion which shall be public and motivated (Article 27, I, 2°).

Before this change in law, the DPA was consulted several times with regard to the deployment of biometrics.

In an opinion of 23rd April 2002, the DPA advised in a positive way on the deployment of three biometric characteristics (fingerprint, iris or hand geometry) for access control of employees to the security area of the airports of Orly and Roissy. The opinion related to a trial project and seemed to imply also a central database. At the same time, the DPA was very sceptical about the use of biometric fingerprints for access control purposes by an employer, stored in a central database, unless the use of these biometrics was necessitated by an undisputable security objective. The DPA approved in 2004 the final project for the use of a fingerprint stored on a token held by the employees of the airports of Orly and Roissy for verification purposes for access control to the security zone of the airport.[48] The project for which the opinion was asked was in fact the continuation of the trial on which the previous mentioned opinion in 2002 was given. By decision of 8th April 2004, however, the DPA refused to give a positive opinion on an access control system for time and attendance control of employees in a hospital in Hyères.[49]

Since the modification of the data protection legislation in France as described above, the DPA has issued so-called 'unique authorisations' with regard to the processing of specific biometric data for specific purposes. In one such authorisation, the use of fingerprints for access control is accepted if the biometric is stored on a token (smart card or USB token) held under the control of the employee.[50] The other unique authorisations relate to the use of hand geometry of pupils for access to a school restaurant[51] and the use of hand geometry for access control and time and attendance control of employees.[52]

---

[48] Commission Nationale de l'informatique et des Libertés, *Délibération n°04-017 relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en oeuvre d'un contrôle d'accès biométrique aux zones réservées de sécûreté des aéroports d'Orly et de Roissy*, 8 April 2004.

[49] Commission Nationale de l'informatique et des Libertés, *Délibération n°04-018 relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels*, 8 April 2004.

[50] Commission Nationale de l'informatique et des Libertés, *Délibération n°2006-0102 du 27 avril 2006 portant authorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail*, 27 April 2006.

[51] Commission Nationale de l'informatique et des Libertés, *Délibération n°2006-0103 du 27 avril 2006 portant authorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire*, 27 April 2006.

[52] Commission Nationale de l'informatique et des Libertés, *Délibération n°2006-0101 du 27 avril 2006 portant authorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle de l'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail*, 27 April 2006.

In a communication on its site in early 2007, the DPA stressed again that an authorisation is required for the processing of biometric data. It also stated that until that date, the DPA has given no authorisations so far or has not conferred to any processing the 'CNIL label'.[53]

In this communication, the DPA clarified its position as fingerprints should always be stored on an individual support.[54] Its position is based on the consideration that fingerprints leave tangible traces on objects and in places where people have been. Fingerprints can easily be used for person identification and linked with other personal data if accessible in databases. This must be avoided, and as such use of fingerprints is not proportionate with the privacy risks such as being identified. According to the French DPA, other biometric characteristics which leave no persistent traces, such as iris or hand geometry, are less intrusive and therefore pose less problems under the proportionality principle.

The statement of the DPA on its website early 2007 that an authorisation for the use of biometrics is always necessary seems somewhat unclear. If biometrics are stored on an object under the control of the individual involved, such biometric is in principle used for verification purposes (on the term verification, see also sections 2.3 and 3.1). As stated above, is is unclear whether the French legislation only requires an authorisation when the biometrics are used for identification purposes. If the term 'identification' is used in the proper sense of comparison with a database (1:N), which is not possible in the case of the exclusive storage on a local object, one could argue that a prior authorisation would in the case of exclusive storage on a personal document or smart card not be required further to this Article 25. Only a notification would be necessary and the DPA could then always verify the functionality, the proportionality and the legitimacy of the processing after such notification. It is therefore desirable that the meaning of Article 25 and the interpretation by the French DPA be further clarified.

In June 2007, the French DPA stated on its website that since early 2007, it had examined more than 200 requests for authorisations for biometric systems and that it used more than 30 % of its control resources for the inspection of biometric systems. Therefore, the French DPA urged for more resources.

The French National Consultative Ethics Committee for Health and Life Science, which published an opinion on Biometrics, identifying data and human rights in April 2007, had already called for more support for the French DPA. The Committee said that '(…) measures protecting the freedom of citizens must be supported by independent structures designed to fight the possibility of technocratic, economic, police and political abuse in connection with the use of biometric data. CNIL, which is an example in France of a body meeting such criteria, should have its status and resources enhanced in order to improve its efficacy and independence.(…)'.[55]

---

[53] Commission Nationale de l'informatique et des Libertés, *Biométrie ? l'autorisation de la CNIL est obligatoire !*, 5 January 2007, available at http://cnil-front1.heb.fr.colt.net/index.php?id=2166&print=1.

[54] The DPA of France stated it as follows : «'D'une manière générale, la CNIL n'autorise que les dispositifs où l'empreinte digitale est enregistrée exclusivement sur un support individuel (carte à puce, clé USB), et non dans une base centralisée ».

[55] National Consultative Ethics Committee For Health And Life Sciences, *Opinion N° 98. Biometrics, identifying data and human rights*, 26 April 2007, 15.

The Netherlands

In the Netherlands, the general data protection law of 2000, as modified, (hereinafter the 'Data Protection Act') is in principle applicable to the collection and processing of biometric data. The Data Protection Act, however, does not contain specific provisions which mention biometric data as such.

The DPA has paid attention to the issues of biometrics and its opinion has been requested several times. In 2001, the DPA was asked to advice on the bill to change the passport legislation in order to introduce biometrics.[56] Other opinions which are relevant for the use of biometrics include an opinion on the use of face recognition and the use of biometrics for access control to public events, combined with use for police investigations.[57] Another opinion relates to an access control system which was (at least) similar (or identical) to a system that was also reviewed by the DPA in Belgium.

In 2001, the Dutch DPA was asked its opinion on an access control system named 'VIS 2000' with biometrics intended for use by restaurant owners and sport centres.[58] The system would be used for access control, marketing and management purposes and the storage of a 'black list' of customers who 'misbehaved' in one of the establishments who installed VIS 2000 (restaurants, sport centres, dancing clubs,…). The system provided for the storage of the templates of the fingerprint and the face. The templates of the face were also stored in a central database, combined with the membership card number and a code for the 'misbehaviour'. The card number could be linked with the identity of the visitor/members communicated at the moment of issuance of the card. The biometric data were also stored on a smart card, and used for membership verification when entering the club. When entering the club, there was in addition a check made with the black list of persons who misbehaved, one of the main purposes of VIS 2000. The biometrics were hence used for the purposes of verification (1:1 check, comparing whether the holders of the membership cards were the owners of the card) and of identification (1:N check, comparing whether the holders were not yet registered in the central database of VIS 2000). In the case of past incidents, the biometric characteristics were also used for the identification of troublemakers (discovery of the 'civil identity' (see *above*, section 2.3) by reverse-engineering the stored templates of the face to images, comparing the images with the images of the troublemakers taken by surveillance cameras and connecting the templates with the name, address and domicile data if a membership card was issued. The purposes of VIS 2000 were named as to increase the security of the other visitors and employees at the clubs, to maintain order and to refuse access to unwanted visitors.

The DPA stated in its opinion that the use of biometric data for access control purposes is far-reaching and that it should be evaluated whether the use of biometric data is *in proportion with this purpose*. The DPA checked the collection and use of the biometric data against several obligations of the Data Protection Act. It should be noted, however, that the DPA did not investigate thoroughly the proportionality of the use of the biometrics as described above.

---

[56] College Bescherming Persoonsgegevens, *Wijziging Paspoortwet (invoering biometrie)*, 16 October 2001.

[57] College Bescherming Persoonsgegevens, *Vragen over inzet gezichtsherkenning*, 3 February 2004.

[58] Registratiekamer, *Biometrisch toegangscontrolesysteem VIS 2000*, 19 March 2001. This case is also known as the 'discopass opinion'.

The DPA did not discuss whether there are other, less intrusive means to maintain order and to refuse troublemakers to the club at their next visit without storing biometrics in a central database. As there is a membership requirement in some cases, the DPA could have suggested for example, that it was sufficient to withdraw the membership card from troublemakers after an incident and to restrict access to those individuals who hold a membership card with picture. Such membership cards could then be issued after a control of a central list, which mentions previous applications and/or suspensions, but without biometrics.

In this opinion, the DPA explicitly recognises the possibility to reconstruct from the template of the face the original scanned facial image based on the algorithm used. It is acknowledged by some that templates of the face can be easily reverse-engineered to the images. This is an important factor in the evaluation in biometrics. This reverse-engineering of the templates was one of the main functionalities of VIS 2000 to identify troublemakers. This technical feature, however, has important consequences. It implies that the face scan at all times may contain information about someone's race, which shall in principle not be processed. The Dutch Data Protection Act contains an explicit exception to this prohibition of processing of this information, in particular, when such processing is used for the identification of the person and to the extent such is necessary for this purpose. The DPA considered it inevitable that use is made of templates of the face (containing information about race) for the identification of troublemakers. As stated above, the DPA *does not make a proportionality test about the use of biometric data*, and seems to mistakenly consider the test about the necessity to use information about race as sufficient.

The DPA continues that the use of personal data for marketing purposes should not include biometric data and that the processing for this purpose should be separated from the other purposes. The DPA concludes its opinion with several recommendations, including with regard to the term of storage and security (requirement for encryption of the templates and membership card numbers) and for the operation of the biometric system. The DPA also requested that any VIS 2000 systems already installed would comply with these requirements.

The divergence of the outcome of this opinion of the Dutch DPA is interesting as compared with the evaluation, comments and conclusion of the Belgian DPA with regard to a similar system (see *above*). As mentioned above, the Belgian DPA reported in its annual report of 2005 that it rendered a negative opinion on a similar system. It considered the use of biometric characteristics for access control for a dance club not proportionate with such a purpose. More particular, the Belgian DPA found the use of biometrics for identification purposes (as explained *above*, in section 2.3 disproportionate and entailing risks for the privacy of the visitors.

The United Kingdom

In the United Kingdom, the Data Protection Act 1998, which came into force in March 2000, (hereinafter the 'Data Protection Act 1998') is in principle applicable to the collection and processing of biometric data. The Data Protection Act 1998, however, does not contain specific provisions which mention biometric data as such.

Biometric data processing, however, has been a topic of discussion as the use of biometrics for the eID card was heavily debated, discussed and researched in the build-up to the voting of the Identity Cards Bill which resulted in the Identity Cards Act 2006.[59] This Act requires

[59] See e.g., London School of Economics, *The LSA Identity Project Report*, June 2005.

all individuals over the age of sixteen to register personal details, including identity (name), address and residential status, as well as a photograph and biometrics, i.e., fingerprint and 'other biometric information'.[60] This information can also be provided to other persons for verification 'or otherwise with consent'. The new legislation will also install a central register, the 'National Identity Register'.

Biometric characteristics are also increasingly used in the private sector. It is noteworthy that there seems an increasing trend for the use of biometrics at schools. The Information Commissioner would not yet have taken position as to the use of biometrics in this context. Other applications in the private sector are trials for the use of fingerprints as approval for payment. It is interesting to note that at the website of the CESG (see *above*, section 3.2.1), it is stated that there are currently no government approved biometric applications and that they 'do not expect any to be available in the near future as none of the technologies have yet, in [their] view, reached the stage where [they] would be happy with them as the sole access control mechanism.[61] The CESG does provide advice on biometrics product selection and for this purpose publishes a on its website a manual 'Biometrics for Identification and Authentication – Advice on Product selection' dated March 2002.

3.2.3 Regulation for biometrics as a primary key for interoperability ?

The role of biometrics in the ongoing efforts to create interoperability of databases in the European Union is hereunder reviewed and the question is raised whether there is an appropriate legislation in this regard. First, the history of interoperability as a policy concept is traced. Furthermore, the assumption is made that biometrics will be regarded as the most important primary key soon. Biometric identifiers are in all EU policy documents referred to as much more reliable than the a-numerical primary keys so far. However, the technical shift towards key-interoperability of biometrics still needs confirmation. The question is whether there is appropriate legislation on interoperability as of yet and if not, whether data protection legislation as the legal framework within which interoperability should be made to work will do for biometrics.

Interoperability of European databases in the 'First Pillar' and the 'Third Pillar'

Surprisingly, in the EU, the term interoperability, though used widely, cannot be defined clearly. The European Commission has tended to present interoperability as a technical concept. The 2005 Commission Communication "on improved effectiveness, enhanced operability and synergies among European Databases in the area of Justice and Home Affairs" defines interoperability as "the ability of IT systems and of the business processes that they support to exchange data and to enable the sharing of information and knowledge".[62] Earlier FIDIS work in the area of interoperability has concluded that "*the subject of interoperability is complex and covers the whole range of issues from technical, legal, policy*

[60] Section 12 (3) (a) and (b) of the Identity Cards Act 2006.

[61] See http://www.cesg.gov.uk/site/about/index.cfm?menuSelected=7&displayPage=7 (last visited on 13 July, 2007).

[62] Commission of the European Communities, *Communication to the Council and the European Parliament on improved effectiveness, enhanced operability and synergies among European Databases in the area of Justice and Home Affairs*, COM (2005) 597 final, Brussels, 25 November 2005.

and cultural dimensions".[63] The FIDIS work has therefore been focused on addressing the diverging issues and deepening understanding, especially of the social and cultural questions.

The exact scope of the term thus remains subject to interpretation and context. In the 2006 Commission Communication on "Interoperability for Pan-European e-Government Services" interoperability was first put forward as a means to enhance the cooperation of administrations in the context of e-government.[64] This introduction within the framework of e-government builds on earlier use of the objective of interoperability in areas within the realm of the free movement of goods, people, workers and services (the so-called First Pillar).[65] Justice and Home Affairs (JHA) issues have been brought into the remit of the European Union much later and fall under the so called Third Pillar, which means amongst others, that decisions are taken on the basis of unanimity. It is obvious, that in the context of the original policy areas, interoperability was basically a technical issue. One technically compatible infrastructure would achieve improved effectiveness and meet the interest of EU, its business community and its citizens.[66] However, whatever the interpretation of the concept, it cannot be denied that in the Third Pillar policy area of Justice and Home Affairs interoperability potentially has a much more intruding effect and can touch fundamental rights, and privacy and data protection issues.

The direct link between eGovernment, EU policies and interoperability is interesting. In a book on ICT and innovation, Meijer and Zouridis[67] have argued that e-government is an innovation which may have undesired effects. They argue that the development of e-government is stagnating in many countries as a result of institutional rather than technical barriers. They point out that there is an absence of debate on competing values in e-government and note that debates tend to be framed in terms of efficient information processing.[68] In this sense, e-government is obviously about efficiency and cooperation, but also about new structures and vehicles for domination and legitimation which need public debate. To see interoperability as an element of e-governmental organisational innovation

---

[63] FIDIS interoperability work package reported on by James Backhouse in *Datenschutz und Sicherheit* 2006, vol 30, 9, 570.

[64] COM (2006) 45, Brussels, 13 February 2006, available at http://77eur-lex-europa.eu/lexuriserv/site/eu/com/2006/com2006-0045en01.pdf

[65] These are policy areas that fall within the core European Union policies as governed by the Treaty of Rome. This means that the European Parliament, the European Court of Justice and the European Commission have an important role to play in complicated decision making procedures, and outcomes can be based on qualified majority in the Council of Ministers. There have been policies on interoperability of the trans-European conventional rail system and the high speed rail system, of telecommunication networks, of electronic road toll systems, air traffic management networks and so forth. See for example the *Commission Communication in the framework of the implementation of Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system*, OJ C 236, of 24 September 2005. Or for the *European Interoperability Framework for Pan-European eGovernment services* version 1: http://europa.eu.int/idabc/en/document/3473/5585 (2004).

[66] This is a rather simplified statement but the point is made. For interoperability and telecommunications see S. Gijrath, "Interoperability Revisited: How far stretches the duty to negotiate interconnection?", *Computer and Telecommunications Law Review* 2006/1.

[67] 'E-Government is an Institutional Innovation" in V. Bekkers *et al.* (eds), *Information and Communication Technology and Public Innovation; assessing the ICT-driven modernisation of public administration*, IOS Press, Amsterdam 2006, 219-229.

[68] *Ibid.*, 226.

could well be instrumental in making sense of emerging new balances between security and liberty, and changing power oppositions and relationships.[69]

In the context of the Third Pillar, the Commission launched as stated above a first Communication on interoperability and synergy among European databases in the area of Justice and Home Affairs in November 2005.[70] The purpose of the communication is to highlight how, beyond the present purposes, the Visa Information System (VIS), the second generation Schengen Information System (SIS II), and other databases "*can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime"*.[71] The term interoperability is used to describe the linking of large-scale EU IT-systems such as VIS and SIS but also to describe linking or even *merging* of national databases (DNA and Automated Fingerprints Identification Systems (AFIS) merging into a European database). Interoperability thus refers to both the linking of large scale IT systems and to the linking of national and international databases.

Biometrics and Interoperability

In the 2005 Commission Communication a clear link is made between biometrics and interoperability. The Commission notes with approval that the challenge of identifying persons in databases with millions of entries has been solved in Eurodac and in the VIS by using biometric searches, "*allowing unprecedented accuracy*". The use of biometric information in SIS II is also applauded, except for its restricted scope: "A*s the SIS II is being developed today, biometrics will only be used to confirm the identification of the wanted person (wanted persons meaning "persons for whom an alert has been issued", including persons who should be refused entry) based on an alphanumerical search. When available, biometric searches would allow more accurate identification of wanted persons. However, SIS II would only store biometric information that could be legally linked to an alert in SIS II*".[72]

The Communication also notes that all the existing European databases, including Eurodac, are underexploited: *"Although the Eurodac Regulation obliges Member States to take fingerprints of all persons aged over 14 who cross their borders irregularly and cannot be turned back, the quantity of such data sent to Eurodac is a surprisingly low fraction of the total migratory flow*". Furthermore, it is observed that there is no possibility to use asylum, immigration and visa data for internal security purposes: "*In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for all SIS II immigration and Eurodac data. This is now considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime*".[73] The Communication contains numerous 'short term scenario' proposals to improve the use of the current databases. For instance, a more comprehensive access to VIS and SIS II by asylum and immigration authorities is proposed to allow these 'Eurodac-authorities' to complete the

---

[69] See V. Bekkers, H. Van Duivenboden and M. Thaens, "Public Innovation and Information and Communication Technology: relevant backgrounds and concepts" in V. Bekkers *o. c*., 3-21.

[70] See *above*, footnote 62.

[71] *Ibid*., 2.

[72] COM (2005) 597 final, 7.

[73] COM (2005) 597 final, 5.

assessment of asylum applications: "V*isa data can help to assess the credibility of an asylum claim and SIS II data can indicate if the asylum seeker constitutes a threat to public order or national security. A check in Eurodac, SIS II and VIS would allow asylum authorities to check the data simultaneously in the three systems*". This recommendation is followed by the suggestion to also consider the opposite move, allowing 'authorities responsible for internal security' to access the VIS and Eurodac data: "*As regards Eurodac, the only information available to identify a person may be the biometric information contained in Eurodac if the person suspected to have committed a crime or an act of terrorism has been registered as an asylum seeker but is not in any other database or is only registered with alphanumerical, but incorrect data (for example if that person has given a wrong identity or used forged documents). Authorities responsible for internal security could thus have access to Eurodac in well-defined cases, when there is a substantiated suspicion that the perpetrator of a serious crime has applied for asylum. This access should not be direct but through the authorities responsible for Eurodac. Access to these systems could also contribute to the identification of disaster victims and unidentified bodies*". [74]

From the above, it becomes already clear that the 2005 Commission Communication discussing interoperability was intended more as the starting point for a large political debate than as a road map with a clearly marked route and identified aim. It contained several scenarios that have since been regarded as middle- and short term objectives. One, for example, is the creation of (a) European register(s) for travel documents and identity cards with biometric identifiers. It also envisages a network linking national databases of this kind, with the purpose of checking the authenticity of travel documents, i.e. to check the identity of the traveller against the document in order to prevent identity fraud. Another scenario envisaged by the Communication is the above mentioned creation of a European Automated Fingerprints Identification System (AFIS) for criminal matters, either by establishing one large EU-wide database or by interlinking national databases.

Elsewhere, we have called the Communication "a wish list" compiled to serve the interest of only one good, viz. security.[75] The Communication cannot be accused of a lack of vision but, by underplaying the political dimension of interoperability, it sets an agenda without making useful distinctions between organisational, technical, and legal interoperability issues and between ordinary and more controversial applications.[76]

Interoperability is thus much more than a technical process of interconnecting ICT-systems. It obviously has technical, semantic, social, cultural, economic, political, organisational and legal dimensions. That is why FIDIS has developed a holistic framework in order to address these diverging issues avoiding the pitfalls of a too limitative or too biased definition.[77] Such

---

[74] COM (2005) 597 final, 8.

[75] P. De Hert, Briefing paper for the EP Citizens Rights and Constitutional Affairs Committee, *What are the Risks and What Guarantees Need to be Put in Place in View of Interoperability of Police Databases?* 01.02.2006 IP/C/LIBE/FWC/2005-25, available through http://www.ipolnet.ep.parl.union.eu/ipolnet/cms, (section 4).

[76] *Ibid.*

[77] See J. Backhouse *o. c.* p 570 and conference announcement Karlstad Summer School: http://www.cs.kau.se/IFIP-summerschool/.

a notion 'can serve as an umbrella, beneath which can exist many disparate but complementary definitions, according to perspective or layer of abstraction'.[78]

Decisions on the choices that can be made, should be informed decisions made through a political and legal process that addresses the question whether the data exchange envisaged is legally or politically possible or required.[79] De Hert and Gutwirth have argued that it is particularly the case when there is interoperability with systems outside the EU, between law enforcement and other systems, or within the framework of intelligence led policing.[80]

If we focus on the interoperability of biometrics in the JHA framework, we observe that the assumption is that biometrics eventually will have to become the primary key. A primary key is the basic unit of data under which all other forms of data collected are categorised and stored. We make this assumption based on the observation that biometric identifiers are expected to be much more reliable than the a-numerical primary keys used so far.[81] De Hert and Gutwirth have stressed the distinction between interoperability of keys and interoperability of content.[82] Traditionally content is made accessible by using alphanumeric data such as names and/or date of birth. Because of problems with spelling and accuracy, the creation of unambiguous identifiers (e.g. biometric data and social security numbers) is now considered to be a necessity by many. Here biometric identifiers are regarded as the perfect solution in the making.

The use of biometric identifiers in the context of SIS II and the Prüm Treaty support this premise.[83] Of course, since the Council and the Commission adopted the Hague Programme in June 2005, the EU has been set on the fast track of rapid introduction of biometric identifiers in passports and travel documents.[84] Biometrics provides unique identifiers that are regarded superior to using a-numerical identifiers such as name and first name.[85] The use of

---

[78] A. Wallwork and J. Baptista, "Understanding Operability" in J. Backhouse (ed.), *D.4.1 .Structured Accounts of Approaches on Interoperability*, FIDIS, 2005, (19-24), 20, available at http//www.fidis.net/487.0.htm#820.

[79] The Commission Communication (2005) 597 final argues the opposite at page 3.

[80] P. De Hert, briefing paper of 2006 cited in footnote 75 above and P. De Hert and S. Gutwirth, "Interoperability of Police Databases within the EU: an accountable political choice?", *International Review of Law, Computers & Technology* 2006, Vol 20, nos 1 & 2, 21-35.

[81] See for example the text on biometrics in the 2005 Commission Communication quoted above: "*allowing unprecedented accuracy*".

[82] P. De Hert and S. Gutwirth, *o. c*. at footnote 80, 26.

[83] The Prüm treaty is an international police-cooperation agreement and was signed by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria in May 2005. For wider implications see T. Balzacq et al., *Security and the Two-Level Game: The Treaty of Prüm, the EU and the management of threats*", CEPS Working Document No 234/ January 2006 and more general: T. Balzacq and S. Carrera (eds.), *Security v Freedom: A Challenge for Europe's Future*, 2006, Brussels, CEPS.

[84] Commission (2006) COM (2006) 331 final Communication *Implementing the Hague Programme: the Way Forward*, 28 June 2006; Commission (2006) COM(2006) 332 final Communication from the Commission to the Council and the European Parliament *Evaluation of EU Policies on Freedom, Security and Justice*, 28 June 2006; Commission. (2006c). COM(2006) 333 final Communication from the Commission to the Council and the European Parliament. *Report on the implementation of the Hague Programme for 2005*. 28 June 2006. Commission (2005), COM(2005) 490 final.

[85] See European Biometrics Forum (forthcoming), *Security & Privacy in large Scale Biometric Systems*, A report commissioned by JRC/ITPS.

biometric technology in combination with increased availability and interoperability of data within the European Union are heavily relied on to enhance future security in Europe. Serious concerns about the societal impact of the use of biometrics at a large scale[86], the underestimated financial implications[87], their technical feasibility[88], their susceptibility to large scale fraudulent use, their privacy implications,[89] and the impact of the uncomfortable mix of the use of biometrics in civil and public sector applications[90] have not gathered the momentum needed to put a stop to the embracing of biometrics at governmental level.

Biometrics, Interoperability and Data Protection

Eurodac has been a test case for the debate about the massive use of biometric technology. The European Data Protection Supervisor (EDPS), in its subsequent opinions regarding the use biometrics in EU databases, has pointed out that the use of biometrics in such databases is useful, but the technology still has important drawbacks, e.g. the accuracy of fingerprints is still not sufficiently high.[91] Therefore, the EDPS has warned in all his opinions on biometrics that all biometric identification systems are inherently imperfect and that they must hence provide for adequate fallback solutions.[92] More fundamentally, the EDPS opposes the use of biometrics as the primary key, as it would make the merging of different databases possible with very little effort and enhanced key-interoperability is simply not a desired good for many: it trespasses a privacy-decent border and the resulting level of transparency of citizens

---

[86] J. Ashbourn, 'The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies', *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission January 2005.

[87] London School Of Economics, *The Identity project: an assessment of the UK identity project and its implications*, London, 2005.

[88] *Ibid.*

[89] See amongst others C. Coelho, EP Report A6-0029/2004 on the Commission proposal for a Council regulation amending Regulation (EC) No 1683/95 (uniform format for visas) and regulation (EC) No 1030/2002 (residence permit for third nationals), p 26 (Minority opinion tabled by Ole Krarup, Sylvia-Yvonne Kaufmann, Mary Lou McDonald and Giusto Catania). In this report huge risks to data protection are highlighted. The report suggests that biometrics do not increase security because they only link a person to an identity established by an identity document opening up an easy world of crime through false identity.

[90] B. Jacobs, 'Select before you Collect', *Ars Aequi*, vol. 54, December 2005, 1006-1009.

[91] All unique identifiers, including biometric applications, have an error-rate that is undesirable when working with large-scale applications. Some biometrical applications are still in an experimental phase, for instance the use of video surveillance at airports combined with 'face recognition' technology to check identities against photographic databases of criminal suspects. Even when one assumes that advances in technology may improve the record of this technology, the fact remains that terrorist will not line up to let their picture be processed in the system. In the same way, ID cards will be forged, purchased from corrupt officials or simply obtained using other documents that are themselves false. Existing business practices to facilitate border procedures for persons with such a card are an open door for terrorists to step in. The ID cards will not help to identify terrorists before they strike. Biometrical operability or numbers operability therefore creates a false promise of efficiency.

[92] See for instance, EDPS, 'Common Consular Instructions-EDPS opinion', *EDPS Newsletter*, no. 7, 14 December 2006, 2 (www.edps.europa.eu.) also EP working document by MEP Ludford on the proposal for a regulation of the European Parliament and of the Council amending Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa application (COM(2006) 88 and 269 final), PE 386.565v01-00).

is problematic in a democratic state keen on power-management.[93] This is recognised as a potential problem in expert reports; at the same time it is suggested that complex technical solutions are available in the form of MOC (matching on card), BAC (Basic access Control), EAC (Extended Access Control) and new methods of matching biometrics data in irreversibly encrypted form. The current weaknesses in key management are also expected to be temporary and technical improvement eminent. [94]

At a public hearing in the European Parliament on 2nd March 2004, European Justice and Home Affairs Commissioner Antonio Vitorino highlighted the successful work of the Eurodac fingerprint database for the comparison of fingerprints of asylum applicants and illegal immigrants, saying that out of 250,000 identifications there has not been one 'false positive' ID.[95] As Eurodac is a hit/no hit European database, this great achievement might come into a completely new light when the data would become used as a key identifier, with unforeseen social, legal, political, cultural or economic implications for the individual involved.[96] According to expert reports, all unique identifiers used as primary keys, including biometric applications, have an error-rate that is undesirable when working with large-scale applications. The technical shift towards key-interoperability of biometrics is not confirmed yet, but if it does, it will need a full public debate and an extended impact assessment as well as expert scenario research.

What is important to note is that this is not an academic discussion on the merits of technology or its legal implications: Schengen II and Prüm have introduced data searches on the basis of biometric identifiers[97] and expectations about the accuracy of biometric data and machine readable documents are now at the heart of European Union policies, also in the area of Justice and Home Affairs.[98] Accuracy is indeed a data protection requirement, but

---

[93] See on the risks created by unique identifiers and on the legal situation in different Member States: Committee of experts on data protection (CJ-PD), The introduction and use of personal identification numbers: the data protection issues, Study prepared by the under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, chapter II, available at http://www.coe.int/T/E/Legal_affairs/Legal_co-cperation/Data_protection/Documents/Publications/4Pins.asp#TopOfPage.

[94] These issues are dealt with in the European Biometric Forum report cited in footnote 85. In this report the protection of biometric data in (inter)nationally managed ID systems is presented in terms of concerns and potential solutions. The cryptographic weakness of BAC and the lack of effective key management for EAC are focus points in the report.

[95] 'European Commissioner highlights benefits of biometric passports', 4 March 2004, available on the internet through http://europa.eu.int/ida/en/document/2221/330 (last accessed February 2007).

[96] Some of these issues are discussed in J. Lodge, ' EJustice, Security and Biometrics: the EU's Proximity Paradox' *European Journal of Crime, Criminal Law and Criminal Justice*, 2005 Vol 13 no 4. pp 533-564. See also I. Ploeg, Van der, "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification", *Ethics and Information Technology* 1999, 1, 295-302.

[97] See R. Thomas, "Biometrics, international Migrants and Human Rights", *European Journal of Migration and Law*, 2005, vol. 7, 377-411 and also P. de Hert, V. Papakonstantinou and C. Riehle, *Data Protection in the Third Pillar. Cautious Pessimism*; T. Balzacq et al, *Security and the Two-Level Game: The Treaty of Prüm, the EU and the management of threats*", CEPS Working Document No 234/ January 2006.

[98] P. De Hert, W. Schreurs and E. Brouwer (2006). 'Machine-readable identity documents with biometric data in the EU: Overview of the legal framework', *Keesing Journal of Documents and Identity*, 21, pp 3-10 and P. De Hert and A. Sprokkereef, *An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics*, 2006, CEPS Briefing Note for the European Parliament's committee on Civil Liberties, Justice and Home Affairs, IP/C/LIBE/FWC/2005-xx, which can be retrieved from: www.ceps.be.

proportionality is it as well. Whilst the technological challenge is to produce reliable and cost effective biometric applications, the biggest challenge in legal terms is to meet the requirements of the proportionality principle. In fact, in a puritan interpretation of this principle, the legal starting point should be a situation of non-interoperability rather than interoperability.[99]

There is no legislation on interoperability and thus data protection legislation is the legal framework within which it should be operated.[100] For institutional reasons, the 1995 EC Directive on data protection excluded the processing of data by justice and home affairs authorities.[101] There is now a proposal for a data protection framework for the Third Pillar. So far, all European initiatives involving any data processing by police and judicial actors have stipulated specific data protection rules, resulting in a fragmented body of regulations. Some have argued that the legal answer to the fragmentation should be one single legal framework for all databases set up under the First and the Third Pillar.

All EU countries have their own national data protection legislation too. Data protection protects a plurality of values that do not always coincide and often conflict. European data protections recognise this in different ways: Firstly, by identifying and distinguishing categories of sensible data that is submitted to tougher rules. Secondly, by imposing the collection limitation principle according to which there should be limits to the collection of personal data and such data should be obtained fairly and lawfully and, where appropriate, with the knowledge or consent of the data subject. Thirdly, by enforcing the purpose specification principle and the use limitation principle. Fourthly, the data collected and exchanged should be adequate, relevant and proportional in relation to the purpose for which they are collected (proportionality principle). As regards the latter, many observers have been quite bold when it comes to assessing the collection of biometric data in the EU. "*A facet of proportionality is that the measures undertaken are urgent enough to justify such radical inroads into privacy rights. There is little or no evidence so far that biometric technology has contributed to reducing either terrorism or irregular migration as intended*".[102] It is doubtful whether this assessment would be different when the question would be whether the policy goal of more efficient government would justify the collection of biometric data.

In his comment on the proposed framework decision on data protection in the Third Pillar, the European Data Protection Supervisor observes that neither the proposed framework decision, nor the proposal for a Council framework decision on the exchange of information under the availability principle address the sensitivity and specificities of biometric data and DNA profiles from a data protection point of view.[103] Data protection will not do for biometrics.[104]

---

[99] As De Hert has put when he assesses the risks of interoperability with systems outside the EU: "Non interoperability should be the rule. An exception can only be allowed for restricted interoperability in certain well-defined cases for restricted purposes and on the basis of reciprocity", in: briefing paper 2006.

[100] Prins was the one of the first to map this out: C. Prins, 'Making Our Bodies Work for Us: Legal implications of Biometric Technologies', *Computer Law & Security Report* 1998, 14. no 3. pp 159-165.

[101] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, OJ L 281, pp 31-50, of 23 November 1995.

[102] R.Thomas , *o. c.* at footnote 97, 399.

[103] Commission. COM(2005) 490 final. Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability. 12 October 2005.

[104] See De Hert and Gutwirth, *o. c.* at footnote 75, 27.

Data protection rules need to be supplemented with incriminations for theft and unauthorised use of biometric data. Legally, we will need to be prepared for new forms of biometric crime and thought should also go into prohibitions on unnecessary or risky use of biometrics, e.g. for ordinary financial transactions. In January 2007 a bank in Rome was robbed because of the use of a severed finger to gain entry. The severed finger was left on the pavement after the hold up.[105] What about prohibitions for schemes such as the scheme for Maastricht coffee shop visitors[106] or prohibitions of central stored biometrics; prohibitions of storing "raw images"[107], prohibitions on non-encrypted processing and transmitting of biometrical data and so forth.

Biometrics and interoperability are presented as answers to an increased security or terrorism threat, but are in fact part of a larger public sector innovation development. Instead of solely referring to biometrics and interoperability as data protection issues we should relate them to the new forms of governance in the context of ICT and public innovation.[108] This will also help us in approaching the opportunities and problems related to the simultaneous use of biometrics by the private and the public sector.

Interoperability is therefore in fact a highly sensitive political issue as it has the potential of striking citizens right at the heart of their social, political and cultural wellbeing. To create key operability would be a political choice. The regulation of biometrics requires recognition that interoperability is a political, rather than a technical concept and merits a broad public debate. The broader aspects of interoperability should be addressed widely, particularly in cases of interoperability with systems outside the EU, between law enforcement and private systems or in intelligence led policing.

3.3 Control schemes within biometric systems

3.3.1 Classification of biometric systems

For making a discussion about the security and privacy aspects and the advantages of biometrics focused, it is suggested to determine in which kind of application biometrics are used. Making blanket assertions on biometrics and its risks is trivial. Only if it is clearly determined for which application(s) the risks discussed are valid, it is possible to propose means and strategies to solve the threat. For this reason, in this section of the report, an attempt is made to give an overview and a classification of applications which deploy biometric functionalities for identity management purposes.

In the past, there have been some attempts to describe and classify the ways in which biometric methods are applied. It is not the purpose of this report to analyse these classifications in depth or to criticise them. Because these previous attempts are interesting, they will hereunder be briefly described. One attempt that was mentioned in the BioVision Roadmap, was the proposed classification of the Association Française de Normalisation

---

[105] *Messaggero* newspaper 28th January 2007 and confirmed by the Roman scientific police.

[106] For quick and efficient control mechanism to verify the age of a coffee shop visitor.

[107] European Biometrics Forum, *o. c*. at footnote 85, 16.

[108] See Bekkers *et al.* above, also Meijer and Zouiridis above and the identity management as an innovation concept of Lips, Taylor and Organ, "Identity Management as a Public Innovation: looking beyond ID cards", in Bekker *et al.*, 204-216.

(AFNOR), the French national standards body.[109] According to AFNOR, four classes of services of biometric applications could be made, based on the 'performance requirement' of the technology:

AFNOR Class 1	Verification of identity
AFNOR Class 2	Authorisation of a privilege
AFNOR Class 3	Proof of uniqueness
AFNOR Class 4	Identity search

Table 1: The four classes of services of biometric applications by AFNOR

With the term performance requirement, AFNOR in fact referred to the purpose and the underlying biometric functionality of the application (see Class 1 (1:1 comparison), and Class 3 and 4 (1:N comparison); however, see Class 2 (1:1 or 1:N comparison).

The consortium of BioVision itself also proposed a classification viewed from another angle: the benefit to the end user/operator:[110]

BioVision : Authentication of identity	For access control / for authentication of a transaction
BioVision : Personalisation	
BioVision : Authorisation	Tracking/tracing

Table 2: Classification in BioVision

In this classification, reference is made to the 'benefit' of the application. One could also describe this as the purpose for which the biometric application will be used. A classification only from the point of view of the benefit or purpose is in our view not sufficient. It is also important to know if a public or private entity is pursuing the purpose (see *below,* section 3.3.3, Type I and Type II applications), or the data subject itself (see *below,* section 3.3.3, Type IV a - Convenience model below) or whether or not public and private entities share the biometric information (see *below,* section 3.3.3, Type III – Mixed model).

The International Biometric Group (IBG), an industry's consulting and services firm[111], also attempted to make a classification of biometric applications according to its privacy friendliness.

[109] M. Rejman-Greene, (ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 October 2003, 12.

[110] *Ibid*., 34.

IBG : Privacy-Invasive	National ID, surveillance
IBG : Privacy-Neutral	Personal PDA, home PC, access control
IBG: Privacy-Sympathetic	Most application can incorporate privacy sympathetic elements
IBG: Privacy-Protective	Biometrics used to protect personal information

Table 3: Classification of biometric applications according to its privacy friendliness by IBG

The classification suggested by IBG above, however, does not convince because as a rule, it should be endeavoured to have all applications at least privacy-neutral, or even better, privacy-sympathetic and protective.

Others have attempted to map different types of biometric databases, depending on which kind of data that were used (raw data, templates called 'signatures' and other personal data). The models should enable a scenario-based discussion of privacy needs regarding the different types of (partial) biometric databases.[112] We do not believe, however, that a classification should be made solely on the basis of the type of the database and the kind of data in the database.

We nevertheless agree and believe that it is important to make an attempt to classify applications. For such classification, however, several factors should be taken into account in a consistent way. The way the control over the biometric reference template is exercised is one of the key factors of such an overview, but also so is the control over the capture and feature extraction as well as the comparison component. Other important distinguishing factors are the purpose of the biometric application and the biometric functionality. It is also important whether a governmental entity or a private party controls the biometric application, because the threats and risks are different. The threat of function creep and the resulting privacy risks, e.g., is especially relevant if the application is government controlled (Type I government controlled ID model – see *below*). From a data protection point of view, the data protection directive is applicable to the processing of biometric data by either public or private entities. However, it is also relevant to question to what extent private parties should be entitled to deploy the identification function of a biometric system and to identify persons.

A discussion about biometric systems will hence be easier to follow in the context of groups of relevant application models.[113] These groups should show common characteristics which are present in the biometric applications which belong to that group. The characteristics which are mentioned in section 3.3.3 in the table 5 below, and which are used to group the application examples, are in fact based on the way control is exercised and two other major criteria used in the data protection legislation. These criteria are based on the following two questions: (1) who is the data controller? and (2) what is the purpose of the application? As

[111] The International Biometric Group, IBG, should not be confused with the Biometric Working Group, BWG, a U.K. government forum for providing technical support and advice on biometrics to the government (see also *above* at footnote 31).

[112] A. Broemme, Discussion on Privacy Needs and (Mis)Use of Biometric IT-Systems, 5 et seq.

[113] See *supra* at footnote 109, 12.

mentioned before, such 'grouping' of the applications around these three criteria should facilitate the discussion about risks and advantages of biometric characteristic. The criteria with details for each of the groups that could be ascertained are further described *infra*, in table 5 in section 3.3.3 below.

The five main groups of biometric applications that could be distinguished according to the above mentioned three criteria are mentioned in the table 4 hereunder in the column 'FIDIS Deliverable 3.10' and are compared with the categories of AFNOR and BioVision. The table 4 shows how the categories of AFNOR and BioVision fit into the types introduced in FIDIS D3.10.

FIDIS Deliverable 3.10	AFNOR	BioVision
Identity applications (Type I)	Class 3 and Class 4	Authentication
Security and access control (autho-risation) applications (Type II)	Class 1 and Class 2	Authentication/ Authorisation/Tracing
Public/private partnership applications (Type III)	/	Authentication Authorisation
Convenience and personalisation applications (Type IV)	Class 1	Personalisation
Tracking and tracing (surveillance) applications (Type V)	Class 1	Tracing

Table 4: The five types of biometric model applications introduced in FIDIS D3.10 compared with the categories of AFNOR and BioVision

As stated before, the relevant questions which were asked in this regard are: by which entity are the biometrics used, for which purposes and functionalities, and what type of control is exercised ? By reviewing existing biometric applications, and by answering these questions, these five types of applications have been ascertained.

The fifth type, biometrics used for tracking and tracing, is only referred to in a limited number of cases in the further discussion of the privacy and security risks, not because that model is not deployed or biometrics are not fit to be used in that type of model, but because the Privacy Directive 95/46/EC often does not apply (in case of the processing for state security,….), because that model is not a good example of an identity management application and because details about the functioning of that kind of system are often not known.

Although biometric applications may at first sight belong to more than one group (e.g., for an access monitoring application, the persons who are subject to the monitoring system will in most cases be identified or identifiable), it is important to distinguish applications from other applications. For example, for access control applications, there are good reasons to defend that there is no need to use the identification functionality of the biometric. A mere comparison of the locally stored biometric characteristics for access control purposes is in most cases sufficient as previous identity control will have been done upon issuance of the card, and therefore no central storage of the biometric characteristics for identification

purposes is required. For government controlled ID applications, there may be a need to use the identification biometric functionality, however.

Based on the models and types described, the risks and advantages of biometrics can be better described, including the recommendations of how to improve the design of the biometric identity application.

3.3.2 Advantages and Disadvantages of the different control models

As stated in today's information security management systems standards such as ISO 27001, personal responsibility and control over every ICT system that has to meet certain, well defined security levels, are essential factors. Control typically has two aspects:

1. a technical component, spanning environmental infrastructure (buildings), communicational infrastructure (networks), systems (servers and other ICT components such as sensors and their operating systems), data storage, and applications (including corresponding software releases and configurations) and related data; and
2. an organisational component, spanning the behaviour of users and administrators of any of the mentioned technical components.

In addition, control can be applied directly (e.g. by the management of an organisation within the organisation) or it can be applied in a shared and trust based way (also called indirectly). In the latter case trust is typically based on contracts that include security service level agreements (SSLAs), audit schemes and optional fines in case of violation of SSLAs. Four types of control schemes have proven to be relevant in the context of security of biometric systems.[114] These types of control are further briefly described in a table in Annex 2 to this deliverable.

In this context biometric systems can be understood as ICT systems as they process digital data captured through a physical measurement process. Table 5 in section 3.3.3 *below* gives an overview of different implementations of ICT and biometric systems with respect to data storage, control and related data protection and security aspects.

Other aspects of the different control models are the type of the controlling entity (is it a public or private authority which controls the data processing?). For the Type I - government controlled ID applications there will be a need of legislative basis for the establishment of the system. Most risks are with the multilateral control model applications which we find in governmental controlled ID applications of Type Ic. The ICT systems may have many outstanding issues, such as access to the databases, the access procedure and the transfer to third countries.[115] At the same time, the best possibilities for effective abuse protection may be with a control system in which the data subject participates, as in Type IIc access control model applications. The characteristics of the control models depend on the architectural

[114] See for example M. Meints, 'Kontrolle und Datensicherheit', *Datenschutz und Datensicherheit* 3/2007, 208, Wiesbaden 2007 and M. Meints, 'Implementierung großer biometrischer Systeme', *Datenschutz und Datensicherheit* 3/2007, 189-193, Wiesbaden 2007, available at http://www.fidis.net/publications/#c1478

[115] See e.g., the discussion in the Council of Europe on the draft regulation for the use of VIS: X., *Note N° 8540/07*, Council of the European Union, 2007.

realisation of the control scheme. Later in this document (see *below*, section 6.3) an architecture with control between data subject and identity management system operator/controller is presented under 'encapsulated biometrics' that splits the control of the biometric system into the biometric processing devices (under the secured control of the operator/controller) and the biometric data (under the sole control of the individual that serves as the data subject).

Other aspects of the different control models are the procedure of enrolment and use of the system. The enrolment and the use of Type I – government controlled ID applications will in principle be done in prescribed conditions upon submission of specific evidence with specifically assigned personnel and use in the verification/identification stage will be done in the presence of officials which should attend to the system. This may not always be the case for Type II – access control models and Type III mixed model applications, and will not be applied in the Type IV – convenience model applications. The risks during enrolment and during use for each of these models are therefore different.

Other advantages and disadvantages of biometric applications could be described according to the control models which are given in the overview below.

3.3.3 Overview of different types of biometric applications

Biometric applications can be grouped into five categories or types:

Type I: Government controlled ID model

In this group, a public authority will take the initiative to collect the biometric data because of the identity verification or identification ability of the data, and include the data in an ID application, such as in ID cards, social security cards or passports. Control over the data could be central (Type Ia), divided over more than one organisation but with appropriate agreements in place (Type Ib) or multilateral (without appropriate agreements for the disclosure or transfer of biometric data) (Type Ic).

Type II: Access control model

In this group, a public or private authority takes the initiative to collect the biometric data to secure the access to a physical place or an online application. Control over the data could be central or divided over more than one organisation but with appropriate agreements in place (Type IIa and Type IIb) or divided such that the data subject shares the control (Type IIc).

Type III: Mixed model

In this group, the biometric data collected will be shared / exchanged amongst public and private authorities.

Type IV: Convenience model

In this group, either the data subject solely takes the decision to use biometrics for exclusive private convenience purposes (secure access to his / her house for authorised members) (Type IVa) or an organisation uses biometrics for simplification of an administrative process with central or divided control (Type IVb and IVc).

Type V: Surveillance model

In this group, a public or private authority takes the initiative to collect and process the biometric data for surveillance purposes.

Although most biometric applications will belong to one specific group, it may be that an application falls in two groups, e.g., a biometric system for a school may fall in both Type II and Type IV b or c.

	Controlling entity	Purpose/functional Requirements	Biometric functionality and place of storage	Examples	Type of control of biometric system	Control by Whom?	Data protection Directive	Information security	EDPS/WP 29/DPA Opinions /decisions
Type I : government controlled ID model	Public authority	Combating Identity fraud/Theft;	Identification (1:*n*) and verification Central and local storage	National eId cards, national social security allowances	Type I a Central Control Control of biometrics is central and direct	By one organisation	Is applicable	Information security management standards such as ISO 27001 can be applied	Yes
	(national or local government)	Avoidance of double dipping	Identification (1:*n*) Central storage	Eurodac, VIS, SIS II	Type I b Divided Control with trust Control is partially indirect via contracts	By one or several organisations jointly	Is applicable	Information security management standards such as ISO 27001 can be applied – recommendations for "outsourcing" can be used	Yes
		Combating Identity fraud / Document fraud Other	Identification (1:*n*) or Verification Central or local storage	EU ePassports	Type I c Multilateral Control Control is divided amongst multiple Parties (operators and/or data subjects	By several organisations, in some cases with concurring security targets	Is applicable	Information security management standards such as ISO 27001 **do not adequately cover this situation** (see also Annex 2)	Yes

	Controlling entity	Purpose/functional requirements	Biometric functionality and place of storage	Examples	Type of control of biometric system	Control By Whom ?	Data protection Directive	Information security	EDPS/WP 29/DPA Opinions /decisions
Type II :Access control model (physical or online) for employees, customers or citisens by government or private organisation)	Public authority (national or local government)	Securing online access / Identity management for internal or external online network (intranet ; e-government or commercial web service)	Identification (1:*n*) or Verification Central or local storage (e.g., on card, token)	E-government applications such as Tax-on-Web in future? (Belgium) Pay per Touch	IIa Central Control or II.b Divided with	By one or several organisations	Is applicable	Information security management standards such as ISO 27001 can be applied	
	or Private organisation	Securing physical access to government or corporate buildings (identity control or use of card control)	Identification (1:*n*) or Verification) (1:1) Central or local storage	Time and Attendance) US Department of Defence Common Access Card		By one or several organisations	Is applicable	Information security management standards such as ISO 27001 can be applied	Yes
	Public or private organisation and data subject	Securing online access / Identity management for internal or external online network	Identification (1:*n*) or Verification (1:1) Locale storage on token	Encapsulated biometrics (Swiss banks)	IIc Divided control with data subject	By one or several organisations ànd the data subjects	Is applicable	Information security management standards such as ISO 27001 can be applied	?

Sub-table 5.2: Type II : Access control model

	Controlling entity	Purpose/functional requirements	Biometric functionality and place of storage	Examples	Type of control of biometric system	Control By Whom ?	Data protection Directive	Information security	EDPS/WP29 /DPA opinions/ decisions
Type III : Mixed model	Public/private Partnership	Security, border control	Identification or Verification	Privium		By several organisations from public/private sector	Is applicable	Same as above	?

Sub-table5.3: Type III : Mixed model

	Controlling entity	Purpose/functional requirements	Biometric functionality and place of storage	Examples	Type of control of biometric system	Control By Whom ?	Data protection Directive	Information security	EDPS/WP29 /DPA opinions/ decisions
Type IV : Convenience model	Data Subject	Private purposes: security / access control / convenience	Identification or Verification Central or local Storage	Home PC, home access, personalised car use,	Private system used and controlled by natural person for purely personal or household activities Type IV a Control Purely private purposes	Full control by data subject	Is NOT applicable	Information security standards, especially ISO 15408 (Common Criteria) and partly ISO 27001 can be applied	?
	Public authority or Private organisation	Convenience Administration	Identification or Verification Central or local storage	Home protection Administration of school meals	Type IV b Central or IV c Divided Control with trust	By one organisation	Is applicable	Information security management standards such as ISO 27001 can be applied	Yes

Sub-table 5.4: Type IV : Convenience model

	Controlling entity	Purpose/functional requirements	Biometric functionality and place of storage	Examples	Type of control of biometric system	Control By Whom ?	Data protection Directive	Information security	EDPS/WP29 /DPA opinions/ decisions
Type V Surveillance model	Public authority (civil or criminal) or Private organisations	Surveillance Tracking & Tracing	Identification	Superbowl Florida	Type Va Central or V b Divided Control with trust Central or Divided Control with trust		Is applicable unless Art. 3.2 Directive applies (public security, State security,..)	Information security management standards such as ISO 27001 can be applied	Yes

Sub-table 5.5: Type V : Surveillance model

Table 5: Different control models and types of biometric systems

From the perspective of the European data protection framework, private ICT and biometric systems which are only used for purely personal or household activities by a natural person without any other (central) controller are out of scope as data protection legislation does not apply (Article 3, al. 2, §2 of the Privacy Directive). An example is the use of biometrics for access control to a home PC purchased and used for purely private reasons by an individual. Another example is the purchase and use of a biometric home access control system. For this reason they are not discussed further.

Concluding remarks on Chapter 3

Chapter 3 described various features and technical characteristics of biometric systems. For this purpose, the general reference model was used as a starting point and it was completed with a detailed explanation on the biometric evaluation process, including several definitions of quality parameters derived from the measurement statistics in biometric systems. This description should allow the understanding of quality factors which are often stressed in the evaluation of biometrics systems, such as the statistical error factors. It has to be clear that all purely statistic quality factors do not give any clue on the security against dedicated impostor attacks with forged biometric characteristics.

The technical characteristics and limitations of biometric systems are rarely taken into account in the legislation and regulation of biometrics. They are relevant because there seems to be a tendency that biometrics become an important key in the various information systems, starting with VIS and SIS II. Furthermore, biometric technologies should be put in the right context of security and data protection schemes. Chapter 3 proposes finally to use five categories to classify biometric systems, which should facilitate further discussions about risks and advantages of biometrics in real world applications. In such debate, it is equally important to use an accurate and appropriate vocabulary on biometrics, as argued in Chapter 3 as well.

4 Security and privacy aspects of biometrics

The debate about biometrics is most of the time framed in two ways which seem incompatible with each other. Some advocate the introduction of biometric applications for increasing security, for examples in air travel or at sea ports, and hereby accept that this is done at the cost of the privacy and the fundamental rights and freedoms of individuals (advocates of biometric applications for increasing security). Others reject the use of biometrics because of the risks for the infringement of privacy rights when using biometric applications in the name of (public) security (privacy advocates). Choosing or rejecting biometrics is herein presented as a choice between either security or privacy.

The debate about biometrics could also be held in another way: if the design, the development and the deployment of biometric applications takes the privacy risks into consideration, biometrics could be advanced as both enhancing security while conserving privacy. Iris scans, as an example of the biometric Type II access model, could be very useful in protecting high security installations, while the iris does not leave persistent traces and would only be required from a limited number of persons who have access to these restricted places. Some authors have already tried to argue that both concepts of 'security' and 'privacy' do not need to exclude one another. Biometric applications could enhance the security if all privacy threatening elements have been dealt with.[116] Security and privacy are then no longer two different sides of the (biometric) story, but, if both concerns taken into account in equivalent ways, both will strengthen the biometric application. Biometric applications, however, become insecure if the privacy rights and risks are insufficiently dealt with. If the biometric characteristic that is used leaves traces, and can in the application easily be spoofed, the security obtained by the use of the biometric for that application decreases significantly, unless specific measures take this privacy risk into account and prevent such abuse. So the security of an application will equally decrease if privacy risks remain. The security of the application will remain high if privacy interests are equally dealt with.

This chapter will summarise the security and privacy risk aspects of biometrics.

4.1 Security aspects of a biometric system

In the previously presented reference model (see *above* figure 3) of a biometric system, we can identify a number of potential points of attack. These attack points vary in function of the operation mode (identification or verification) and the control model. The main risks of a biometric system have been compiled by several IT security and certification organisations. An example of such a compilation can be found in the ISACA auditing guidelines G36 Biometric controls.[117] An extract of such a risk list is presented in the table below. The references in the 4th column refer to Figure 11:

---

[116] One element is also the privacy-friendliness or unfriendliness of the different biometric characteristics. The International Biometric Group has tried to make a useful classification of the biometric characteristics in this regard. See also *supra*, footnote 111.

117 See http://www.isaca.org/Content/ContentGroups/Standards2/Standards,_Guidelines,_Procedures_for_IS_Auditing/IS_Auditing_Guideline_G36_Biometric_Controls.htm

Regardless of any details of a specific biometric system, it is always true that general design principles to make a system more secure also apply to biometric systems. Such concepts are compartmentalisation, defence in depth, shared control, tamper resistant devices, security audits and certifications and other methods and techniques.

Risks	Examples	Possible Countermeasures	
Spoofing and mimicry attacks	Artificial finger used on fingerprint biometric device	Multimodal biometrics, vitality detection, interactive protocol	1,2, 8
Fake reference template risk	Fake reference template stored in server or supplied during enrolment	Encryption, intrusion detection system (IDS), supervised enrolment	1,2, 6,7,8,
Transmission risk	Data intercepted during transmission during enrolment or data acquisition	Interactive recognition, rejection of identical signals, system integration	1-7
Component alternation risk	Malicious code, Trojan, etc.	System integration, well-implemented security policy	5,6,9
Enrolment, administration and system use risk	Data altered during enrolment, administration or system use	Well-implemented security policy	1-7
Similar template/similar characteristics risk	An illegitimate user has a template similar to a legitimate user.	Technology assessment, multimodal access, calibration review	1-6
Brute-force attack risk	An intruder uses brute force to deceive the system.	Account lock after number of unsuccessful attempts	1
Injection risk	Captured digital signal injected into authentication system	Secure transmission; heat sensor activated scanner (warm body present); date/time stamps in digital representation of images	4
Users' rejection	The invasive nature of biometrics techniques could cause users to reject using the system.	Training and awareness of users and the selection of the least intrusive technique possible	1
Changes in physical characteristics	Some techniques depend on face or hand characteristics, but these human aspects change with the years.	Monitoring of template evolution during use of system	4,5,6
Cost of integration with other legacy systems	Coherence with other techniques used for legacy systems than have to be integrated	Cost-benefit analysis	9
Risk of loss of data	Hard disk/hardware failure	Data backup and restoration	6,9
Risk of biometric data dissemination	Exchange of biometric data between operators without consent of data subjects	No storage of raw data, limit for the lifetime of a biometric template, encapsulated storage of biometric data in the hand of the data subject	2,3,4, 6

Table 6: Main risks of a biometric system

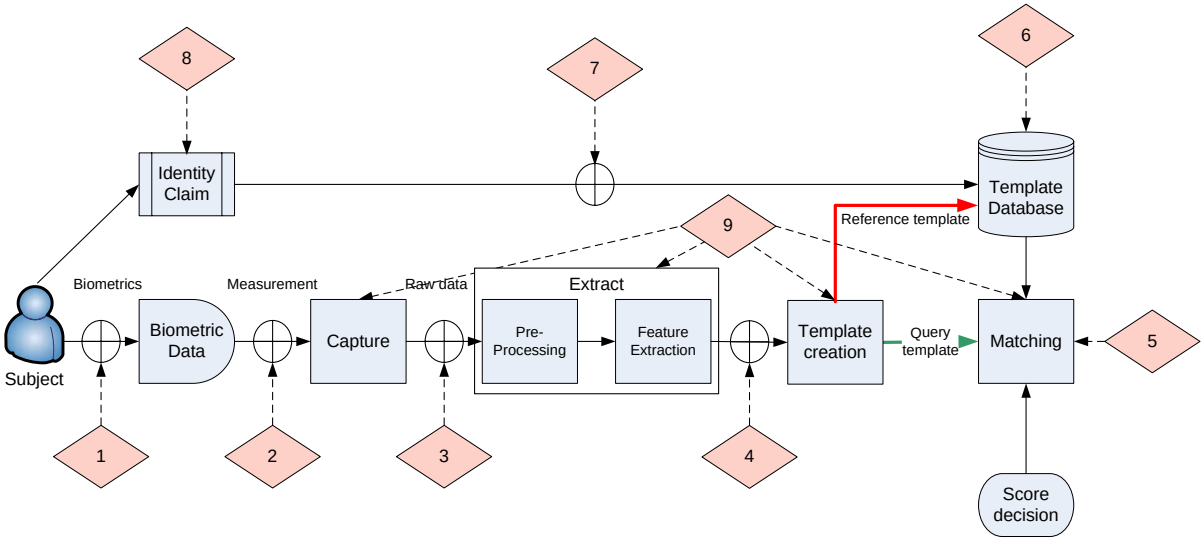

Figure 11: Fault sensitive points of a biometric system:

1. Spoofing of biometric identifier by physical entity
2. Spoofing of biometric identifier data by electronic data manipulation
3. Alteration of captured data
4. Alteration of template
5. Manipulation of matching algorithm or policy
6. Alteration or dissemination of reference template
7. Error introduction in transmission of identity claim (verification mode)
8. False identity claim during query or enrolment step)
9. Manipulation of system components, DoS

The problem of impostors spoofing biometric credentials of another person, however, is not an intrinsic problem of biometrics only. There are certainly much easier and therefore more frequent attacks on secret based credentials (PIN, password, passphrase etc). But the issue of biometric spoofing is often discussed in the community of security professionals. In this report we will discuss the threats and methods of impostors to biometric systems more in depth in section 4.4.

4.2 Proportionality and Revocability

4.2.1 Revocability

Today, spoofing of biometric sensors and, as a result, identity theft and identity fraud using biometric systems is a realistic security threat (see section 4.4 and Geradts 2006). The consequences can be severe and long lasting for the operators and users of biometric systems, because physical or behavioural features such as the face, the finger tips or the gait cannot be changed easily.[118]

[118] See M. Gasson, M. Meints, *et al*., (eds.), *o.c.* at footnote 3.

As a solution to this problem, the use of biometrics in combination with additional, revocable factors of authentication such as possession or knowledge have been suggested in the late 1990s (e.g. by Cavoukian in 1999[119]), has been taken up by other authors (e.g. Clarke 2002[120]) and is held up as a relevant measure (e.g. by Cavoukian in 2007[121]). Nevertheless, many of today's systems do not implement biometrics in a revocable way. One example of this is the European passport.[122] The reason seems to be that currently no standardised and cost efficient solution is available that can be easily integrated into the various biometric systems. There are some new approaches like match-on-card or even system-on-card (see *below*, section 6.2.2) that may solve the problem of revocability, but in today's implementations they are rarely integrated (see 6.3). Research to improve the revocability of biometrics by using specific cryptography alternatives is ongoing.[123]

The revocability of biometrics is important for all biometric models, but it is clear that it is most crucial in the Type I government controlled ID model, where the use of the biometric identifier is mandatory for individuals in ID related documents. It is also important in the Type II a and b Access model and the Type III Mixed model as described in section 3.3.3, where the biometric used in the aforesaid documents and tokens is used in relations with the government and/or private organisations for access purposes, e.g., to e-government services or commercial banking. If the biometric has been compromised and it cannot be revoked, the relations of the individual with the government and other concerned organisations will become severely damaged, if not impossible.[124] Revocability is less of an issue for the Type IV a Convenience model, as an individual could in that case still choose to no longer use the biometric application (e.g., for access to the house, etc) or, in case the template is compromised, and cannot be replaced, change to another method for authentication (e.g. another biometric method, a chip card or even a username-password-combination). If the biometric system is compromised, the user may eliminate it from the authentication process. Revocability is intrinsically realised in Type II c models ('encapsulated biometrics'), where the biometric template data is never accessible to persons other than the owner. A lost or out of date device incorporating such data cannot be abused as the data can technically not leave the device. Once a device that carries an 'encapsulated biometric' system is out of service, the stored biometric data is lost and thus revoked.

---

[119] See A. Cavoukian, *Privacy and Biometrics*, Information and Privacy Commissioner, Ontario, Toronto, 1999, available at http://www.pco.org.hk/english/infocentre/files/cakoukian-paper.doc.

[120] Clarke, R., 'Biometrics' Inadequacies and Threats, and the Need for Regulation', Presentation on the Computers, Freedom & Privacy 2002; see http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html

[121] A. Cavoukian and A. Stoianov, *Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, Information and Privacy Commissioner, Ontario, March 2007, 48 p.

[122] M. Meints, M.Hansen (eds), *o.c.* at footnote 26.

[123] See P. Tuyls and J. Goseling, *Information-Theoretic Approach to Privacy Protection of Biometric* Templates, Eindhoven, Philips Research, 2004, referred to by E. de Leeuw, 'Biometrie en national identiteitsmanagement', *Privacy & Informatie*, 2, 2007, footnote 22.

[124] See J. H. A. M. Grijpink, "Een beoordelingsmodel voor de inzet van biometrie", *Privacy & Informatie* 2006, vol. 1, 14-17.

4.2.2 Proportionality

Proportionality is another very critical aspect of biometrics. It is often raised and referred to in general terms, without much further explanation. The question rises as to the meaning of the proportionality principle, how the review is done and which factors are taken into account. In this report, it is not the intention to describe in detail the proportionality check that is or should be made by each DPA in their national countries.

The proportionality principle refers to a general principle of law that requires in general a fair balance and reasonable relationship between the *means* requested or used, including the severity and the duration of the means, and the *objective* sought. The proportionality principle has its origin mainly in public law, where it, as developed in case law and legal doctrine, lays down some fundamental rules for justifying state interference with fundamental rights and freedoms of individuals. The proportionality principle is not only relevant for the right to privacy, but also to other fundamental rights (e.g., the freedom of expression), which are, for Europe, laid down in the European Convention of Human Rights of 1950 ('ECHR') and the Convention on Civil and Political Rights.

In case law and legal doctrine, there is in addition and in combination with the proportionality of the measure, also the requirement that the interference serves a 'legitimate aim' (finality principle) and that the interference shall be 'prescribed by law' (legitimacy principle). 'Prescribed by law' means that that there shall be either a written legislative act or a 'rule of law' which justifies the interference, to the extent this law is sufficiently precise and adequately accessible.[125] The finality principle requires that restrictions are only imposed for lawful and legitimate purposes. The proportionality principle, which allows certain restrictions to fundamental rights and obligations, applies in addition to these two principles and requires that even if one has a legitimate purpose for such restriction, prescribed by law, the restriction needs to be in proportion with the aim sought and 'necessary in a democratic society'. Legal scholars have written a lot about the meaning of this proportionality principle and requirement. One could summarise that the proportionality principle is a bundling of two requirements: (a) the restriction has to be *relevant* for the purpose sought (or there must be a 'pressing social need' to restrict) and (b) the restriction needs to be *proportionate* to the legitimate purpose pursued.

Traditional legal doctrine in principle proclaims that the fundamental rights and freedoms of the ECHR are only guaranteed to the individual in his relationship with the government. There is however an important evolution in that more and more scholars defend that the fundamental rights and freedoms shall also be valid and applied amongst private parties ('Drittwirkung').[126] This implies that fundamental rights and freedoms, such as the right of privacy, can also be enforced amongst private parties. As a result and by analogy, private

[125] See also e.g., *Sunday Times*, ECHR,26 April 1979, *Serie A*, Vol. 30, §49. In this decision, the Court found that the Sunday Times was not rightfully enjoined from publishing a further article on the use of a dangerous drug (relying on Article 10 (freedom of expression)) as this injunction – which sought to protect the legitimate aim of upholding the authority of the judiciary - was not 'necessary in a democratic society').

[126] For one of the first legal scholars to defend the direct effect amongst private parties, see A. Drzemczewski, *European Human Rights Convention in domestic law*, Oxford, Clarendon Press, 1983, 199. See also the judgement of the European Court of Human Rights of 10 April 2007 in the case of Evans v. the United Kingdom, in which Article 8 was applied in a conflict between two private individuals (see paragraph n° 73).

parties will also be confronted with limitations to these fundamental rights and freedoms, in accordance with the same principles of legitimacy, finality and proportionality.

If we now look at the framework relating to data protection, we notice that the principles of legitimacy, finality and proportionality, which clarify the criteria for restrictions to fundamental rights, are also expressly incorporated in Article 6 of the Directive 95/46/EC. They are set forth as the criteria and principles which should guarantee a certain *data quality* in relation with personal data processing.

(i) The legitimacy principle states that personal data shall be processed 'fairly and lawfully' (Article 6 of the Directive 95/46/EC). The notion of 'fairly' is quite general and refers to several observations. Some authors include in the notion a reference to the interests and reasonable expectations of data subjects[127], a requirement that a person is not unduly pressured into providing data about him-/herself and that the processing of the data is transparent.[128] Bygrave states that the notion of 'fairly' in itself already contains a notion of balance and proportionality. 'Lawfully' implies that the processing is in accordance with the national data protection legislation, in accordance with other laws and statutory provisions, legally enforceable obligations (e.g., binding agreements) and legal competences. We see that for Type I government controlled ID model, the legislator will attempt to provide a legal basis for the collection and processing of biometric data. This is often criticised, as such law or other legislative measure is not always very balanced and is often incomplete in terms of providing sufficient guarantees to the data subject for security and integrity.[129]

(ii) The purpose or finality principle. The second core principle of data protection that is relevant is that the data shall be collected for specified and lawful/legitimate purposes. This principle is in fact a cluster of three sub-principles, i.e., 1) the purposes of the data collection shall be specified, 2) the purposes shall be lawful / legitimate, and 3) further data processing shall not be incompatible with the original purposes. Owners of biometric systems hence need to specify the purposes for which the biometric data will be used. This is often a problem for the Type I government controlled ID model[130], and sometimes also the Type III Mixed model.

(iii) The proportionality principle. The third core principle requires that the personal data shall be adequate, relevant, and not excessive in relation to the purposes for which they are processed. There are no legal provisions on interpretation of this principle and there are very few guidelines on what criteria shall be used. The criteria for the application of the principle, even if the principle is embedded in a legal provision, are debated, in particular in the context of the enforcement of fundamental human rights (see also *above*). Therefore, it is necessary to see how this principle is applied by reviewing the decisions of the national courts and the European Court of Human Rights in relation with privacy rights and other rights, to see how it is applied by the national DPAs and courts in relation to biometric systems and to derive, if possible, conclusions for such systems.

---

[127] R. JAY en A. HAMILTON, *Data Protection. Law and Practice*, London, Sweet & Maxwell, 2003, 155-156.

[128] L. A. BYGRAVE, *Data Protection Law. Approaching its rationale, logic and limits*, in B. HUGENHOLTZ en E.A. (eds.), *Information Law Series* , The Hague, Kluwer Law International, 2002, 58 – 59.

[129] An example is the inclusion of biometrics in e-passports and other MRTDs. See M. Meints, and M. Hansen, *o.c*. at footnote 26, 60 - 62.

[130] M. Meints and M.Hansen, *o.c*. at footnote 26, 63-66.

The Article 29 Data Protection Working Party discussed in its opinion the use of biometric data for access control purposes[131], and stated in this context that the way biometric data could be stored, i.e., in a central way or on an object exclusively under the control of the data subject, will determine to what extent the fundamental rights of individuals are at risk. The central storage of biometric data poses more risks, in particular for so-called 'function creep' (the risk that the data are used for secondary purposes which are not compatible with the purposes for which the data were initially collected) and the linking of information in several databases. At the same time, the Article 29 Data Protection Working Party stated that such central storage could be permitted for high security installations. The Article 29 Data Protection Working Party touches other criteria, such as the kind of biometric (e.g., the outline of a hand as opposed to fingerprint is more proportionate) and the way biometric data are digitalised. The criteria for deciding upon the proportionality of the use of biometrics, however, are not stated in the Directive and remain therefore unclear.

Nevertheless, the DPAs apply the proportionality principle as a decisive criterion in their decisions. The French DPA (CNIL) stated it as follows in an opinion of 8th April 2004 : '*It is in the light of the whole of these reflections that the Commission shall appreciate, in each case, if the use of biometric recognition techniques and the set up of a data base, because of the physical identification characteristics of biometric elements and the possible uses of the established data base, are fit and in proportion with the purposes'*.[132] The DPAs and the courts hence review whether the use of biometric identification techniques is lawful and in proportion with the purposes of the application based upon Article 6 of the Directive 95/46/EC.

The use of biometrics in private sector applications has until now received less attention than the intended use of biometrics in applications of the public sector, such as in passports and travel documents, visas and VIS and SIS II[133]. The deployment of biometrics in this context has caused tumult as the legal texts which intend to introduce such use in the public sector were often too general with regard to the purpose specification and did not provide adequate safeguards for the individuals in relation to the (security) risks involved. The deployment of biometrics in private sector applications however also requires attention.

The advisory opinion of the Article 29 Data Protection Working Party of 2003 on the application of the data protection principles on biometrics in general, which is general in nature, remains relevant for an evaluation of this proportionality issue in the private sector.[134] The Article 29 Data Protection Working Party pointed out in this opinion that in its view the principle of purpose and proportionality is a decisive factor in the legal review of biometric systems by the DPAs. The Article 29 Data Protection Working Party hereby also referred to

---

[131] This could be compared with the biometric Type II Access model suggested in this report.

[132] Opinion N° 04-018 of 8 April 2004 of the CNIL on the request for opinion by the Hospital of Hyères relating to the employment of a fingerprint verification application for the management of the employees' time and attendance. See also *above* at footnote 49. The original text reads as follows : '*C'est au regard de l'ensemble de ces considerations qu'il y a lieu pour la Commission d'apprécier, dans chaque cas, si le recours à des techniques de reconnaissance d'éléments biométriques et la constitution d'une base de données sont, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données ainsi constituées, adaptés et proportionnés à la finalité assignée au dispositif*'.

[133] These could be compared with the biometric Type I government controlled ID model suggested in this report.

[134] See also *supra* at footnote 8.

Article 6 of the Directive 95/46/EC that requires that '(…) personal data must be (a) processed fairly and lawfully, (b) collected for specified, explicit and legitimate purposes (…)' and that the data shall be 'adequate, relevant and not excessive (..)'. The Article 29 Data Protection Working Party however did not further clarify how these principles are to be applied.

Proportionality means in practice that a biometric application is used to link the biometric sample with the necessary and sufficient attributes of the identity of an individual to allocate the rights or authorisations that the specific individual is entitled to in the application context. The term of proportionality can be explained in the triangle of a value transaction between two parties (see Figure 12). The requesting party undergoes an authentication process (e.g. biometric recognition), that identifies the identity attributes necessary and sufficient to define his rights in the context of the transaction. This enables the delivering party to give the requested allowance to the rights requesting party. Proportionality means that the allowance delivering party collects only the necessary and sufficient identity attributes to correctly define the rights of the allowance requesting party. It especially means that biometric recognition should not be used for any other purposes than for the specific application within which the individual delivered his biometric sample data. Any evaluation of biometric data outside the context of the immediate application potentially violates the request for proportionality. It is clear that the proportionality issue is a crucial point in any identification process that does not have the full approval of the individuals involved. Such an involuntary identification may violate the proportionality criterion. However, there are applications, especially in the context of fraud and forensics where individuals are not cooperative, where the notion of proportionality has to be extended to the basic purpose of the identification process. It is possibly not a violation of proportionality if passengers of an airline are screened against templates of known terrorists as long as the biometric data of the screening are not used for other purposes and there is a legal basis for this practice.

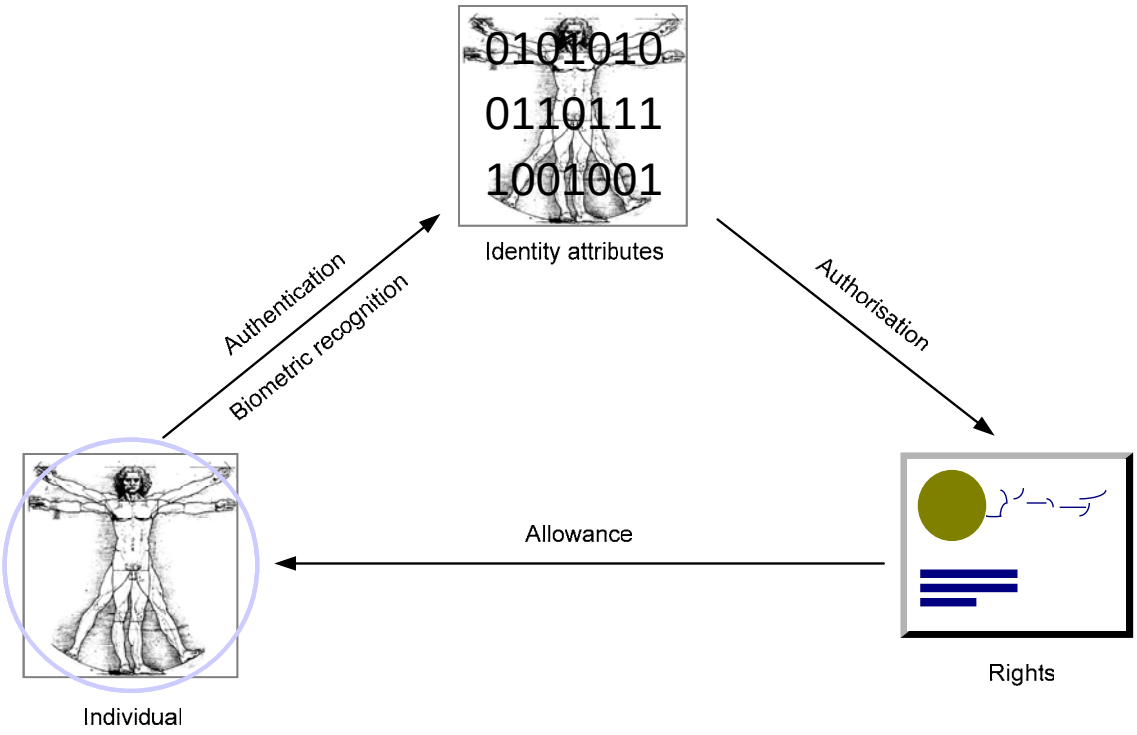

Figure 12: The triangle of a value transaction and the use of biometric recognition

One should know that the proportionality principle is also closely connected to the margin of appreciation doctrine. This doctrine finds its origin in administrative law of civil law jurisdictions according to which administrations are granted some 'discretion' or 'freedom' in taking decisions in application of a rule.[135] If there is no clear answer as to which interest outbalances the other, the margin of appreciation for the court will increase. This means that if there are no concrete guidelines as how to apply biometrics, DPAs and courts have more freedom to decide whether the application is 'fairly and lawful' and 'proportionate'.

The margin of appreciation of the national DPAs and the different interpretations by the DPAs of when a biometric system infringes the individual fundamental rights is now exactly the opposite of what the Article 29 Data Protection Working Party in its opinion of 1st August 2003 tried to establish. The Article 29 Data Protection Working Party said it as follows:

> 'The purpose of the present document is to contribute to the *effective and homogenous application of the national provisions on data protection* adopted in compliance with Directive 95/46/EC *upon biometric systems*. (…) The Working Party intends to provide uniform European guidelines, particularly for the biometric systems industry and users of such technologies'.[136]

The proportionality principle, a main principle in the evaluation of biometric applications and models, therefore leaves many open questions and provides no concrete guidance as how to design and implement biometric models.

Since the functionalities of biometrics (i.e. identification and verification) which serve a specific purpose (e.g., avoidance of 'double dipping', securing proper use of an employee card, etc) need to be clearly distinguished as explained above (see section 2.3), we believe that a first step would be to clearly link these functionalities to a specific type of application.

The Council of Europe has set forth this idea in general terms in 2005 as follows:

> *'In choosing the function of verification or identification, much depends on the purpose to be served by the biometric system and the circumstances under which it is to be applied. The function must serve the purpose for which data have been collected and not amount to an overkill. The same statement would be in legal terms : the instrument should not be disproportionate in relation to the purpose it has to serve. The choice of an identification system in cases where a verification system would be sufficient to serve the envisaged purpose needs special justification. Verification problems should not be solved by identification solutions.'* (underlining added)[137]

---

[135] See Y. Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Antwerp-Oxford-New York, Intersentia, 2002, 14; see also N. Emiliou, *The Principle of Proportionality in European Law. A Comparative Study*, London – The Hague – Boston, Kluwer Law International, 1996, 288 p, and W. Van Gerven, 'Principe de proportionnalité, abus de droit et droits fondamentaux', *J.T.* 1992, 305-309.

[136] *Ibid*., 3.

[137] Council of Europe, Progress report on the application of the principles of convention 108 to the collection and processing of biometric data, Strasbourg, February 2005, 22.

4.3 Privacy problems

For a description of the privacy problems of biometric systems, an analysis of the privacy problems of biometrics will in principle start from the issues which were described in the opinion of the Article 29 Data Protection Working Party (Article 29 Working Party) on biometrics of 1st August 2003.[138] The privacy problems which were put forward in this opinion will in this document not be discussed at length since this was already done in FIDIS deliverable 3.2*: A study on PKI and biometrics*.[139] The overview of the privacy problems given in that working document of the Article 29 Working Party, however, remains valid as a starting point for the present report. For a proper understanding, the main privacy concerns which were outlined in that document are hereunder represented again, in brief, in a schematic overview.

Privacy Risk	Storage	Qualifying factors	Data Protection principle	Suggested remedy in WP 80 to counter risk
Identification	Central storage	Size of database Type of biometrics used	Proportionality Art. 7	
Biometrics contain sensitive information (health, race)	Central (or local) storage		Prohibition to process sensitive data Art 8 Data minimisation Art. 7	No images Use of templates which exclude such information
Secret capture and/or surveillance	Central storage	Especially vulnerable are low-level intrusiveness biometrics (e.g., face, voice), but also fingerprint, …	Fair collection and processing Art. 6 (a)	Local storage under control of data subject
Incompatible re-use (‘function creep’)	Central storage		Special risks to rights and freedoms Art. 20	Prior checking with DPA
Theft	Central (or local) storage		Appropriate technical and organisational security measures Art. 17	Appropriate security measures Including revocability of templates and impossibility to reconstruct biometric

[138] See *above* at footnote 8.

[139] See *above* at footnote 23, 101-105.

				raw data from template
Use as unique identifier for connecting databases	Central storage	Use by governments	Conditions to be determined Art. 8 § 7 Right to object Art. 14 (a)	Mathematical manipulations
FAR/FRR	Central or local storage	Type of biometrics used	Prohibition of automated decisions Art. 15	Re affirmation of outcome, appropriate back-up procedures

Table 7 : Overview of privacy risks of biometrics as stated in WP 80

Almost all of the privacy concerns which were described, in fact relate to biometric Type I , II and III models (for the models, see *above*, section 3.3) and the use of biometrics in these models requires special attention for the reasons set out above. The risks also relate most often to the place of storage of the biometrics. In the case where the biometric characteristics are stored in a central place, the risk increases. The Article 29 Working Party has already warned that setting up a centralised database containing personal data and in particular biometric data of all (European) citizens 'could' infringe the proportionality principle.[140]

There are however additional concerns which the use of biometrics raise. The Article 29 Data Protection Working Party already stated in its opinion that the document was only a 'working document' which it intended to revisit in the light of the experiences of data protection authorities and technological developments linked to biometric applications.[141]

Some of these additional privacy concerns and issues under the framework of the data protection legislation are hereunder identified and further described.

Data quality

One of the privacy problems which need to be further investigated is in relation to the data quality of specific biometric data, such as face scan and hand geometry, for specific groups of people. Such a group is that comprised of children and teenagers, which is likely to have a higher risk of processing of inaccurate or outdated biometric data.

One of the basic principles of the data protection legislation as set forth in the Directive 95/46/EC is the data quality. The principle requires that the personal data must be '*accurate*, and, where necessary, *kept up to date*'; furthermore, 'every reasonable step must be taken to ensure that *data which are inaccurate* or incomplete, having regard to the purposes for which they were collected or for which they are further processed, *are erased or rectified*' [emphasis added].[142] This requirement with regard to the data quality poses a problem for specific forms of biometric data which relate to a human characteristic that changes over time, for example,

[140] Article 29 Data Protection Working Party, *Opinion on Implementing the Council Regulation (EC) N° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 30 September 2005, 8.

[141] See *above* footnote 8, 11.

[142] Article 6.1 (d) of the Privacy Directive 95/46/EC.

if the individual grows older. The reference biometric data relating to hand geometry or the face of younger persons, for example pupils of a school, at a certain point may not be of good quality anymore, as the characteristics change and these changes are not reflected in the reference data. This problem has been recognised in relation to the use of the facial image of children for the use of identity documents in a study performed for the Ministry of the Interior in the Netherlands in 2005.[143] The report stated that 'it is very likely that facial recognition of children of twelve years or younger, on the basis of a reference image that is some years old, is problematic. The reason is the significant changes in the proportions of the characteristic points in the face during growth. These changes take place after a complex process that is to a large extent determined by the sex and genetic background'.[144] Furthermore, the report stated that the problem also exists for children older then twelve, and that additional research on this topic is needed. The data quality of the reference biometric data of younger persons (for example, under eighteen) is therefore a concern, not only from a practical point of view, but also under the data protection legislation, which imposes requirements for the quality of the data, in particular that the data shall be accurate. Inaccurate data would lead to increased False Acceptance Rates (FAR) and False Rejection Rates (FRR) and would render the whole biometric application unreliable. FAR and FRR also pose risks for the data subjects, by either having somebody else in your place identified for the service or by being wrongly rejected.

While biometric applications are sometimes promoted in schools or other environments involving children, for convenience and other purposes (for example the administration of meals)[145], this privacy concern should not be neglected and the efficiency of the whole biometric application could become questioned if there are no appropriate (technical) measures implemented to solve this problem. In the absence of such technical measures which should ensure that the reference data do not become outdated too soon, the inaccurate data shall be kept up to date. This would mean that the reference data needs to be replaced at regular intervals with new reference data by a new enrolment of the data subject. If this would not be possible, the data shall not be used any longer and is to be erased. The administrative and operational requirements for such replacement and the consequences of this principle is most important for the biometric Type I government controlled ID model; the importance remains but decreases in the biometric Type II Access model, the Type III mixed model and the Type IV convenience model.

Data quality of face recognition in general

In preparation of the introduction of the e-passport in Europe, two relevant tests of face recognition systems using biometric face reference data standardised by the International

---

[143] X., *2b or not 2b. Evaluatierapport. Biometrieproef. 2b or not 2b,* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2005, available at http://www.minbzk.nl/onderwerpen/persoonsgegevens_en/reisdocumenten/publicaties?ActItmIdt=54771 (last visited on 16 January 2007).

[144] *Ibid.*, 15.

[145] See, for example, the debate about the use of biometrics in schools in the United Kingdom, W. Grossman, 'Is School fingerprinting out of bounds?', Guardian, 30 March 2006, available at http://technology.guardian.co.uk/weekly/story/0,,1742091,00.html (last visited on 4 January 2007). The debate about the use of biometrics in school is to a lesser extent also held in other countries, see e.g., press releases about the introduction of the use of fingerprint in a school in Luik, Belgium in February 2007, available at http://www.nu.nl/news/966081/21/Belgische_school_eist_vingerafdruk_tegen_spijbelen.html and http://www.waarmaarraar.nl/pages/re/9907/Leerlingen_moeten_met_vingerafdruk_school_in.html (last visited on 5 July 2007).

Civil Aviation Organisation (ICAO) were carried out by the German Federal Office for Information Security (BSI)[146] and the Ministry of Interior of the Netherlands. The results were summarised and analysed in the FIDIS deliverable 3.6 (V. 1.1, pp. 25-26). In general 2D face recognition accuracy could not compete with fingerprinting and iris scan, and the use of ICAO-compatible reference data seemed to decrease the quality compared to vendor-proprietary templates. As a consequence most European counties currently do not intend to use 2D face recognition for border control purposes yet, among them Germany – instead fingerprinting is planned to be used.[147]

In March 2007 the results of the "Face Recognition Vendor Test 2006" were published by the (U.S.) National Institute of Standards and Technology (NIST).[148] One of the remarkable conclusions of this report is that now face recognition can well compete with the quality of fingerprinting and iris scan. Looking into the details of the set up for the testing it has to be pointed out that no ICAO-compliant reference data format has been used, so these results can not be compared directly with the previously mentioned test results from 2005. In fact the best results were achieved with high and very high resolution pictures (resolution of 4 Mbit and higher) or 3D face recognition. Especially low resolution, use of compression (JPEG picture format) and non-standardised light conditions led to results that were not impressive (FRR higher than 5% with FAR = 0.1%).

In general it can be concluded that the quality problems of face geometry compared to finger printing and iris scan still remain when using ICAO-compatible reference data.

Recognition (matching) decisions are intrinsically inaccurate to some extent

As described above, the personal data processed should be accurate. A fundamental element of biometric systems is the recognition (matching) decision and the threshold employed (see section 3.1.2). Because of the inherent statistical nature of a biometric system, a decision of a biometric system merely gives a degree of correlation between the submitted biometric samples and the reference biometric data. Each type of biometric system has a FRR and a FAR to a higher or lower degree depending on the threshold. It is the system designer or the operator (owner) who will set the acceptance threshold and error rate, often decided and adapted to the requirements of a specific application. In a low security application, e.g., the registration of meals of pupils, one could decide to reduce the FRR, which will have as effect an increased FAR. This trade off and the fact that the match is never a complete match (but only a probability) imply that the decisions that biometric systems make about an individual and the data relating thereto are never for 100% correct or sure. One could question if this is in conformity with the requirements of the Directive that the data relating to individuals shall be accurate. Biometric matching decisions of biometric systems fail per definition to fulfil this requirement. Individuals may always be subject to false decisions which affect them. To avoid a negative impact of the failure rates of biometric systems for the data subject appropriate back-up procedures have been suggested (e.g. by Clarke[149]). Consequently

---

[146] 'Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II', German Federal Office for Information Security (BSI), Bonn 2005. http://www.bsi.de/literat/studien/biop/biop_2.htm.

[147] See http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/90754

[148] See http://www.frvt.org/FRVT2006/Results.aspx

[149] R. Clarke, 'Biometrics' Inadequacies and Threats, and the Need for Regulation', Presentation on the Computers, Freedom & Privacy 2002; see http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html

authentication using biometrics never should be solely based on biometrics using one feature only.

Right to object

If biometrics are used by a private owner for access control purposes, e.g., to a place open to the public such as a dancing club or soccer stadium, the public interest (securing (public) order) is often invoked, or the interests of the controller, outweighing the interests of the individuals.[150] The Directive 95/46/EC states that especially if the processing is based on these grounds, the data subjects should have the right to '*object at any time on compelling legitimate grounds relating to his particular situation'* to the processing, unless the national legislation states otherwise.[151] Legitimate grounds could be the contention that biometric data include sensitive data, difficulties to enrol, or also religious belief. The principle of the right of individuals to object to the processing of data shall be taken into account in the discussions about biometrics in the way that alternatives for use of a biometric system will always have to be provided. This will be especially true for the biometric Type II access models operated by a private organisation. For biometric Type II access models operated by a government, e.g., for e-government services, the use of alternatives will be even less desirable in view of a streamlined organisational model where as much as possible the biometric verification or identification functionality will be used. The use of alternative means for biometric Type I government controlled ID models, will even be much more difficult. Biometric systems will therefore probably never include all individuals to whom it might be directed (e.g., controlling access of passengers to specific zones in airports). Appropriate specifications as to when somebody is entitled to object to become enrolled in a biometric system would therefore be needed.

Unauthorised access to biometric data stored on RFID chip

Biometric data that are stored on a contactless chip need to be sufficiently secured in order to prevent unwanted disclosure of the data contained therein. This security is often lacking or insufficient. FIDIS and other authors have strongly advocated the use of appropriate security measures to avoid tracking and eavesdropping of the personal biometric data stored on media which involve new technologies such as RFID.[152] This issue has become very important, because the use of a contactless chip has been agreed for the issue of the so-called e-passports, following the ICAO specification for Machine Readable Travel Documents in May 2004, and confirmed and mandated in the 2252/2004 Regulation. The vulnerability of the biometric data stored on the RFID chip has been proven by documented attacks on the e-passport in several countries, including Germany, the Netherlands, the United Kingdom and Belgium.[153]

---

[150] See Article 7 (e) and (f) of Directive 95/46/EC.

[151] Article 14 (a) of Directive 95/46/EC.

[152] See X, *Budapest Declaration on Machine Readable Travel Documents (MRTDs)*, Future of Identity in the Information Society (FIDIS) (ed.), 2006, 6 p., available on www.fidis.net; Meints, M., "Implementierung grosser biometrischer Systeme. Kriterien und deren Anwendung am Beispiel des ePasses", *Datenschutz und Datensicherheit* 2007, vol. 31, 189-193. See also A. Juels, D. Molnar, and D. Wagner, 'Security and privacy issues in e-passports' in *Proc. 1st Intl. Conf. on Security and Privacy for Emerging Areas in Communications Networks*, Los Alamitos, CA: IEEE Computer Society, 2005, 74-85. Copy of the paper is available on http://www.eecs.berkeley.edu/Faculty/Homepages/wagner.html (last visited on 5 July 2007).

[153] For Belgium, see G. Avoine, K. Kalach & J-J. Quisquater, 'Belgian Biometric Passport does not get a pass… Your personal data are in danger', June 2007, available on http://www.dice.ucl.ac.be/crypto/passport/index.html

In addition to the privacy threats and ethical concerns described above, biometrics raise in principle concerns of link ability, disclosure of additional health information and unobserved verification or identification.

4.3.1 Direct identify ability, link ability and profiling

Biometric characteristics are tightly bound to a physical person. In most cases, an individual is even unable to influence his biometric characteristics without harming himself. It is therefore difficult to deny or to hide biometric properties. For governments and identity management system operators, biometrics offer the unique possibility to authenticate individuals that are uncooperative and even to prove to an impostor his true identity (negative authentication). Biometrics is the only authentication concept with this quality. In a world where identity theft becomes a serious threat for whole populations, biometric properties become the crucial factor for secure authentication.

On the other hand, the use of biometrics inherently holds some risks for the privacy and the social life of a user. The lifetime of a typical identity credential should be shorter or at least not exceed the lifetime of a typical identity record in an IMS of a biometric system. For biometric templates used as identity credentials, this is clearly not the case. Most biometric characteristics remain identical for a long time and some of the characteristics even remain unchanged for a full lifetime of a person. In addition, individuals have to use the same biometric characteristic as a biometric credential in many different authentication situations.

Therefore, a corrupted biometric credential can severely harm a person. There is naturally no revocation list for corrupted or out of date biometric characteristic and properties. Therefore biometric data should never run the risk of corruption or disclosure to non-authorised entities. The usual concept of a central repository for the storage of identity credentials is not adapted to this request. States and large organisations collect and store huge amounts of biometric data from their citizens or members in large databases. Nobody can guarantee that such data will not be abused for privacy violating profiling or fall in the hands of an external attacker. A further drawback of centralised databases is the limitation on scalability (see section 3.1.3). Depending on the technology, biometric template databases have collisions between individual templates already with a few hundred or thousands of Biometric Information Records (BIRs). This can lead to confusion of persons with potentially dramatic consequences for innocent people.

Especially face pictures can be used to *identify* data subjects outside the biometric system *directly* if analysed by people who know the person on the picture. This identity information then can be used to *link additional information* from publicly and not publicly available sources such as the internet or databases from the police or national security agencies. Based on these linked information items *profiling* can be done.

Civil liberty organisations warn with good arguments of such dangers and the population is still reluctant to accept biometric authentication within such boundary conditions. Neither the measurement of biometric data nor the comparison with a stored reference template should be done outside a highly protected and user-controlled infrastructure. There is no good reason to measure, store or compare biometric data in a centralised architecture. In most cases it is sufficient that the result of biometric identity verification is transmitted in a secure way to the IMS.

4.3.2 Additional and in some cases health related information in biometrics

Biometric raw data potentially in many cases contain *additional information* about the person they belong to. In many cases, this additional information is health related. In this context also the term "indirect medical implications"[154] is being used. In the context of the Data Protection Directive 95/46/EC this kind of additional information is considered highly sensitive. Many implementations of biometrics use templates as biometric reference data instead of biometric raw data. It is obvious that in these cases additional information is reduced compared to the use of raw data, but mostly no systematic research has been carried out so far with respect to remaining additional information *in templates*. In some cases it can be concluded from the method used for feature extraction that additional information might still be present in certain types of templates. The following table lists commonly used biometric methods, additional information known to be found in the raw data and additional information likely to be still included in templates.

Biometric method	Additional information in raw data	Additional information in templates
Face geometry	• Liver diseases (from colour of the skin)[155]	• Likely not included
	• Diseases of the nerve system such as stroke (asymmetry of the face)[156]	• Likely still included
	• Marfan syndrome (special symmetry parameter of the face)[157]	• Likely still included
	• Information on age, colour of the eyes and hairs, sex, and ethnic origin can be extracted from the pictures; in some cases automated methods have been developed for extraction of these information[158]	• Likely not included

[154] 'European Commission, Joint Research Centre (DG JRC), Institute for Prospective Technological Studies (IPTS)', *Biometrics at the Frontiers: Assessing the Impact on Society*, p. 18, Brussels 2005, available at http://www.biteproject.org/documents/EU_Biometrics_at_the_Frontiers.pdf

[155] See e.g. http://www.asklepios.com/globaleindikationen/GlobaleIndikationenInnereMedizin/lebererkrankungen.htm

[156] See *below*, at footnote 178.

[157] See e.g. http://www.marfan.de/marfan/diagnose.php

[158] Von Graevenitz, G., *Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren*, 98-99, LIT Verlage, Berlin 2006.

Fingerprints	• Skin condition such as eczema may cause false rejection or error to enrol[159]	
	• Certain types of fingerprints seem to be related with a likelihood of 50% with stomach problems [160]	• Seems not to be investigated yet
	• Nutrition status of the mother in the first three months of pregnancy (from macroscopic papillary structures)[161]	• Seems to be not investigated yet
	• Socio-psychological constitution (from macroscopic papillary structures)[162]	• Seems to be not investigated yet
	• Partial overview on historic research with respect to additional information in finger-prints such as likelihood to belong to a certain race or to have a certain geographic origin [163] and increased likelihoods of bearing or developing certain diseases, among them genetically caused diseases[164]	• Seems to be not investigated yet

[159] See *above* at footnote 154, 53.

[160] *Ibid.*, 52.

[161] Von Hardenberg, I., 'Warum Neugeborene mehr wissen, als Große manchmal ahnen', *GEO (7)*, 27-42, Hamburg, July 2001.

[162] See http://www.edcampbell.com/PalmD-History.htm. Large parts of the literature cited there has not a scientific background.

[163] Cole, S. A., *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*, University of California, Irvine. Download via http://www.ksg.harvard.edu/dnabook/

[164] See *above* at footnote 158, 84-86.

Iris scan[165]	• Iritis[166] and other infectious diseases of the eye • Iridology suggests that a lot of other diseases such as glaucoma can be diagnosed from the iris.[167] As scientific evidence is weak or missing, this is highly disputable.[168] • Missing eyes, aniritis and pronounced nystigmus leads to errors to enroll[169]	• Seems to be not investigated yet
Hand geometry	• Arthritis[170] • Gout[171] • Marfan syndrome[172]	• It can be expected that geometry-related information still is included in the template. • Reverse calculation from the reference value to the hand geometry seems to be impossible in some investigated cases[173].
DNA analysis	• Complete genetic information encoded	• In some cases the ethnicity of the person behind the genetic fingerprint can be determined with some likelihood; this possibility was used to analyse the remains of multiple victims[174]. • Due to the neighbourhood of analysed STR to coded parts of the DNA there could be a relation

[165] Some iris scan systems perform liveness detection by checking the reaction of the pupil when exposed to light. A weak or missing reaction to light can also disclose health related information as it can be caused by the use of illegal drugs or drugs used legally in the context of a medical examination or treatment (e.g. for iritis).
[166] See e.g. http://www.augenarzt-lahr.de/iritis.html. This information refers to diagnosis of diseases in visible light. It is very likely, that bacterial coverings and blood also can be seen in near infrared light used for the iris scan.
[167] See e.g. http://www.meine-gesundheit.de/225.0.html
[168] See http://www.augentagesklinik.com/de/informationen/patienten/irisdiagnostik.php
[169] See http://www.icdri.org/biometrics/iris_biometrics.htm
[170] See e.g. http://www.cse.msu.edu/~cse891/Sect601/HandGeometry.pdf and http://bioenabletech.com/biometrics/handgeometry.htm
[171] See *above* at footnote 170.
[172] See *above* at footnote 157.
[173] See http://www.cse.msu.edu/~cse891/Sect601/HandGeometry.pdf
[174] See: http://www.benecke.com/popscidna.html
[175] Benecke, M., 'Coding or non-coding, that is the question', *EMBO reports* vol. 3 no. 6, June 2002. See http://www.benecke.com/coding.pdf

		between them and the analysed loci. This was discussed with the locus THO1 and the diabetes type 1 gene where the risk determined by analysis of a certain allele today is 0.12 % higher than the statistically average (0.4%).[175] • Recently strong evidence was discovered that coded and non-coded parts of DNA may be linked very closely.[176]
Voice recognition	• Diseases of the nervous system such as Parkinson's disease[177] and stroke[178]	• Not investigated yet
Key stroke dynamics	• Diseases of the nervous system such as Parkinson's disease and stroke[179]	• Not investigated yet
Signature recognition	• Diseases of the nervous system such as Parkinson's disease and stroke[180]	• Not investigated yet
Vein analysis	• Varices[181]	• Not investigated yet

Table 8: Additional information in biometric raw data and templates

For many biometrics it is currently not clear whether biometric templates include additional information or not. Based on the used method in some cases, it is very likely that health related additional information potentially might still be in the template. Examples for this are face geometry (face asymmetry potentially indicates certain diseases of the nervous system) and hand geometry measurement (certain geometry pattern indicate Marfan syndrome, gout or arthritis).

In this context future research is necessary. In cases where no additional information is contained in templates, the use of templates could have – together with an appropriate system

[176] Rigoutsos' I., Huynh, T., Miranda, K., Tsirigos, A., McHardy, A. andPlatt, D., 'Short blocks from the noncoding parts of the human genome have instances within nearly all known genes and relate to biological processes', *Proceedings of the National Academy of Science of the United States* vol. 103 no. 17, pp. 6605-6610, Washington D. C., April 2006.

[177] See e.g. http://www.parkinsons.org.uk/Templates/Internal.asp?NodeID=100640

[178] See e.g. http://www.vitanet.de/herz-kreislauf/schlaganfall/symptome/

[179] *Ibid.*

[180] *Ibid.*

[181] See e.g. http://www.venenmittel.info/inh/krampfadern.html

design – a positive influence on the proportionality for the use of this biometrics for certain areas of applications.

4.3.3 Unobserved and non interactive authentication

Certain biometrics, such as behavioural biometrics and face geometry, allow for the collection and processing of biometric raw data without active participation of the user. In most cases, it is possible to use hidden sensors that cannot easily be observed by the persons that are going to be authenticated using the biometric system. The described types of biometrics thus support *unobserved and non-interactive authentication* (by identification or verification using biometrics). Depending on the area of use, this type of authentication can have especially negative consequences for the data subject in cases where the authentication fails due to technical reasons (e.g. False Rejection Rate (FRR)). In many cases, failure rates of biometric systems can be expected to increase in cases where the data subject is unaware of the authentication procedure and therefore does not co-operate. As testing of biometric systems supporting non-interactive authentication typically is done with volunteers supporting the testing, no research data seems to be available with respect to the impact of lack of co-operation on failure rates. This type of use of biometrics may be in a biometric Type III mixed model and Type V tracking model. As no informed consent by the data subject is possible in this case, this type of authentication should be limited to areas of application which are strictly regulated by law.

4.4 Threats to a biometric system from impostors

Following up on the work done in FIDIS Deliverable 6.1[182], and the previous identification of fault sensitive points in a biometric system (see *above* section 4.1), this section discusses a number of tests regarding security vulnerabilities of biometric devices. As discussed in the Common Criteria (CC)[183] document, a biometric system in general has a variety of locations that are potentially vulnerable to attacks of impostors (see table 9 *below*). For example, a device could be misled with artificial biometric samples, data transmissions between different biometric system components could be intercepted or modified, and hardware components could be tampered with. Direct effects of such attacks include unauthorised system access, denial of service and unauthorised extraction of biometric data of system users. The main focus of this section is on impostor attacks. The CC model gives a detailed overview of weaknesses and opportunities for an impostor attack in a biometric system.

The CC model structures the attacks into the categories summarised below:

[182] 'FIDIS Deliverable 6.1: Forensic Implications of Identity Management Systems', January 2006, available at http://www.fidis.net

[183] Common Criteria Biometric Evaluation Methodology Working Group, 'Common Criteria – Common Methodology for Information Technology Security Evaluation – Biometric Evaluation Methodology Supplement', Version 1.0, August 2002.

Impostor collusion, social engineering, template replacing, template stealing: User Threats. Authorised user provides own biometric sample, unknowingly, unwillingly (coercion), or willingly (collusion), to impostor	
	Impostor covertly captures a biometric sample from authorised user, e.g. record voice, photograph face.
	Impostor steals a biometric sample from an authorised user e.g. gets fingerprint from a object that the user had in hand, or install fake biometric readers to capture biometric sample.
	Authorised user knowingly provides own biometric sample to impostor (collusion)
	Authorised user modifies own biometric sample to facilitate an impostor attack (collusion)
	Impostor steals or inserts a reference template
Fake biometrics: User/ Capture Threats	
	Impostor presents own biometric sample in a zero-effort attempt to impersonate (a) a randomly selected authorised user (for verification), (b) any authorised user (for identification), (c) a selected weak biometric template, or (d) an authorised user with a biometric sample similar to that of the impostor (e.g., a twin).
	Impostor modifies own behaviour (e.g. voice, signature) or physiology (e.g. face, hand) in an attempt to impersonate (a) a selected authorised user, or (b) a selected weak biometric template.
Data insertion, replay, change of decision policy by impostor	
	Non-hostile administrator (unintentionally or under coercion) or hostile authorised user or impostor who has acquired administrator privileges: (a) incorrectly modifies matching threshold (b) incorrectly modifies user privileges (c) allows unauthorised access to template storage (d) allows unauthorised modification of audit trail (e) enrols an unauthorised user
	Administrator fails to properly review and respond to audit trail anomalies. attacker modifies matching threshold
User/ Policy Management Threats / Threats to Portal	
	Impostor authenticates as authorised user through non-biometric means, e.g. collusion, coercion, password, backup system, alternative authentication method, or exception handling procedure.
	Audit data collection inadequate to detect attacks (e.g., hill-climbing or other repeated-attempt attacks).
	Attacker modifies user identifier
	Attacker inserts appropriate "grant privileges" signal directly into portal, thus bypassing the entire biometric system.
	Attacker cuts power to system. Either (a) system fails in "open" or "insecure" mode allowing unauthorised access; or (b) system fails in "closed" or "secure" mode disallowing authorised access
	Attacker defeats backup system, alternative authentication method, or exception handling process: (a) during normal operation, or (b) after a "secure" system failure
	Attacker defeats backup system, alternative authentication method, or exception handling process: (a) during normal operation, or (b) after a "secure" system failure
	User gains access to unauthorised privileges after privileges have been improperly modified.
	Attacker tampers, modifies, bypasses, or deactivates one or more hardware components.
	Attacker exploits hardware "back-door," design flaw, environmental conditions, or failure mode
	Attacker floods one or more hardware components with noise, e.g. electromagnetic or acoustic energy)
	Impostor intercepts/ inserts authorised biometric template from/to one or more hardware components.
	Impostor takes session over
	Attacker tampers, modifies, bypasses, or deactivates one or more software or firmware executables

	Attacker exploits software or firmware "back-door," algorithm quirk, design flaw, or failure mode.
	A virus (or other malicious software) is introduced into the system.
	Impostor intercepts/ inserts authorised biometric template from/ to one or more software or firmware components.
	Attacker tampers, modifies, bypasses, or deactivates one or more connections between components.
	Impostor intercepts or inserts authorised biometric sample or template as it is being transmitted between subsystems or components.

Table 9: Impostor threats to a biometric system according the CC Biometric Evaluation Methodology study (BEM)

4.4.1 Impostor threats in practice

Ideally, all threat locations should be analysed. However, the scope of the investigation in this section is limited to testing of artificial fingerprints (*User / Capture* threats[184]) and USB port data interception (*Capture / Extraction* threats[185]). Note that the biometric system Type I government controlled ID model and Type III mixed model tend to have more strictly controlled enrolment and use environments than Type II access control and Type IV convenience models. As User / Capture and Capture / Extraction threats often require some kind of undetected physical or logical access to the biometric system, these threats are relatively more relevant for Type I and III models than for Type II and IV.

User/Capture threat analysis

For an explanation of most fingerprint scanner technologies, the reader is referred to FIDIS Deliverable 6.1 (although Lumidigm's multispectral imaging technology is not explained in that deliverable). Figure 13 shows two fingerprint scanners that were tested by the Netherlands Forensic Institute for this deliverable. It entails the capture of nine different fingerprint images in a fraction of a second. For each image, a unique illumination and polarisation combination is used. It is claimed to allow the capture of data from both the surface and beneath the surface of the skin. The Lumidigm scanner is also claimed to be able to detect spoofs by comparing spectral characteristics against those of a wide range of known spoofs. In case of future spoofs, the developers can update the software to include characteristics of those as well. The scanner is much more expensive than most other fingerprint scanners.

[184] *Ibid.*

[185] *Ibid.*

Figure 13: Left side: Lumidigm J110-E1 fingerprint scanner using multispectral imaging technology ; Right side: RiTech BioSlimDisk USB memory stick protected with capacitive fingerprint scanner

The Lumidigm fingerprint scanner J110-E1 has undergone the same testing as the fingerprint scanners in Deliverable 6.1[186]. All spoofs were recognised as such, except, in a limited number of cases, the Super Soft Plastic[187] spoof. The success rate of that spoof was very sensitive to positioning, which diminished the repeatability of the test.

The RiTech 128 MB BioSlimDisk proved to be easier to spoof - using a gelatin[188] spoof worked nearly all the time. Another spoofing method for this device uses the latent fingerprint of the previous user. If such a fingerprint is present and of sufficient quality, the device can easily be spoofed by breathing on the sensor, thereby activating the latent fingerprint. The device does get warm after a short period of use, after which the breathing technique does not work as well anymore. In such a case a can of Airduster (e.g. from Electrolube) held upside down can be used to spray compressed gas on the sensor, which rapidly cools the sensor and activates the latent fingerprint as well (see Figure 14).

[186] See *above* at footnote 182.

[187] *Ibid.*

[188] *Ibid.*

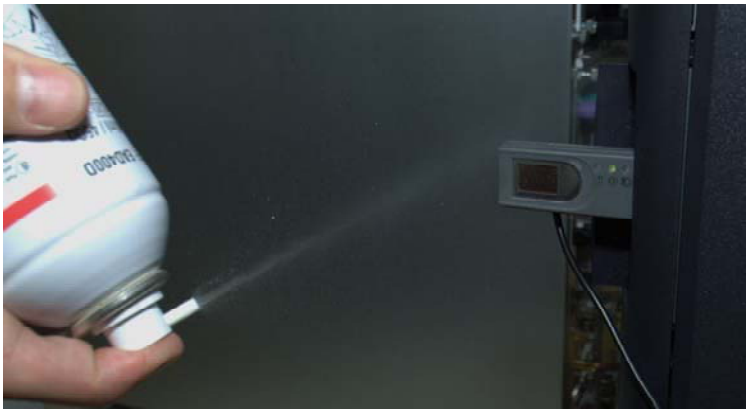

Figure 14: Activating a latent fingerprint on the BioSlimDisk with a can of airduster

Table 10 shows a summary of the spoofing test results. Success rates are categorised as None (meaning it did not work at all), Low (meaning it only worked occasionally, and with difficulty), Medium (meaning it works quite often) or High (meaning it nearly always works).

	Spoof material / method	Gelatin	Super Soft Plastic	Wood glue	Grey rubber stamp	Breath blow / Airduster
Spoof	Mould material / source	Silicone from live finger	Silicone from live finger	Laser print on sheet	Digital image of slapped fingerprint	Good quality residual fingerprint
Biometric Device	J110-E1	None	Low	None	None	None
	BioSlimDisk	High	None	None	None	Medium

Table 10: Success rates of fingerprint spoofs with two biometric devices

Capture/Extraction threat analysis

Another potential threat to the security of biometric systems is that data traffic between the biometric device and a connected PC is intercepted. Such data could be analysed for the presence of user data, from which personal biometric samples may be reconstructed. A step further would be to relay[189] the data through a customised software driver that modifies the data. Thus, previously recorded authorised biometric sample data could be inserted[190] (a so-called 'replay attack') to allow access to the system. The success of such attacks depends not only on the programming of the driver and the analysis of the intercepted data, but also on the security of the biometric system infrastructure. The driver should be installed on the system,

[189] Hoglund, G. and Butler, J., 'Rootkits: Subverting the Windows Kernel', July 2005

[190] Kiviharju, M., 'Hacking fingerprint scanners', January 2006, available at http://www.blackhat.com/html/bh-media-archives/bh-archives-2006.html#eu-06

for instance through a virus or physical or logical access to the system, and it should be hard to detect when active.

The scope of the current research is limited to the analysis of intercepted data. A number of tests[191] have been performed at the Netherlands Forensic Institute, in which data traffic between USB-connected biometric devices and a PC was intercepted, using USB-sniffing software called 'USB Monitor[192]'. USB-sniffing software essentially displays all data packets in USB data traffic. Table 11 shows the fingerprint scanners that are analysed. The sensor technologies mentioned therein are explained in FIDIS Deliverable 6.1.

Sensor technology used	Company	Device model
Frustrated Total Internal Reflection (FTIR)	Digital Persona	UareU4000
Surface Enhanced Irregular Reflection (SEIR)	BioCert	Hamster III (SecuGen FDU02 sensor)
Electro-optical	Security First Corp	Ethenticator 2500 USB
Electric field	Targus	DEFCON Authenticator PA460U (Authentec Entrépad AES 4000 sensor)
Piezoelectric	IdentAlink	UFIS210 (BMF BLP-100 sensor)
Thermal (sweep sensor)	IdentAlink	UFIS110 (Atmel FingerChip FCD4B14CC thermal sensor)
Ultrasonic	Ultra-Scan	Ultra-Touch 203

Table 11: Tested biometric devices

The general approach taken is to filter out communication protocol data and other overhead data, and analyse the remaining packet payload data. Basically, software was written to display byte values of data packages as pixels in an image, with the value determining the colour of the pixel (see Figure 15a). By varying the image width and experimenting with byte formatting, images may be extracted from the data (see Figure 15b and Figure 15c).

[191] Lenting, N. and Schutte, J., for the Netherlands Forensic Institute, 2006

[192] http://www.hhdsoftware.com/Products/home/usb-monitor.html

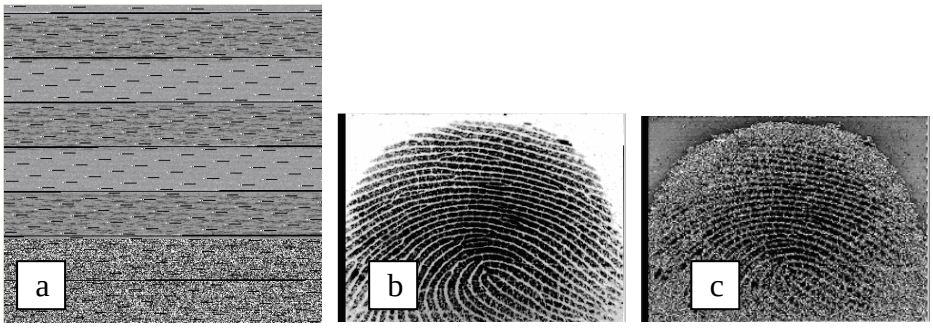

Figure 15: Intercepted data from the Secugen scanner, visualised using image pixels. a) A pattern is clearly visible. b) The even bytes, with proper image width. c) The odd bytes, with proper image width.

Some of the devices claim to make use of data encryption. For those devices, encryption was confirmed and indeed no intelligible biometric sample data could be found. As breaking the encryption is beyond the scope of the test, further analysis of the devices in questions was abandoned. From all of the devices that have no encryption, fingerprint images could be reconstructed from the data packages with the previously mentioned approach. The test results are summarised in table 12.

Threat analysis conclusions

Combining conclusions from Deliverable 6.1 with the results in this section, it is clear that many biometrics devices are still not adequately protected from spoof attacks and data interception attacks. Of the currently tested fingerprint scanners only the Lumidigm device seems to have effective spoof protection, which the manufacturer can upgrade to include future spoofs. The offered protection is however reflected in the device price. The data interception threats to the fingerprint scanners can easily be reduced by implementing some form of data encryption.

Fingerprint scanner model	**Data encryption?**	**Extraction example**
UareU4000	Yes (128 bit)	not successful
Hamster III	No	
Ethenticator 2500 USB	No	
DEFCON Authenticator	Yes	not successful

PA460U	(256 bit AES)	
UFIS110	No	
UFIS210	No	
Ultra-Touch 203	Yes (Unknown)	not successful

Table 12: Results of USB sniffing attempts

4.4.2 Combined technologies

Biometrics are often combined with other technologies, such as RFID technology, chip cards and other storage devices or databases.

The RFID chip card is commonly used in access control to buildings and public transportation. Often implementations only require the card. If the card gets stolen, someone else can enter the building or the public transportation with the card. To limit unauthorised access, pin codes and biometric features such as fingerprints are used.

The biometrics can be stored either in a database or on the card. It is important in the implementation to do this in a secure way. An example of biometrics that is stored on a RFID chip is a biometric passport. A different example is an iris scan in the Privium[193] project for entering the border in Schiphol Airport, where a template of the iris is stored on a smart card. If the current security schemes are implemented properly, it becomes nearly impossible to extract the biometric data without having access to the secret keys.

In low cost solutions, it is possible that the encryption is not properly implemented, and that it becomes easy to capture the biometrics, from example from the USB cable. This was demonstrated during the Blackhat conference in 2006 with a consumer fingerprint device.[194]

It is expected that these vulnerabilities will be reduced. The problem was that the time to develop these devices was fast, and so less secure solutions were developed. A known example is the USB stick with fingerprint reader. There are fingerprint USB sticks on the market, where the data is not encrypted on the storage device. This means that someone can circumvent the encryption by going into the hardware of the stick itself, and after the circuit for the biometric comparison, as a result it becomes possible to circumvent this by sending out the right signal. Another possibility is just to ask several persons to try to access the key.

[193] http://www.airport-technology.com/projects/schiphol/

[194] http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Kiviharju/bh-eu-06-kiviarju.pdf

In theory, if the Equal Error Rate is 1 percent, which is in some practical devices the case[195], this means that with 100 different fingerprints, one will gain access to the USB key and with 100 correct fingerprints one person will not get access. In this case, it is trial and error with different people.

For evaluation of the security of these systems, one should look at the separate parts and the whole system before drawing conclusions. It is also necessary to check the claims of the manufacturer by using your own test set to evaluate if the settings are the same as the manufacturer has specified.

For access to mobile phones, biometric features such as fingerprint and face recognition are implemented in products (such as OKAO Vision Face Recognition Sensor which is software that can be used in mobile phones for face recognition and the Pantech GI100 phone). Although commercial implementations have been available on the market since 2005, the mainstream mobile phone brands have not implemented this widely yet

When combining biometrics with other technologies, additional threats need to be analysed and countered by appropriate security measures. One example for this which has been discussed above is storage of biometric reference data on RFID chips. The confidentiality of these biometric reference data among others strongly depends on control over the biometric system (or system) and effectiveness of access control mechanisms for the biometric data stored on the RFID chip. Development of additional technical security solutions is required before these technologies can be used securely in combination. This applies to all Types as discussed *above*. Obviously this was not done sufficiently for MRTDs such as the ePassport (Type I c government controlled ID model). As a consequence, Basic Access Control (BAC) as the access control mechanisms applied for today's MRTDs shows a number of severe weaknesses.[196] The weak part of encryption can be that the secret key has to be shared with widespread use. There are methods available to store a digital feature available which can not easily be computed back to the real biometric feature.[197]

As RFID is developed for wireless and remote readability, tracking of passport holders is a potential additional threat compared to purely paper based passports. To prevent tracking several measures such as Faraday cages, randomly chosen identifiers for the RFID chip and cryptographic access control mechanisms can be used. Unfortunately, the implementation of these measures is insufficient or missing, so that under certain circumstances tracking of passport holders seems to be well possible. An additional threat is tracking using biometric raw data (especially the digital photos) stored on the RFID chip. As the range of readers can be extended up to 50 cm, unrecognised readout of the raw data and abuse for tracking purposes using hidden cameras and biometric matching systems is a possible scenario.

A possible solution to prevent unauthorised readout of RFID chips is to use them only in an active mode (dual port chips). In this case the data subject has to power up the RFID holding

---

[195] http://www.springerlink.com/index/HXGUUQNQE84HKD79.pdf

[196] See e.g. M. Meints and M. Hansen (eds.), *o.c.* at footnote 26.

[197] http://doi.ieeecomputersociety.org/10.1109/TC.2006.138

device by a wilful act before the chip can be read by an external device. Such a scheme greatly reduces the possible physical points of attack.

Concluding remarks on security and privacy aspects of biometrics

Biometric systems contain numerous sensitive points which may be attacked by impostors or attackers that intend to make the biometric system inoperative. The aim of an attacker is to manipulate the system in a way that it produces untrustworthy or wrong results. For the points of attack which have been identified, appropriate countermeasures shall be taken both on a conceptual as on an organisational level before a biometric system is put into use. Direct attacks on the physical biometric characteristic of a subject are conceptually not avoidable and the risk that such an attack succeeds is difficult to estimate. In addition to the security threats biometric systems pose also several and significant privacy risks which have been summed up above. These security and privacy threats are elements which need to be taken into account when evaluating the proportionality and the efficiency of the use of a biometric system for a specific purpose and in the context of a specific type of application (see *above*, section 3.3.3). Biometric applications should not be introduced if the privacy and security threats for individuals are disproportionate in comparison with to the benefits of the system.

5 Advantages and needs for biometrics

Traditionally biometrics are understood as a third factor for authentication in addition to possession (token, such as a chip card or key) and knowledge (such as a PIN or password) (see *above* section 2.3). Obviously, biometric characteristics are valuable in cases where the two traditional factors of authentication are not sufficient for security reasons.

In a world where identity theft becomes a serious threat for whole populations, biometric features become the crucial factor for some authentication applications with enhanced security requests. In addition, biometrics show a number of additional advantages and correspondingly areas of use that will be introduced in the following.

5.1 Binding between physical and digital world

A token (possession) or a secret (knowledge) as traditional factors for authentication have a common problem: is its user the legitimate user or has the token be stolen and is being used by an unauthorised person? To secure the binding between a token and an authorised user, knowledge as an additional factor of authentication (e.g. in the SecureID systems by RSA Inc.) or a facial image (photo, e.g. in paper based travel documents) can be added.

In this context biometrics can be used instead or in addition to knowledge or printed photos on ID documents to secure the binding between a physical person and a token. This could be applied not only to Type I government controlled ID models, but also to the Type II access model, the Type III mixed model and the Type IV b convenience model.

At that point, however, one should question which functionality of biometrics shall be deployed in order to meet the proportionality criterion. To improve the security by deployment of biometrics, the security can in most cases already be improved considerably by applying the verification mode of biometrics in combination with a token. Biometrics will than be used for verification purposes. This is especially valid for the biometric Type II access model for securing access to online systems (see above, section 3.3), even if the biometrics in that model are used in an environment where there is no supervision (e.g., web access at home for financial services). The use of biometrics for identification purposes through deployment of that biometric in combination with a token for a 1:N comparison locally[198] in a Type II model does not add much to the security for that application, while the central storage of the biometric which is needed for the 1:N check contains considerable risks for the person involved (such as the loss of control over the use of the biometrics - see also *above*). The use of biometrics in combination with a token for identification could for that reason be considered disproportionate.[199] This problem becomes void if one assumes that the biometric is stored in a secured token, which cannot be easily counterfeited or hacked.

Decisions of DPAs in some countries seem to follow that approach. The DPA in France has issued on 27th April 2006 a 'single authorisation' decision in which it allows the use of

[198] A local storage of a biometric reference database today is a theoretical model only, as updating the database on all tokens at any time is a real maintenance problem, not solved so far. As a result practically 1:N matching needs a centralised reference database.

[199] See also *above*, section 4.2, and in particular the statement of the Council of Europe (see also footnote 137).

fingerprints to the extent the fingerprint of employees is verified with the template stored on the card for access control, without central storage.[200]

5.2 Negative identity verification

The biometric factor has special qualities for the authentication process. Unlike a secret or a token, biometric characteristics are tightly bound to a physical person. A person cannot deny that he or she carries a certain biometric. This opens the unique possibility to authenticate an uncooperative person or even to prove to an impostor his true identity (negative identification) if the person can be urged to deliver a biometric sample.

Thus biometric identification has the unique potential to prove that a person that claims to have a certain identity is an impostor or that he or she has already enrolled under another identity, for example, in a biometric Type I government controlled ID model. This can be used, for example, for preventing terrorists from boarding airplanes. As opposed to other identification or verification systems, e.g. username password systems or the possession of a physical token, only biometrics offer this mode of operation. It is inherent to the identification mode that a large number of false matches will be triggered. This problem is adequately described by Prabhakar *et al*.[201]

Thus biometrics may become a useful method to deploy a reliable identity verification system in a hostile or non cooperative community. This quality of biometrics is also useful in forensics to discharge innocent persons.

5.3 Biometrics as a privacy guard

Existing security vulnerabilities of biometric systems and potential misuse of biometric data combined with an intensified commercial and governmental interest in biometrics stemming from their inherent identification capabilities which promise to overcome the limitations of current identification and authorisation systems have resulted in an increased concern over the way they can affect the persons' privacy. However, the security enhancement of existing systems in a large set of applications comprises one of the main promises of biometric technology. In fact, biometrics seem to be not only a threat but also an opportunity to privacy.

The accurate and thus reliable identification and verification of individuals comprise a major goal for both governments and private organisations. Identification or authentication processes are included in various applications in many fields from entertainment and education to law enforcement and access control. High false rejection and false acceptance rates in existing identification and verification systems result in unnecessary duplication, regular cases of identity fraud and resulting customer disruption and thus comprise a heavy cost for organisations. Biometric technology offers the potential of overcoming the security vulnerabilities and the performance limitations of conventional identification and authentication systems which mainly rely on the use of unique identifiers such as PINs, passwords and smart cards which can be fraudulently stolen or guessed. The personal data of the individuals as well as these resulting from the individual's interaction with the system data are thus less vulnerable to attacks.

---

[200] See Section 3.2.2 and footnote 50.

[201] Prabhakar, S., Pankanti, S., Jain, A.K., "Biometric recognition: security and privacy concerns," *Security & Privacy Magazine*, IEEE , vol.1, no.2 pp. 33- 42, Mar-Apr 2003.

A technology can be characterised as privacy-enhancing when it protects informational privacy by preventing unnecessary or unauthorised personal data disclosure and processing but still maintaining the functionality of the system.[202] A biometric (sub-)system built with a privacy enhancement orientation and offering the promised increased security levels can in fact serve as a privacy guard. The most profound use of biometrics as a privacy protecting technology is as a means of controlling access to the individual's personal data through a strict authentication system. The very nature of biometric authentication systems is using "what you are" information for access purposes in contrast to conventional authentication / authorisation systems which are based on "what you have" (e.g., smart card) and "what you know" (e.g., passwords) with the benefit of being a set of features tightly linked to a person's identity that cannot be shared or easily duplicated. Thus, privacy issues are reduced due to the decrease in the ability to duplicate an individual's identity as well as in the need to maintain multiple forms of identification means (e.g., credit cards, passwords, etc).[203] The notion of protecting privacy includes providing the ability to correct an error or to prevent fraud that is related to a suspected misuse or abuse of personal information by the authorities. According to Neuman "*a biometric can enhance privacy, such as when an authority looks something up in a system, and their authority to do so is also verified through the use of their own biometric identifier*".[204] But in general, access to databases and other types of data storage containing sensitive personal information including religious, financial data, medical records, criminal records and others, can be monitored and recorded through the use of biometric authentication of the one accessing the data. Examples of such applications include:

- access to personal - including medical - information which can be restricted to healthcare workers granted with authorisation rights through the use of biometrically protected smart cards and an underlying authorisation structure
- access to emergency contact information and special medical information of students which requires the presence of the student
- access to specific facilities of a laboratory being possible only to the permanent staff of the lab (e.g., printers, oscilloscopes, etc).

Moreover, biometrics serving as a profiling technique[205] or as a link between personal data[206] can comprise a big asset – provided that they are being developed and implemented in the context of the appropriate legal framework - when conducting background investigations to

---

[202] Van Blarkom, G.W., Borking, J.J., Olk, J.G.E., *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*, College bescherming persoonsgegevens, 2003, 33 p.

[203] Oliver, G. M., *A study of the use of biometrics as it relates to personal privacy concerns*, July 31, 1999, available at http://faculty.ed.umuc.edu/~meinkej/inss690/oliver/Oliver-690.htm

[204] Brown, D., Brook, D., 'Biometrics: Implications and Applications for Citizenship and Immigration - Report on a Forum hosted by Citizenship and Immigration Canada', October 7 & 8, 2003 – Ottawa, Ontario.

[205] Hildebrandt, M., Backhouse, J., *Descriptive analysis and inventory of profiling practices*, FIDIS *Deliverable 7.2*, European Union IST FIDIS Project, 2005, available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp7-del7.2.profiling_practices.pdf

[206] Andronikou, V., Demetis, D., Varvarigou, Th., 'Biometric Implementations and the Implications for Security and Privacy', 1st in-house FIDIS journal issue, 1-2007, available at http://journal.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf

ensure the individual does not have a negative history, particularly in the areas of child abuse and sex offenders.[207]

For this reason, apart from the formation of the suitable legal framework, many technological efforts have been made in order to eliminate the biometric system vulnerabilities that threaten the user's privacy which put into their shade the privacy-enhancing capabilities of biometrics. It should be noted that these efforts aim at offering a beneficial additional layer in the privacy aspect of the biometric systems and not providing a complete solution. The centralised storage of the collected biometric data is strongly discouraged, whereas concepts such as cancellable or revocable biometrics – biometrics distorted in a non-invertible manner both during enrolment and verification – have been introduced in order to deal with the protection of the biometric data.[208] More specifically, instead of storing a digital representation of the specific biological feature, a distorted image of that feature is stored during enrolment. Every time the same individual tries to access the system, the machine scanner distorts the image during scanning, and the matching process involves the comparison of the two distorted images. The non-invertible transformation of the biometric data ensures that even if the transform function and the produced biometric data are known, the original biometric data cannot be extracted. Used this way, biometrics can comprise a mechanism to verify an individual's identity without linking it to their private data by supporting the unlinkability aspect of privacy. However, provided that serious restrictions are posed by the special requirement for cancellable biometrics that the transformed version of the biometrics should not only *not* match the original biometrics of the individual but they should also not match the biometrics of any other individual as well as that current techniques suffer from lack of high levels of accuracy[209], cancellable biometrics cannot yet guarantee high levels of unlinkability.

The combination of multiple biometrics (also called multimodal biometrics) has also been regarded as a technique that can enhance the privacy aspects of biometrics. In this case, more than one separate biometric feature are combined to obtain a non-unique identifier of the individual. Example of multiple biometrics include use of imprints of more than one fingers or iris scans of both eyes, or combination of totally different biometric data, such as a facial image combined with an iris scan. Although the key comparative advantage of multiple biometrics against single biometrics lies in the information richness, it is not limited to it. In fact, not only are there expectations for performance enhancement but also the risk of misuse and privacy invasion is reduced, as a potential attempt for intentional false positive requires

---

[207] Oliver, G. M., cited *above* at footnote 203, available at http://faculty.ed.umuc.edu/~meinkej/inss690/oliver/Oliver-690.htm

[208] Ratha N. K., J. H. Connell, and R. M. Bolle, 'Enhancing security and privacy in biometrics-based authentication systems', *IBM Systems Journal*, 40(3), pp. 614–634, 2001; Ang R., R. Safavi-Naini, L. McAven, 'Cancelable Key-Based Fingerprint Templates', ACISP 2005, pp. 242-252, 2005; Cheung K. H., Ad. Wai-Kin Kong, D. Zhang, M. Kamel, Jane You, Ho-Wang Lam, 'An Analysis on Accuracy of Cancellable Biometrics Based on BioHashing', Lecture Notes in Computer Science, Springer, 2005, 1168-1172.

[209] Toh, K.-A., Lee, Ch., Choi J.-Y., and Kim J., *Performance based revocable biometrics*, Industrial Electronics and Applications, 2007. ICIEA 2007, 2nd IEEE Conference on 23-25 May 2007, 647 – 652; Boult, T. E., Scheirer, W. J., Woodworth, R., 'Revocable Fingerprint Biotokens: Accuracy and Security Analysis', Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on 17-22 June 2007, 1 – 8.

the provision of more than one biometric to the system.[210] Currently the main deterring factor for the implementation and utilisation of systems integrating multiple biometrics is the cost involved, since they involve the need for the combination of expensive equipment (iris patterns and fingerprint scanner and processing system). However, cases of multiple biometrics being extracted by the same body part (e.g. fingers) could be the first step in that direction.

Biometric encryption[211] is another possible improvement of biometrics. Encryption is the process through which the information which is transmitted or stored in a database is disguised. The basic idea behind key-based cryptography is that the data is scrambled up so that only the sender and the recipient of the data can actually read it. More specifically, in public-key cryptography the user has a pair of keys: a private and a public key. The sender uses the public key as the basis for the encryption of the data, whereas only the owner of the private key can decrypt the encrypted data.

Biometric encryption is a process which results from the merging of biometrics with cryptography. In an effort to take advantage of the main features of biometrics including uniqueness and variability, it uses one or more biometric feature as a method for *secure key management*, rather than data encryption / decryption with the main reason for the latter being the great variability of biometrics. In other words, biometric encryption aims at enhancing the crypto system so that the keys are less vulnerable to attack through the secure binding of the key with the biometric so that neither the biometric nor the key could be retrieved from the stored template. The rapidly increasing information exchange via the Internet has led to an intensified need for protection of sensitive data connected to open networks which are either transmitted or stored in databases. Moreover, biometric encryption goes a step beyond the traditional biometric systems and allows individuals to use a single biometric for multiple accounts and purposes with no fear that these separate identifiers or uses will be linked together by a single biometric image or template.[212] According to Cavoukian, another application of biometric encryption could be a privacy-protected *one-to-many* database for "double dipping" prevention. More specifically, this database is multimodal containing both conventional (but anonymous) templates and private templates that control a link with the user's encrypted records. Thus, the decryption of the user's records is possible provided that a positive match is achieved on both types of templates. Biometric encryption aims at protecting this information and hence can act as a supporting technology for a privacy enhancing system.

---

[210] Yanikoglu B. and Al. Kholmatov, *Combining Multiple Biometrics to Protect Privacy*, Proceedings of ICPR-BCTP Workshop, Cambridge, England, Aug. 2004.

[211] Soutar, C., Roberge, D., Stoianov, Al., Gilroy, R., Kumar, B.V.K. V., 'Biometric Encryption', chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill, 1999.

[212] A. Cavoukian and A. Stoianov, *o.c. above* at footnote 121.

5.4 Forensics with biometric methods

In forensic science, biometrics has been used for a long time.[213] The first textbook on the subject was authored by Sir Francis Galton in 1892. The French policeman Bertillon[214] had developed a system of personal identification by bodily measurements. It became known as the Bertillon system. From about 1910, the fingerprint became more widely used, since it was easy to compare and store in comparison to the Bertillon system where many measurements had to be taken from each body part, with many errors possible.

Nowadays there exist large Automated Fingerprint Identification Systems (AFIS).[215] The first automated systems where available in 1950 with punch cards which were mechanically searched. In the early 1970s, computer based systems were feasible for fingerprints. Nowadays the largest network of AFIS has over 25 million subjects[216] in the database. Also palm prints are entered in a database. Barefoot soles, lip prints, ear prints are also examples of prints, but are not stored in such a centralised database.

Face comparison is also commonly done at police stations. The scientific background of face comparisons still should be validated.[217] In forensic science, there are several efforts for making a face comparison more objective. Despite the face databases that are available, automated searching in these databases is not feasible without going through many false hits (the equal error rate is high, and with aging of a person this can be as high as 0.4-0.5, which means that one has to search through half of the database before finding the right person).[218]

Iris systems and databases are described to be very effective.[219] However, in forensic science, we do not often get cases with iris-comparisons. In National Geographic[220], one case is shown where a comparison of a photograph of an Afghan girl with the photograph of a woman gives evidence that they are the same person. The resolution of commonly made digital photographs is not enough to compare the irises. Commercial systems for iris comparison for access control are implemented in airports. The largest database of irises is reported to be in United Arab Emirates[221], where over half a million irises were in the database in 2005.

---

[213] Moenssens, Fingerprint Techniques, 1971, 1-26.

[214] http://en.wikipedia.org/wiki/Alphonse_Bertillon.

[215] Moore, "Automatic Fingerprint Identification Systems", Advances in Fingerprint Technology, Lee and Gaensslen (eds), 1991, 173.

[216] http://www.necam.com/IDS/AFIS/IntegratedNetworks.cfm

[217] http://www.ies.krakow.pl/fitwg/abstracts_FIDIS/Ruifrok_FIDIS_abstract.pdf

[218] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, 2003. Face recognition: A literature survey. *ACM Comput. Surv.* 35, 4 (Dec. 2003), 399 - 458. http://doi.acm.org/10.1145/954339.954342

[219] Accuracy and performance of biometric systems Gamassi, M.; Lazzaroni, M.; Misino, M.; Piuri, V.; Sana, D.; Scotti, F.Instrumentation and Measurement Technology Conference, 2004. IMTC 04. Proceedings of the 21st IEEE Volume 1, Issue , 18-20 May 2004 Page(s): 510 - 515 Vol.1

[220] http://magma.nationalgeographic.com/ngm/afghangirl/index.html

[221] http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf

There exist many DNA databases for criminal cases. In the UK, approximately 4.2 million people or seven percent of the population is in the database in 2006.[222] Compared to Germany and the USA, they only have DNA of 0.5 percent of the population. DNA data is easy to store and not expensive anymore to extract. The time to extract it is currently the limitation. In 2006, no commercial access control system existed based on DNA profile.

Handwriting is also commonly used in forensic science. It is used as evidence in forgery cases, kidnappings with ransom notes and many other crimes where handwriting is used. Document examiners also find much work in civil cases. Handwriting analysis is a field which covers lots of experience and training.[223] The handwriting examiners have several groups and quality assurance models in order to have solid conclusions. Databases of handwriting are developed[224], however they are not in widespread use. Also commercial implementation of handwriting comparison exists in the field of biometrics.

For forensic science, also several other biometric features are used as evidence. Evidence such as nail marks (from fingernails), are more easily accepted in court.[225]

The advantage of the databases of biometrics, such as fingerprints, irises, faces and many more, is that there exist a database and more information can be extracted from them based on statistics. The drawback is that the database should be filled in a standardised way, which in practice has been demonstrated[226] to be an issue.

5.5 Convenience

Another benefit and advantage of biometrics – hereby making abstraction of any possible adverse effect of biometrics as described in this report and other studies – is the ability of biometrics to simplify physical access to specific areas, networks and objects. As the biometric characteristic is always carried with the person, there is no risk of forgetting or losing the biometric. This is different with other access keys such as physical keys or personal identification numbers (PINs) as these keys need always to be carried or remembered. In smart cards, the signing functionality and data stored on the card are protected by a PIN. Now biometrics can be used in addition to the PIN, or even replace it, in order to unlock the card's functionality.[227] In a way, biometrics enhance user authentication indirectly if they are used to unlock a private key needed to perform the authentication.

The advantage of combining biometrics with a PIN is that they allow a finer control over the release of information from the card. They increase security without increasing the

---

[222] http://www.geneticsandhealth.com/2006/01/06/uks-largest-dna-database-in-the-world/

[223] http://en.wikipedia.org/wiki/Questioned_document_examination

[224] Automatic writer identification using connected-component contours and edge-based features of uppercase Western script Schomaker, L. Bulacu, M. AI Inst., Groningen Univ., Netherlands; Pattern Analysis and Machine Intelligence, IEEE Transactions on, Publication Date: June 2004. Volume: 26, Issue: 6 On page(s): 787- 798.

[225] JB Kempton, A. Sirignan, DH DeGaetano, PJ Yeat, WF Rowe, "Comparison of fingernail striation patterns in identical twins", Journal of Forensic Science, Vol. 37, 1992, 1534 - 1540.

[226] Geradts, Z., "Content-based retrieval from Forensic Image Databases", http://forensic.to/Dissertation.pdf

[227] See also M. Gasson, M. Meints, *et al.* (eds.), *o.c.* at footnote 3.

complexity towards the user. User acceptance is a critical success factor in eGovernment applications. Therefore it might be a good idea to take into account the preferences of the user and offer the ability to choose which biometric recognition mechanisms should be activated, if any. The potential convenience of integrating biometrics in electronic identity documents can give a boost to user acceptance and is a synergy of the government controlled ID model (Type I) and the convenience model (Type IV b).

Biometrics is not only an advantage to the benefit of the user-individuals because it is simple to gain access, but also an advantage for the entities which traditionally manage physical or magnetic keys (e.g., a hotel lobby or a car rental company) or passwords.

Moreover, the use of a biometric characteristic also allows distinguishing amongst multiple users of one product or service, which allows personalisation of the product or service. This area of application of biometrics for convenience is part of a larger area called Human-to-Computer Interaction (HCI). The goal of using biometrics in this case is to improve the performance and the accuracy of interfaces between human beings and computers. The biometrics would in that case allow the machine to recognise the user and to adapt the system to user specific characteristics for recognition tasks.[228] This feature of the use of biometric characteristics and systems could be applied to consumer products, such as cars or personal computers used by different persons. As everyday life may evolve into an ambient intelligence environment with seamless and ubiquitous computing, human-machine interface will gain importance.[229] In case biometrics are used in this context for purely private purposes and are fully controlled by the individuals, the applications would fall in Type IV a convenience model. HCI could however also be applied to an array of different services. In that case, HCI will not be solely controlled by the user (data subject), but also by a commercial organisation, in which case the use of the biometrics would exceed private use and fall in the Type IV b and c convenience model.

Concluding remarks on the advantages and needs of biometrics

By way of a conclusion, one can say that the increasing popularity of biometric technologies in combination with the association of some of them (e.g. fingerprints) with criminals is followed by an intensified concern over the loss of privacy and potential misuse of biometric data. The security vulnerabilities of current biometric systems and the resulting privacy concerns, however, seem to be mistakenly putting aside the privacy enhancing aspect of biometrics. Thus, an extended legal, social, economical and technical analysis of both positive and negative effects of biometrics on privacy should take place. From the technological perspective, applications must be designed and implemented following a decentralised vision and with the individual being given the ability to control access to his own biometric data, whereas the system should safeguard the individual's data and include mechanisms for the

[228] See also C. Vielhauer, *Biometric User Authentication for IT Security. From Fundamentals to Handwriting*, U.S.A., Springer, 2006, 14-15.

[229] See also FIDIS Deliverable 7.3 *Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence*, August 2005, 9 et seq. In this deliverable, SmartHome has been introduced and described as a private AmI environment.

protection of this data against theft or misappropriation. In fact, biometrics can be privacy enhancing if the technology is designed and implemented with this requirement in mind.[230]

[230] A. Cavoukian, *o.c.* above at footnote 119.

6 Recommendations and guidelines

In this report, an attempt is made to make a general overview of applications which deploy biometric functionalities. The risks of the use of biometrics and advantages of biometric verification or identification have been described, with reference where possible to the biometric types and models which were developed in section 3.3. This deliverable concludes with formulating some recommendations and guidelines for the further deployment of biometrics. The recommendations, guidelines and best practices for biometrics should keep the functionalities of biometrics and a specific model of application as discussed in section 3.3 in mind in order to be well understood and effective.

6.1 Best practice: some examples

If biometrics are stored in central database, such databases will be subject to attacks. Such attacks may have several purposes, including identity theft. Identity theft with the use of biometric information, however, could also occur in other ways, such as theft of traces unknowingly left. In order to cope with this concern, it should be further researched how templates, which are used for a specific application and stored on a local or central place, and which are often linked with other personal data such as name and address, which permit linking of biometric information with a 'civil' identity, *could be rendered unique by encryption* in such way that if the (uniquely) encrypted biometric template is stolen, it could be rendered useless (much like revocation of a PIN). In fact, biometric data cannot be used to secure or to authenticate because it can be intercepted easily. The strength of biometrics could be based on the fact that it provides a convenient piece of unique information which someone always has. However, as it will always remain subject to a risk of misappropriation, it should in a particular system be combined with other authentication information (such as a secret knowledge of an access number), which will reinforce the authentication. The strengthening of the authentication procedure could in fact be considered as a main purpose of use of biometric characteristics in private applications. The use and storage of templates is only a very partial solution as templates can also be stolen, and once stolen, it could still be used by an impostor. Therefore, one area of further research (and standardisation) could be the use of biometrics to secure and authenticate in a reliable way through the use of uniquely encrypted templates, which, once stolen, can be revoked and replaced. This may solve the storage problem of reference tokens, but it does not solve the problem of leakage in the biometric processing from the capture to the comparison component. This could be solved only by making attacks unattractive: decentralisation of critical data, user control and encapsulation of the whole processing into a tamper resistant device.

From an application point of view, a further rule on best practice should be to evaluate the proportionality of the use and the used functionality of the biometric data. Biometrics will in general be used to enhance the security of an application. However, because of the risks associated with biometrics as explained above, in particular also in relation with the type of control that is exercised over the biometric system (central, divided, multilateral), the use of biometric data shall be carefully designed and biometric data will only be used in cases where no other means are available to guarantee the same level of security. Furthermore, for most applications, the verification function of a biometric system will do.

6.2 The integration of biometrics in electronic documents issued by the government

In this section, we investigate the possibility to integrate biometrics in electronic documents issued by the government, which is an application of the government controlled ID model (Type 1). We discuss some of the privacy issues that arise with the integration of biometrics in these documents, and we present some solutions to tackle them.

6.2.1 Identity documents and issues

Identity documents come in many flavours and have many applications. According to their purpose, we can distinguish between "general purpose" identity documents on one hand, like national identity cards, and identity documents that were issued for a specific purpose on the other hand, like health insurance cards, travel documents or passports.

In general, identity documents provide three basic functionalities: identification; authentication of the owner; and storage of information needed to perform the first two functions, or other information related to the owner's identity such as the owner's address, gender, noble condition, etc.. Depending on the application, these functions are performed automatically or manually. Many governments already claim to be issuing biometric passports or eID cards because the owner's digital picture is stored in the document. This picture is, in many cases, only usable for manual verification of the owner's identity, and requires the presence of a human verifier. One can argue that this is hardly a biometric document.

The intended usage of the documents often determines their structure and limits their potential for including biometrics. Nowadays, travel documents are often no more than a paper booklet containing an integrated RFID chip with limited functionality; while the majority of the European national eID cards are smart cards with extended computational capabilities; e.g., many eID cards can be used to generate electronic signatures for strong authentication or to create legally binding signatures. Tamperproof smart cards offer more flexibility to include biometrics in a secure and privacy-friendly way than RFID chips.

Biometrics add security to applications because they provide a stronger link between the card and the card holder, thus between the physical and the electronic identity (see also *above*, section 5.1).

e-Government applications are used on a large scale, often nationwide, and therefore not all biometric modalities are suited for integration into identity documents because they do not offer a high degree of distinctiveness. However, one might consider using a "less unique" modality if it is only used to control the release of less critical information. An evaluation of suitable biometrics for e-Government applications and smart cards has been carried out by Dessimoz and Richiardi.[231]

[231] D. Dessimoz and J. Richiardi, *Multimodal Biometrics for Identity Documents*, Research Report PFS 341-08.05 v.1.0 (September 2005), available at http://www.biometricscatalog.org/documents/MBioIDStateOfTheArt_v1.0-8.pdf

Privacy issues with biometrics have been explained in chapter 4, and in the following section we will present three possible architectures[232] that offer a decentralised solution for integrating biometrics in identity documents.

As mentioned previously, one of the main functions of identity documents is to authenticate the holder. Very often, electronic identity documents are used to authenticate users online, with the incentive of getting access to a certain resource on the Internet. Therefore, the described systems also fit in the access control model (Type II).

6.2.2 Integrating biometrics in identity documents

6.2.2.1 Template-on-card

In order to increase the protection of the biometric reference template, it is possible to store it on a secure token like a smart card. This is called a template-on-card architecture, which avoids the use of databases containing large amounts of reference templates. These databases are considered to be worse than storage on a secure token because the latter rules out the possibility of using the biometric reference templates, which in fact should be regarded as unique identifiers, as keys in databases to increase linkability of personal data, from which different partial identities belonging to the same entity can be deduced (see also *above*, section 4.3.1).

Irrespective to the discussion of linkability, implementing relations between personal data and biometric database keys should be avoided, because this would require extensive processing of biometric data. This is negatively assessed by Rodotà[233], who bases his argument on Directive 95/46/EC of the European Parliament, because "the data subjects will have no possibility to object to the processing of their biometric data".

Database keys should be generated independently of biometric data so that it remains possible to use different keys for databases from distinct parts of a large organisation. For example, when government administrations store personal information electronically, it might be favoured not to use the same key for the linking of personal data stored by all authentic sources. This would allow the linking of pieces of information that is not justified by the presupposed purpose stated at the time of collection of the personal data. This purpose should be communicated clearly and not be violated afterwards.

In this architecture, the only thing the token provides for the biometric recognition process is the template. It is communicated through a secure channel to the reader's side where collection, extraction and matching takes place. The storage of the reference template on a secure token depends on the application and the identity document being used. When a user looses a card, a tamperproof smart card provides better protection of the reference template than a simple memory card.

The biometric matching is performed off-card, by the card reader or by a software module or middleware, and therefore the reference template has to leave the card. To prevent identity fraud, the reference template should be digitally signed to ensure the integrity and authenticity

---

[232] See also Yau Wei Yun and Chen Tai Pang Lawrence, *An introduction to biometric match-on-card*, Synthesis 2005 Section Three (2005), available at http://www.itsc.org.sg/synthesis/2005/3_BiometricMOC.pdf

[233] Stefano Rodotà, Working document on biometrics, IPA Herfstdagen on Security

(2003-08-01), http://www.win.tue.nl/ipa/archive/falldays2005/Paper_1_Leenes.pdf

of the template. At home, a user may trust her card reader or the system where the matching is performed, hence biometrics bring more convenience to the user (Convenience model - Type IV a). However this is not the case when the system is not under control of the user. This limits the use of biometrics to off-card recognition - in this system biometrics cannot be used to unlock the card's functionality.

6.2.2.2 Match-on-card

Although template-on-card already diminishes privacy concerns reasonably, these concerns can be further diminished with the matching on card of the freshly collected biometric template and the reference template. Although it is not required to combine match-on-card with storage-on-card, both implementations re-enforce each other's security and usually go together.

Most often in literature when the term match-on-card is used, also storage-on-card is implied and we adopt the same terminology. Collection and feature extraction is still performed on the reader's side, external to the card, but matching as well as storage of the reference template is now performed on the card. In this way, in the biometric recognition process, only the freshly collected template is being communicated outside the card and the reference template as well as the matching process stays in the secure environment of the card.

A match-on-card architecture is a more secure solution for biometric verification then just a storage-on-card architecture, but the freshly collected template still needs to be communicated. Obtaining this freshly collected template might be just as useful for an attack as obtaining the reference template. The user still has to trust that the reader and the system not to store any templates.

A drawback of this architecture is the lack of computational power in current smart cards to perform the matching on the card, although this will not be a hindrance in the near future.

An advantage of this system is that it can be used to unlock the card's functionality. However a general note on the security of biometrics is in place here. As mentioned earlier on, people leave their biometrics wherever they go and it is often possible to reconstruct fake samples, e.g., from latent fingerprints. eID card issuers should keep this in mind when deciding for what applications biometrics will be used. Most eID cards are capable of creating two types of electronic signatures; for authentication of the user and for creation of legally binding signatures. It is generally not a good idea to use biometrics for the latter. Nonetheless, with the match-on-card architecture it is possible to have a secure solution with increased convenience for its holder and since the card is issued by the government, the application is implicitly controlled by the government (Type IVb).

6.2.2.3 System-on-card

An even more secure solution for biometric verification is to include the biometric sensor on the card, on top of the previous match-on-card architecture - this is called system-on-card. This biometric system architecture currently is only an option for fingerprint and signature verification, thus a preference for the system-on-card architecture extremely limits the choice of biometric modality for integration in identity documents.

Choosing a system-on-card architecture increases the cost of the token, but decreases the cost of the system external to the token. The system-on-card is a totally self-containing system, keeping the reference and sample template on card as well as the matching process and

thereby leaving no opportunity to intervene maliciously, except in the communication between the card and the card reader, after matching is performed. Therefore, a secure communication channel remains imperative for any biometric recognition implementation, even for the system-on-card implementation.

Similar to the previous architecture, performance might be an issue here.

6.2.2.4 Hybrid Architectures

For many biometric modalities, it is not yet possible to perform biometric data collection, feature extraction and matching on a smart card. This leads to hybrid architectures based on the ones that were just explained.

A first option is to do feature extraction and matching on the card reader's side, but both the sensor and reference template storage remain on the smart card. A second option is similar, but only feature extraction is done off-card. These architectures are certainly not preferable, because both options require the transmission of raw biometric data from the card with the sensor on board to the card reader where extraction is done. Potential attacks that follow from this were indicated in section 4.1.

Besides this risk, we also note that fingerprint is the only biometric modality that currently has commercial implementations with a sensor-on-card architecture and that it is also possible to do fingerprint verification with a more secure system-on-card architecture. The requirement of transmission of raw biometric data has a negative impact on user's (perception of) privacy and thus on their acceptance of the biometric recognition implemented with these last two architectures.

6.2.2.5 Privacy-enhanced Biometrics

In the presented systems the reference data is used in the matching process which results in a yes or no answer. The problem is that this reference data is sensitive data that cannot be leaked which explains why the focus in the presented systems was on protecting the reference templates.

Several mechanisms exist to extract random information from biometrics that can be used as cryptographic keys. These keys can be used later in the matching process without leaking information about the user's biometrics or the key. The key not only serves to verify the user's identity but can also be used in cryptographic applications.

Due to the nature of biometrics, it is impossible to obtain two samples that are identical. Exact reconstruction of the key from a sample that is slightly different than the one used during enrolment requires some extra data that was derived from the original sample. A biometric verification architecture that uses public helper data was proposed by Linnartz and Tuyls[234]. The public helper data does not reveal any information about the derived keys or any useful information about the biometrics of the user. Similar structures called fuzzy extractors have been defined by Dodis[235] *et al*.

---

[234] J.P. Linnartz, P. Tuyls, *New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates*, AVBPA 2003, LNCS

[235] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: 'How to generate string keys from biometrics and other noisy data', *Proceedings of the International Conference on Advances in Cryptology* (EUROCRYPT '04), Lecture Notes in Computer Science, Springer, 2004.

A cryptographic hash of the derived key and the helper data can be stored in a central database without compromising the user's biometrics, without revealing the derived key and without violating the user's privacy. This mechanism is easily applicable to each of the architectures presented earlier on. The helper data can be stored on the identity card and even on an insecure storage token.

6.3 User Side Identity Management System – encapsulated biometrics

The biometric comparison process is far more complex than a password or PIN code check. It always includes physical measurement processes. Biometric authentication systems therefore all need some locally installed infrastructure to perform at least the capture process to which the data subject has to have physical access. This fact constrains the possible architectures of biometric systems. It is not possible to concentrate all processes in a physical completely secured environment; there are always points with immediate interaction with the outside world.

6.3.1 Drawbacks of traditional centralised biometric system architecture

Today's biometric systems often work within architectures with central controlled components (see figure 16 and discussion about control types in section 3.3). The server or the server controlled peripherals collect biometric data from the individuals through the capture devices. The further processing is done under the sole control of a centralised biometric application infrastructure which keeps the biometric information of all enrolees in an central and operator controlled database (most of Type I,II and III systems). Even if the centralised equipment is well protected, at least the capture devices are weak points in the system. In addition, the specific biometric characteristic may be expressed in very different forms from human to human. General purpose measurement equipment may fail to make an optimal raw data recording over the full population. As a consequence the requested features may not be reconstructed by the feature extraction algorithm for a substantial fraction of the population or the resulting query templates may be to far away for a unique and reliable result in the comparison step.

In addition centralised control systems bear all the dangers to the security and the privacy of the enrolled individuals that have been discussed in the previous chapters.

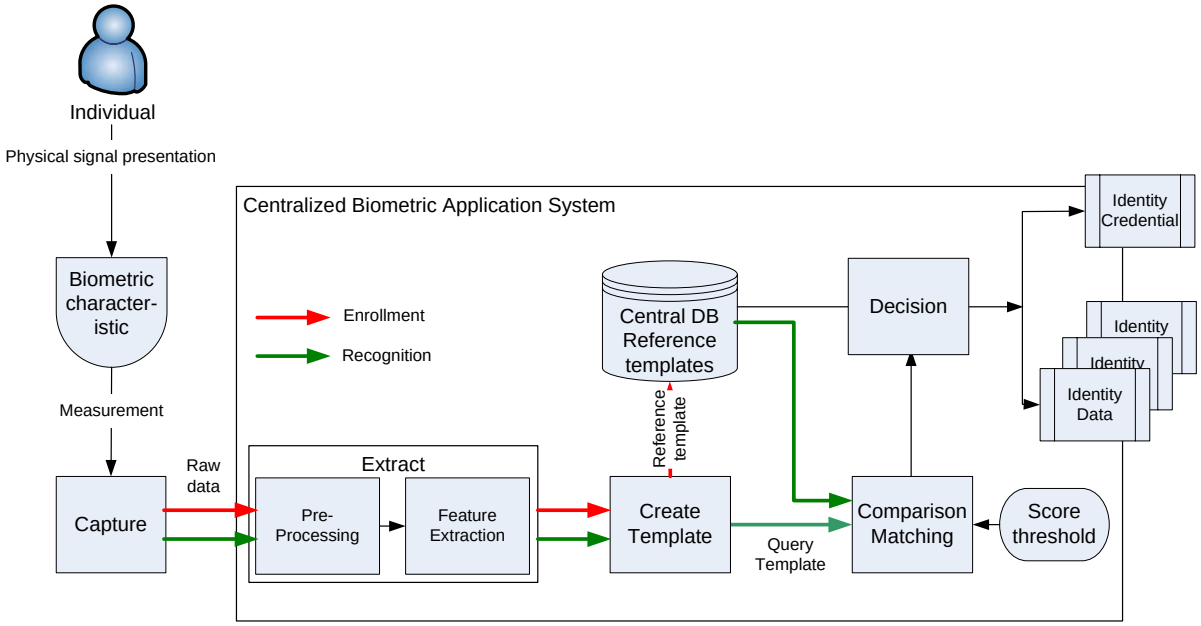

Figure 16: Architecture of a traditional centralised system. The box illustrates the security and control range of the operator.

6.3.2 User-side biometric process for added robustness

The storage of a biometric reference template, the measurement and the comparison process should be under the sole control of the user and then be linked in a secure way to a digital credential that does not disclose any biometric information. There are two alternative architectures that provide such a more robust biometric model with no single point of attack to threat the biometric data. These are:

- The concept of reference template on card.

Through the distribution of the reference templates to the enrolees with a smart card as carrier, the problem of large scale stolen biometric data can be solved. Still problematic is the fact that the processing system captures the biometric query samples without any possibility for the individual biometric data provider to control the further treatment of this data.

- The concept of encapsulated biometrics.

This new system is a consequent continuation of the distributed control approach (Type II c) where the full processing and storage of the biometric data is distributed to the enrolled individuals in the form of a tamper resistant token (system architecture see figure 17). The token hardware and its integrated functions are produced by the system operator and no one can change these functions at reasonable costs. In this sense, the operation functionalities are controlled by the operator. On the other hand, the delivery, the storage and the use cases are controlled by the user who decides if he wants to use his token. The user especially also controls the physical device with the stored biometric data. Such a concept has been developed and will be described in D3.14. The key component of such a biometric authentication system is an autonomous personal token with sufficient computing, electrical power and hardware resources to perform the full biometric processing in the token. The

token provides cryptographically secure communication channels with the central authentication system. Only digital identity credentials without any biometric information can leave the token to confirm a successful verification of the identity claim of the user. The whole implementation is protected in a tamper resistant processor on the token. Such an implementation reduces to a great extent the above discussed threats to a biometric system.

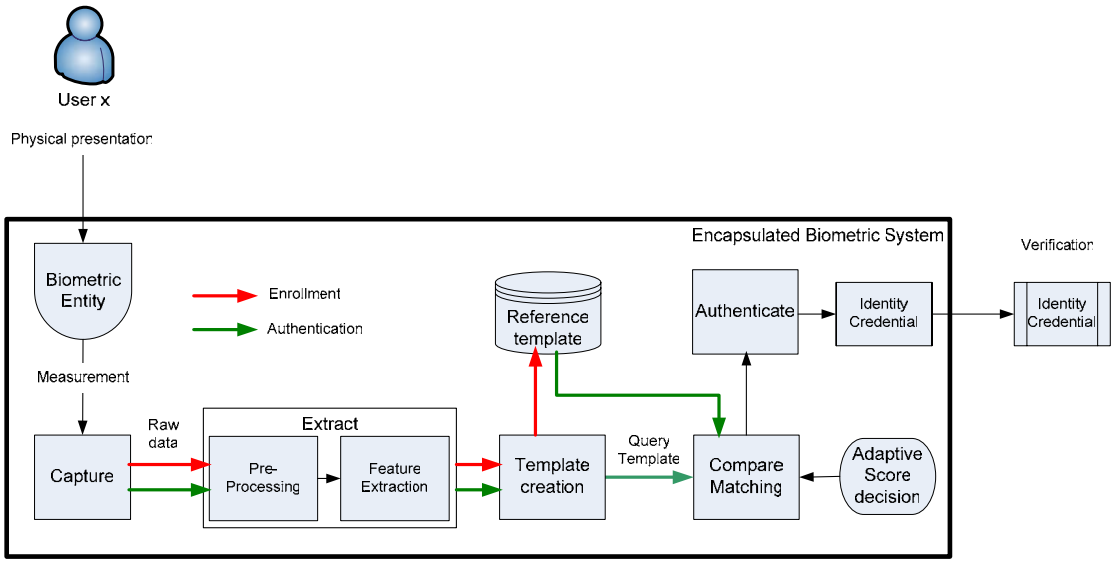

Figure 17: The encapsulated biometric system is a realisation of the previously defined multilateral control model (Type II c). The biometric system is defined and provided by the operator and enclosed in a highly secure and tamper resistant implementation (e.g. sealed token). The user as data subject has the full control over the use of the device.

6.4 Future areas of research

Most authors on biometrics agree that the legal aspects of the use of biometric data for verification and identification purposes should be further researched and, if needed, regulated. Because of the privacy and security risks, the legislator could also impose specific technical safeguards and conditions on the use of biometric applications. This is in general only partially done for the use of biometrics in specific biometric Type I governmental controlled ID model applications, such as the use of biometrics in ePassports. The imposed measures for the storage of biometrics in the RFID enabled ePassports however are still criticised as being insufficient and should therefore be further researched. Specific technical safeguards and conditions for the use of biometric data in other applications are in most countries not even regulated.

Biometric methods are still further developed and researched. For certain methods, especially face geometry measurement, impressive improvement in quality was achieved in the last two years. In addition, security and privacy protection of the implementation of certain biometric systems was improved significantly, as new methods for template protection were developed and encapsulated biometrics became available on the market. Research with the target of further improvements should (and will) be continued.

Research with respect to additional information in biometric reference data (both, raw data and templates) is needed – especially templates are mostly not investigated in this respect.

Because raw data and templates can also be stolen and abused by impostors, further research is also needed on the use of uniquely encrypted templates, which, once stolen, can be revoked and replaced.

The availability of this type of research results would be very useful in the risk assessment of biometric methods (with respect to privacy also called Privacy Impact Analysis, PIA[236]) and the assessment of proportionality of different methods for the same purpose in comparison.

[236] Clarke, R., *Privacy Impact Assessments*, Xamax Consultancy Pty Ltd, Canberra, Australia, 1997.

7 Conclusions

This report analysed in detail the steps of a biometric authentication process and stressed that at all times the functionalities of biometrics, i.e. identification and verification, should be properly distinguished and understood. Specific models of application which are suggested in section 3.3 should be kept in mind in order to facilitate the debate about the use and regulation of biometrics. These models can be summarised in five main types, according to the purposes for which the biometrics are used, the controller(s) and the type of control over the biometrics. The main types which were found and described are a government controlled ID model (Type I), an access control model (Type II), a public-private (mixed) model (Type III), a convenience model (Type IV) and a surveillance model (Type V). Control over the biometrics differs in each of these types and an appropriate regulation for many of these types, such as for example for the multilateral control and use of biometrics in travel documents or for the use of biometrics by employers for access control purposes of employees, is not in place yet. At the same time, the research describes that the decisions of the Data Protection Authorities show a great diversity in criteria and requirements applied to biometric systems, often leading to contrary decisions for similar systems. This does not at all concur with the harmonisation attempted by the Privacy Directive. The proportionality criterion which is invoked by these authorities is an area of further research. In addition, appropriate terms for the biometric process should be used. The standardisation work in general and the work on a harmonised vocabulary for biometrics, such as which is presently ongoing in ISO/JTC 1 SC 37, is indispensable for a good debate and understanding of the critical aspects of biometrics.

The report emphasised the various quality factors in the biometric capture and extraction process, in particular the system errors and failures in relation to both the verification and identification mode. It stressed that notions of FMR and FNMR become complex if biometrics are used in the identification mode as it is in that case not clear which reference template in the list with matches over the threshold really belongs to the individual. Especially in identification mode, the values of FMR(T) and FNM(T) are approximated calculations over the biometric variability of the identifiers within a population. These values are not calculated for each separate individual (as this is practically not feasible) and are also not dependant from the position of the compared templates in the feature vector phase space. The comparison functionality of biometric systems in the identification mode has therefore intrinsic limitations. Parties involved in the biometric process and regulators should understand this and the interpretation of the expected or promised values shall be made with care.

This document has also further explored how biometrics may eventually become a primary and interoperable key under which other data can be categorised and stored. The use of biometric identifiers in the context of large scale databases, such as in Eurodac, VIS and SIS II, and the cooperation set forth in the Prüm Treaty, support this premise. The European Data Protection Supervisor opposes such use, as well as other experts in various reports. Especially interoperability with systems outside the EU (Type I b Government controlled ID model), between law enforcement and private systems (Type III Mixed model) and in intelligence led policing (Type V Surveillance model), should be addressed appropriately and needs an adapted framework.

The report argues that protecting biometrics should start at the place where the biometric data are collected, i.e. the collection device. Anno 2007, there are still many biometric data

scanners, in particular fingerprint scanners, which do not provide for any data encryption at all and which are not adequately protected from spoof attacks and data interception attempts. From the scanners which have no encryption, the fingerprint images could be reconstructed as described in this report.

The document stressed various other privacy problems in relation with biometrics, such as the difficulties in reaching data quality or the fact that not only captured biometric samples but also the biometric templates may contain sensitive information about someone's health. The report contains in this respect an extensive overview of biometric methods and related information about someone's health condition in captured biometric samples that could also be included in templates as no systematic research has been carried out so far with respect to remaining additional information in such templates.

The report finally underlined the advantages of biometrics, as biometrics remain an undeniably unique tool to link an individual to the digital world and made recommendations as to making an efficient use of this new technology. In order to combine the advantages while minimising the risks of abuse of biometric data, the concept of encapsulated biometrics is described. According to this concept, the biometric data remain under the control of the data subject, and the data subject has increased decision powers as to when and for what purposes its biometrics are going to be used. This type of use of biometrics could well be combined in a Type 3 IMS system for user-controlled context-dependent role management, as described in earlier deliverables of FIDIS.

8 Bibliography

Andronikou, V., Demetis, D., Varvarigou, Th., 'Biometric Implementations and the Implications for Security and Privacy', 1st in-house FIDIS journal issue, 1-2007, available at http://journal.fidis.net/fileadmin/journal/issues/1-2007/Biometric_Implementations_and_the_Implications_for_Security_and_Privacy.pdf

Ang R., R. Safavi-Naini, L. McAven, 'Cancelable Key-Based Fingerprint Templates', ACISP 2005, pp. 242-252, 2005.

Archmann, S. and M. Meyerhoff Nielsen, 'Interoperability at Local and Regional Level- a logical development in eGovernment', *EIPASCOPE* 2006/1, pp 39-44.

Article 29 Data Protection Working Party, *Working document on biometrics*, 1 August 2003, 11 p.

Article 29 Data Protection Working Party, *Opinion on Implementing the Council Regulation (EC) N° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, 30 September 2005, 12 p.

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 20 June 2007, 26 p.

Ashbourn, J., 'The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies', *Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission January 2005.

Avoine, G., Kalach, K., and Quisquater, J.-J., *Belgian Biometric Passport does not get a pass… Your personal data are in danger*, June 2007.

Backhouse, J., `Interoperablity of Identity and Identity Management Systems´ in: *Datenschutz und Sicherheit*, 2006, vol 30, 9, pp 568-570.

Balzacq, T et al, *Security and the Two-Level Game: The Treaty of Prüm, the EU and the management of threats*", CEPS Working Document No 234/ January 2006.

Balzacq, T and S. Carrera (eds.), *Security v Freedom: A Challenge for Europe's Future*, 2006, Brussels, CEPS

Bauer, M., Meints, M., (eds.), *D 3.1 Structured Overview on Prototypes and Concepts of Identity Management Systems*, FIDIS, 2004, 77 p.

Bekkers, V *et al.* (eds), *Information and Communication Technology and Public Innovation; assessing the ICT-driven modernization of public administration*, IOS Press, Amsterdam 2006, pp 219-229.

Bekkers, V., H. van Duivenboden and M. Thaens, 'Public Innovation and Information and Communication Technology: relevant backgrounds and concepts' in Bekkers, 2006, pp 3-21.

Benecke, M., 'Coding or non-coding, that is the question', *EMBO reports* vol. 3 no. 6, June 2002, available at http://www.benecke.com/coding.pdf

Boult, T. E., Scheirer, W. J., Woodworth, R., 'Revocable Fingerprint Biotokens: Accuracy and Security Analysis', Computer Vision and Pattern Recognition, 2007. CVPR '07. IEEE Conference on 17-22 June 2007.

Brömme, A., *A Discussion on Privacy Needs and (Mis)Use of Biometric IT-Systems*.

Brown, D., Brook, D., 'Biometrics: Implications and Applications for Citizenship and Immigration - Report on a Forum hosted by Citizenship and Immigration Canada', October 7 & 8, 2003 – Ottawa, Ontario.

Cavoukian, A., *Consumer Biometric Applications : A discussion paper*, Toronto, Information and Privacy Commissioner, Ontario, September 1999, 62 p.

Cavoukian, A., *Privacy and Biometrics*, Toronto, Ontario, Information and Privacy Commissioner, Ontario, September 99, 15 p.

Cavoukian, A. and Stoianov, A., *Biometric Encryption : A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, in, Information and Privacy Commissioner, Ontario, March 2007, 48 p.

Cheung K. H., Ad. Wai-Kin Kong, D. Zhang, M. Kamel, Jane You, Ho-Wang Lam, 'An Analysis on Accuracy of Cancelable Biometrics Based on BioHashing', Lecture Notes in Computer Science, Springer, 2005, pp. 1168-1172.

Clarke, R., 'Biometrics' Inadequacies and Threats, and the Need for Regulation', Presentation on the Computers, Freedom & Privacy 2002, available at http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html

Cole, S. A., *Fingerprint Identification and the Criminal Justice System: Historical Lessons for the DNA Debate*, University of California, Irvine. Download via http://www.ksg.harvard.edu/dnabook/

Commission of the European Communities, *Communication to the Council and the European Parliament on improved effectiveness, enhanced operability and synergies among European Databases in the area of Justice and Home Affairs*, COM (2005)597 final, Brussels, 25 November 2005.

Commission of the European Communities, *Communication to the Council and the European Parliament on* Interoperability for Pan-European e-Government Services, COM (2006) 45, 13 February 2006

Commission of the European Communities, *Proposal for a Council Framework Decision on the Exchange of Information under the Principle of Availability*, COM(2005) 490 final,12 October 2005

Commission of the European Communities *Implementing the Hague Programme: the Way Forward*, COM (2006) 331 final Communication, 28 June 2006

Commission of the European Communities, Communication from the Commission to the Council and the European Parliament. *Evaluation of EU Policies on Freedom, Security and Justice*, COM(2006) 332 final, 28 June 2006

Commission of the European Communities, *Report on the implementation of the Hague Programme for 2005*. COM(2006) 333 final Communication from the Commission to the Council and the European Parliament, 28 June 2006.

Committee of experts on data protection (CJ-PD), The introduction and use of personal identification numbers: the data protection issues, Study prepared by the under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1991, chapter II,

available at http://www.coe.int/T/E/Legal_affairs/Legal_co-cperation/Data_protection/Documents/Publications/4Pins.asp#TopOfPage

Commissie voor de Bescherming van de Persoonlijke Levenssfeer, *Verslag over de werkzaamheden 2005*, 2005, 159 p.

Council Of Europe, *Progress report on the application of the principles of convention 108 to the collection and processing of biometric data*, Strasbourg, February 2005, 26 p.

Dessimoz, D. and Richiardi, J., *Multimodal Biometrics for Identity Documents*, Research Report PFS 341-08.05 v1.0 (September 2005), http://www.biometrics catalog.org/documents/MBioIDStateOfTheArt_v1.0-8.pdf

De Hert, P., W Schreurs and E. Brouwer, 'Machine-readable identity documents with biometric data in the EU: Overview of the legal framework', *Keesing Journal of Documents and Identity*, Issue 21, 2006, pp 3-10.

De Hert, P. and A. Sprokkereef, *An Assessment of the Proposed Uniform Format for Residence Permits: Use of Biometrics*, CEPS Briefing Note for the European Parliament's committee on Civil Liberties, Justice and Home Affairs, IP/C/LIBE/FWC/2005-xx, can be retrieved from www.ceps.be.

De Hert, P., *What are the Risks and What Guarantees Need to be Put in Place in View of Interoperability of Police Databases?* 01.02.2006 IP/C/LIBE/FWC/2005-25, Briefing paper for the EP Citizens Rights and Constitutional Affairs Committee, available through http://www.ipolnet.ep.parl.union.eu/ipolnet/cms, (section 4).

De Hert, P., V. Papakonstantinou and C. Riehle, *Data Protection in the Third Pillar. Cautious Pessimism.*

De Leeuw, E., 'Biometrie en nationaal identiteitsmanagement', *Privacy en Informatie* 2007, afl. 2, 50-56.

European Data protection Supervisor (EDPS), 'Common Consular Instructions-EDPS opinion', *EDPS Newsletter*, no. 7, 14 December 2006, 2 (www.edps.europa.eu.)

European Biometrics Forum (forthcoming), *Security & Privacy in large Scale Biometric Systems*, A report commissioned by JRC/ITPS

European Commission, Joint Research Centre (DG JRC), Institute for Prospective Technological Studies (IPTS)'**,** *Biometrics at the Frontiers: Assessing the Impact on Society*, Brussels 2005, available at http://www.biteproject.org/ documents/EU_ Biometrics _at_the_Frontiers.pdf

Gasson, M., Meints, M. *et al.*, (eds.), *D.3.2.: A study on PKI and biometrics*, FIDIS, 4 July 2005, 138 p.

Geradts, Z., Sommer, P. (eds.), D6.1. 'Forensic Implications of Identity Management Systems', FIDIS, 2005, available at www.fidis.net

Gijrath, S., 'Interoperability Revisited: How far stretches the duty to negotiate interconnection?', *Computer and Telecommunications Law Review*, 2006/1

Grijpink, J. H. A. M., 'Een beoordelingsmodel voor de inzet van biometrie', *Privacy & Informatie* 2006, afl. 1, 14-17.

Hildebrandt, M., Backhouse, J. (eds.), *D.7.2. Descriptive analysis and inventory of profiling practices*, FIDIS**,** 2005, available at http://www.fidis.net/fileadmin/fidis/_deliverables/fidis-wp7-del7.2.profiling_practices.pdf

Jacobs, B., 'Select before you Collect', *Ars Aequi*, vol. 54, December 2005, 1006-1009

Jay, R. and Hamilton, A., *Data Protection. Law and Practice*, London, Sweet & Maxwell, 2003

Juels, A., Molnar, D. and Wagner, D., 'Security and Privacy Issues in E-Passports', *Proc. 1st Intl. Conf. on Security and Privacy for Emerging Areas in Communications Networks, IEEE Computer Society, Los Alamitos, CA*, vol. 2005, 74-85.

Kindt, E., 'Biometric applications and the data protection legislation', *Datenschutz und Datensicherheit* 2007, vol. 3, 166-170.

Linnartz, J.P. and Tuyls, P., New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates, AVBPA 2003, LNCS

Lips, M. Taylor and Organ, 'Identity Management as a Public Innovation: looking beyond ID cards', in Bekker *et al.* (2006), pp 204-216

Lodge,J., 'EJustice, Security and Biometrics: the EU's Proximity Paradox', *European Journal of Crime, Criminal Law and Criminal Justice*, 2005, Vol 13 no 4., pp 533-564

LSE, *The Identity project: an assessment of the UK identity project and its implications*. London, 2005.

Ludford, S. (rapporteur), EP working document on the proposal for a regulation of the European Parliament and of the Council amending Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa application COM(2006 (88), PE 386.565v01-00

Meints, M. and Hansen, M. (eds.), *D3.6. Study on ID Documents*, FIDIS, 2006, 160 p.

Meints, M., 'Implementierung grosser biometrischer Systeme. Kriterien und deren Anwendung am Beispiel des ePasses', Datenschutz und Datensicherheit 2007, afl. 31, 189-193.

Müller, G., Rannenberg, K., *Multilateral Security in Communications*, Vol. 3 Technology, Infrastructure, Economy, Addison Wesley, München 1999.

National Consultative Ethics Committee For Health And Life Sciences, Opinion N° 98 . Biometrics, identifying data and human rights, 26 April 2007, 22 p.

Oliver, G. M., *study of the use of biometrics as it relates to personal privacy concerns*, July 31, 1999, available at: http://faculty.ed.umuc.edu/~meinkej/inss690/oliver/Oliver-690.htm

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

Pfitzmann, A. and Hansen, M., *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v.0.30*, 26 November 2007, available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Ploeg, I. Van der, 'The Illegal Body: 'Eurodac' and the Politics of Biometric Identification, *Ethics and Information Technology,* 1999, 1, pp 295-302

Prabhakar, S., Pankanti, S. and Jain, A.K., "Biometric recognition: security and privacy concerns," *Security & Privacy Magazine*, IEEE , vol.1, no.2 pp. 33- 42, Mar-Apr 2003.

Prins, C., 'Making Our Bodies Work for Us: Legal implications of Biometric Technologies', *Computer Law & Security Report*, 14. no 3., 1998, pp 159-165

Ratha N. K., J. H. Connell, and R. M. Bolle, 'Enhancing security and privacy in biometrics-based authentication systems', *IBM Systems Journal*, 40(3), 2001

Rejman-Greene, M. (Ed.), *Roadmap for Biometrics in Europe to 2010*, BioVision, 15 October 2003, 202 p.

Rigoutsos, I., Huynh, T., Miranda, K., Tsirigos, A., McHardy, A. , Platt, D., 'Short blocks from the noncoding parts of the human genome have instances within nearly all known genes and relate to biological processes', *Proceedings of the National Academy of Science of the United States* vol. 103 no. 17, pp. 6605-6610, Washington D. C., April 2006.

Rodotà, S., Working document on biometrics, IPA Herfstdagen on Security, August 1, 2003, available at http://www.win.tue.nl/ipa/archive/falldays2005/Paper_1_ Leenes.pdf

Rotenberg, B., *The Legal regulation of Software Interoperabilty in the EU: confronting Microsoft with Appleby and Chasagnou*, Jean Monnet Working Paper 07/05, 2005, New York, NYU School of Law

Soutar, C., Roberge, D., Stoianov, Al., Gilroy, R., Kumar, B.V.K. V., 'Biometric Encryption', chapter 22 in ICSA Guide to Cryptography, edited by Randall K. Nichols, McGraw-Hill, 1999.

Thomas, R., 'Biometrics, international Migrants and Human Rights', *European Journal of Migration and Law*, 2005, vol 7, pp 377-411

Toh, K.-A., Lee, Ch., Choi J.-Y., and Kim J., *Performance based revocable biometrics*, Industrial Electronics and Applications, 2007, ICIEA 2007, 2nd IEEE Conference on 23-25 May 2007.

Van Blarkom, G.W., Borking, J.J., Olk, J.G.E., *Handbook of Privacy and Privacy-Enhancing Technologies – The case of Intelligent Software Agents*, College bescherming persoonsgegevens, 2003, 33 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, 2-66.

Von Graevenitz, G., *Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren*, LIT Verlage, Berlin 2006.

Von Hardenberg, I., 'Warum Neugeborene mehr wissen, als Große manchmal ahnen', *GEO (7)*, pp.27-42, Hamburg, July 2001.

Wallwork, A. and J. Baptista, 'Understanding Operability' in J. Backhouse (ed.), *Structured Accounts of Approaches on Interoperability*, Ch 4, Report D4.1 Future of Identity in the Information Society (FIDIS), 6th Framework Programme, European Commission, 2005, pp 19-24, see p 20, available through: http//www.fidis.net/487.0.htm#820

Weichert, T., 'Staatliche Identifizierung durch Biometrie', *Datenschutz Nachrichten* 2004, afl. 2, 9-19.

Yanikoglu B. and Al. Kholmatov, 'Combining Multiple Biometrics to Protect Privacy', Proceedings of ICPR-BCTP Workshop, Cambridge, England, Aug. 2004.

Yau Wei Yun and Chen Tai Pang Lawrence, An introduction to biometric match-on-card, Synthesis 2005 Section Three (2005), http://www.itsc.org.sg/synthesis/2005/3_BiometricMOC.pdf.

Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate string keys from biometrics and other noisy data. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04), Lecture Notes in Computer Science. Springer Verlag, 2004.

Annex 1: Acronyms and Glossary

Note of the editors:

For biometric terms and terminology, the editors refer in the first place to the definitions and terms as currently being drafted by the ISO JOINT TECHNICAL COMMITTEE ISO/IEC JTC 1, SUBCOMMITTEE SC 37.

The latest version of the working document is named Biometrics. Standing Document 2 (SD 2) version 8, Harmonized Biometric Vocabulary, is dated 22 August 2007 and is available at: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/2263034/2299802/JTC001-SC37-N-2263.pdf?nodeid=6714553&vernum=0 (last visited on 30 August 2007).

Terms of the glossary of the present report which are defined in that working document are indicated with an asterisk and the suggested definition of the aforementioned working document of JTC 1/SC 37 is used in this glossary.

An extract of the terms of a previous version of a working document of this group is also available at:

http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&objAction=browse&sort=name (last visited on 29 June 2007))

A shorter list of biometric terms which is already available since some time can be found on the CESG-Homepage (National Technical Authority for Information Assurance, UK), at:

http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=401 (last visited on 30 August 2007).

Some of the terms mentioned at the CESG page are also mentioned in this glossary.

Because the definition of biometric vocabulary is in full development, full consistency of the terms used in this glossary as well as in the present report has been strived for but is not guaranteed.

Attempt	The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify
AFIS	Automated Fingerprint Identification System
AFNOR	Association Française de Normalisation
BAC	Basic Access Control
BEM	Biometric Evaluation Methodology
BEM WG	BEM Working Group
Biometrics*	Automated recognition of individuals based on their behavioural and biological characteristics
BioAPI	Biometrics Application Programming Interface standard
Biometric data*	Biometric sample at any stage of processing, biometric reference, biometric feature or biometric property
Biometric feature*	Numbers or labels extracted from biometric samples and

	used for comparison
Biometric identification application*	System which contains an open-set or closed-set identification application
Biometric reference*	One or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used for comparison
Biometric sample	A biometric measure presented by the user and captured by the data collection system
Biometric system*	System for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics Note that in CC evaluation terms, a biometric system may be a product or may be (part of) a system for evaluation
Biometric template*	Set of stored biometric features comparable directly to biometric features of a recognition biometric sample
Biometric verification (application)*	Application that shows true or false a claim about the similarity of biometric reference(s) and recognition biometric sample(s) by making a comparison(s)
BIR*	Biometric Information Record
CBEFF	Common Biometric Exchange File Format standard
CC-BEM	Common Criteria Biometric Evaluation Methodology
CEM	Common Criteria Evaluation Methodology
Closed-set identification*	Application that ranks the biometric references in the enrolment database in order of decreasing similarity against a recognition biometric sample
Common Criteria	An international scheme for the security evaluation and certification of IT systems
Comparison*	Estimation, calculation or measurement of similarity or dissimilarity between recognition biometric sample(s)/biometric features/biometric models and biometric reference(s)
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EDPS	European Data Protection Supervisor
Enrolee	A user with a stored biometric reference template on file
Failure to acquire rate (FTA)	The failure to acquire rate is the proportion of attempts for which a biometric system is unable to capture an image of sufficient quality. When a biometric system allows multiple attempts, FTA measures failure to capture over these multiple attempts

Failure to enrol rate (FTE)	The failure to enrol rate is the proportion of the user population for whom the biometric system is unable to generate reference templates of sufficient quality. It is the equivalent of FTA for the enrolment process, and depends on the procedures used in enrolment (which may differ from the procedures for later identification). It includes those who, for physical or behavioural reasons, are unable to present the required biometric feature
False Acceptance	An incorrect identification of an individual, or an incorrect verification of an impostor
False Accept Rate (FAR)	The probability that a biometric system will incorrectly identify an individual, or will fail to reject an impostor. For a positive (verification) system, it can be estimated from: (the number of false acceptances) ÷ (the number of impostor verification attempts)
False Match Rate (FMR)	The rate for incorrect positive matches by the matching algorithm for single template comparison attempts. For a biometric system that uses just one attempt to decide acceptance, FMR is the same as FAR. When multiple attempts are combined in some manner to decide acceptance, FAR is more meaningful at the system level than FMR
False Non-Match Rate (FNMR)	The rate for incorrect negative matches by the matching algorithm for single template comparison attempts. For a biometric system that uses just one attempt to decide acceptance, FNMR is the same as FRR. When multiple attempts are combined in some manner to decide acceptance, FRR is more meaningful at the system level than FNMR
False Rejection	A failure to identify or verify a genuine enrolee
False Reject Rate (FRR)	The probability that a biometric system will fail to identify a genuine enrolee. For a positive (verification) system, it can be estimated from: (the number of false rejects) ÷ (the number of enrolee verification attempts)
Impostor	A person making a false claim about identity to the biometric system
ICTs	Informaton and Communication Technologies
Matching score	A measure of similarity or dissimilarity between the biometric data and a stored template, used in the comparison process

Multimodal biometric	A biometric device which uses information from different biometrics - e.g. fingerprint and hand shape; or fingerprints from two separate fingers. All statistical analysis of multimodal systems should consider how the modes are combined in the comparison process
Negative claim	A claim by a user not to be enrolled in the biometric system. This may be needed to establish that double claims are not being made
MRTDs	Machine Readable Travel Documents
NIST	National Institute of Standards and Technology
One-to-many comparison*	Process in which a recognition biometric sample/biometric feature/biometric model set of one biometric data subject is compared against the biometric references of more than one biometric data subject to return a set of comparison scores
One-to-one comparison*	Process in which a recognition biometric sample/biometric feature/biometric model set from one biometric data subject is compared to biometric reference(s) to produce a comparison score with respect to one biometric data subject, perhaps using additional data from the enrolment database
Open-set identification*	Application that determines a possible empty candidate list by collecting one or more biometric samples from a biometric capture subject and searching the enrolment database for similar biometric references
Positive claim	A claim by a user to be enrolled in the biometric system. An explicit claim is often accompanied by a user identification, and may also be associated with a password or PIN.
PP	Protection Profile. A form of generic Security Target defined in the Common Criteria
Receiver Operating Characteristics (ROC)	A method of showing the performance of the biometric system over a range of decision criteria - usually shown as a graph that relates FAR to FRR as the decision threshold varies
ROC	Receiver Operating Characteristics
ROC curve	Receiver Operation Characteristic curve
SOF	Strength of Function
Template ageing	The gradual change of a user's biometric feature(s) which requires periodic updating of the user's reference template
Threat	An intentional or unintentional potential event that could compromise the security integrity of the system
Threshold	A parametric value used to convert a matching score to a decision. A threshold change will usually change both FAR

	and FRR - as FAR decreases, FRR increases
UI	User Interface
UKBWG	UK Biometric Working Group
Vulnerability	The potential for the function of a biometric system to be compromised by e.g. intention (fraudulent activity); design flaw (including usage error); accident; hardware failure; or external environmental condition

Annex 2: Characteristics of the different control schemes

Control scheme	Characteristics	Security aspects	Privacy aspects
Central control	Biometric system controlled by a single organisation (data controller). Mostly centrally hosted database of reference templates. Individual data subjects deliver their biometric sample to the system on request of the operator (controller). Treatment and interpretation of the data is controlled by the operator (controller) only. Applied in the verification and identification mode.	Operator has to supply and guarantee confidentiality, integrity and availability of the data processed using the biometric system over the full lifetime. Central storage of the reference templates and the central processing leads to the scaling problem and it is a critical point of failure or attack.	The data subject has no individual control over the use of his biometric data.
Divided control with trust	Biometric system is shared between organisations which use all the same central reference template repository or operated using an external service provider. Capture and processing are distributed over the operator federation. The processing follows common standards. There is a common security and privacy policy which however is only marginally influenced by the data subject.	One or more data controllers are responsible for the central security concept of the biometric system, dealing with confidentiality, integrity and availability of the data. Security in the system is based on trust, which in turn is based on Security Service Level Agreements (SSLAs), (mutual) audit schemes and in cases needed also fines. The distribution of	The data subject has no individual control over the use of his biometric data. Data subject may be traced over all involved organisations. In some cases, multiple enrolments and identity mismatch may lead to serious problems for the concerned persons.

		the reference templates to the peripheral control instances is critical. Leakage of biometric data needs to be prevented.	
Multilateral control	The multilateral control model allows an easy sharing of the biometric application among different operators without allowing a direct access to biometric data. It requests a relative high level of standardisation of the biometric processing and the biometric data representation.	ISO 27001 covers control objectives and controls for a situation where a risk assessment covering all relevant assets is carried out centrally or jointly, leading to a standardised level of security requirements and measures spanning all participating organisations. A situation of multilateral security requirements is not covered by ISO 27001 and other security management standards.	The data subject has no individual control over the use of his biometric data.
Divided control with data subject	Control over the biometric system is divided among data controller and data subjects who may have different security requirements. The biometric system is defined and sealed within a physical device by the operator (e.g. encapsulated in a personal token or match-on-card schemes). The operator provides at least parts of the biometric system to the data subject	The compartmentali-sation of the biometric data makes a general loss of such data hardly impossible. The storage of a single or of only very few templates in a device prevents an attacker to invest in the breaking of such a device as the return on investment	The biometric data stays always under the full control of the data subject. The operator has no direct access to the biometric data and therefore can not cause any biometrics related privacy violation.

	who decides about the enrolment and the occasions to be recognised by the system. The biometric data never leave the device; only the result of the decision step is sent to the operator. The biometric data remain under the control of the data subject who decides about the recall or the destruction of this data. The system may operate in the identification mode without any loss of performance.	is too low. The system can be scaled to arbitrary number of units and thus individuals enrolled in the system. There is no scaling problem. The device carrying the biometric system has to be secured to prevent from attacks by non cooperative users.	
Data subject control	The biometric system and the biometric processing is under the full and sole control of the data subject. There is no guarantee on the reliability of the biometric recognition process and therefore it will not be trusted by an external operator of a value service	The outcome of the biometric recognition process is under the control of the data subject only. An external organisation can not trust this outcome more than any other uncertified identity statement of the data subject.	The privacy of the biometric data needs to be protected by the data subject. The data subject may lose the control by inadvertence or under attack of a malware.