



Project no. ICT-2007-216339

## TURBINE

### TrUsted Revocable Biometric IdeNtitiEs

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

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

## D2.3.3 Research findings for standardisation

Due date of deliverable: 31/01/2010

Actual submission date: 02/02/2010

Publication date: 02/02/2010

Start date of project: 1 February 2008

Duration: 36 months

Name of lead contractor for this deliverable: Bian Yang, Christoph Busch, Davrondzhon Gafurov, Patrick Bours (GUC)

Name of reviewers for this deliverable: Vincent Despiegel (SAG), N. Delvaux (SAG), S. Despinoy (ART)

Abstract: This deliverable reviews biometric template protection relevant standards and presents the research findings which are promising for standardisation from the TURBINE project.

Revision R1

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

## Table of Contents

---

<b>Glossary .....</b>	<b>2</b>
<b>1. Executive Summary.....</b>	<b>3</b>
<b>2. Introduction .....</b>	<b>4</b>
2.1 Project scope .....	4
2.2 Background and objectives .....	4
2.3 Organization .....	5
<b>3. Standards Overview .....</b>	<b>6</b>
3.1 Standards on Biometrics .....	6
3.1.1 ISO and ISO/IEC standards.....	6
3.1.2 Other Standards.....	7
3.2 Targeted Standard - ISO/IEC JTC1 WG5 SC27 24745 (Biometric Template Protection).....	7
<b>4. Potential Contributions to Standards .....</b>	<b>8</b>
4.1 Security and Privacy Requirements on Biometric Template Protection.....	8
4.2 A General Framework for Template Protection Equipped with “Renewability” .....	8
4.3 Technique Improvement.....	9
<b>5. Research Findings from TURBINE.....</b>	<b>10</b>
5.1 Security and Privacy Requirements Formulation .....	10
5.2 Reference Architecture for Template Protection .....	12
5.2.1 PIR Approach.....	12
5.2.2 PIV Approach.....	13
5.3 Supportive Research Work for the Proposed Requirements and the Reference Architecture .....	13
<b>6. Conclusions .....</b>	<b>18</b>
<b>7. Bibliography .....</b>	<b>19</b>
<b>8. Annexes – Publication List from TURBINE Researches.....</b>	<b>21</b>

## Glossary

---

<b><u>Abbreviation / acronym</u></b>	<b><u>Description</u></b>
GUC	Gjøvik University College
PBAB	Precise Biometrics AB
PRE	Philips Research Europe
SAG	Sagem Sécurité
UTW	University of Twente
MTE	Minutiae template encoder
MTC	Minutiae template comparator
PIE	Pseudo identity encoder
PIC	Pseudo identity comparator
PIV	Pseudo identity verifier
PIR	Pseudo identity recoder
ISO	International organisation for standardisation
IEC	International electro-technical commission
ANSI	American national standards institute

# 1. Executive Summary

---

This document presents the overview of standards relevant to the project TURBINE, the purpose and targets of standardisation work in TURBINE, and the corresponding research findings contributed by the project partners involved in WP2.3 *Protected biometrics with appropriate fingerprint data* required for the secure protection and assured privacy of fingerprint features. The document is the deliverable D2.3.3: *Researching Findings for Standardisation* which is due in M24. Another deliverable D5.4.2 *TURBINE Standardisation* concerning specific standardisation work done and milestones achieved during the ISO/IEC JTC1 SC27 meetings (2008-2009) is due in M24 as well as action results of this deliverable D2.3.3. One of objectives in WP2.3 is to study and research a Pseudo Identity template protection system, which shall generate research findings for standardisation.

Some research findings have been described in existing TURBINE project deliverables:

- Template protection requirements and the reference architecture for pseudo identities described in D1.1.1 *Requirements for privacy protection and trusted identity verification*;
- Fingerprint data transformation, fixed-length feature extraction and binarisation to address the interoperability and template format requirements, described in D2.2.1 *Noise-robust minutiae (feature) sets, fingerprint image attributes and SW modules*.

Besides, other research findings to support the template requirements and the reference architecture are described in the Section 6.3 –

- Error Correction coding
- Security Analysis over Helper Data systems
- Innovation Based on IBM scheme – Privacy Enhancement against Traceability
- Efficient Comparison-on-Card Biometric Identification Respecting Privacy

The research findings presented in this document constitute the reservoir for the standardisation work as reflected in D5.4.2 *TURBINE Standardisation*.

## 2. Introduction

---

### 2.1 Project scope

The TURBINE project proposes a multi-disciplinary privacy enhancing authentication technology. Based on innovative developments in cryptography and fingerprint biometrics, it aims to resolve the current privacy concerns regarding the use of fingerprint biometrics for ID management.

To achieve this it will develop and evaluate the foundation and application of revocable protected biometric templates and pseudo-identity bit-strings using fingerprint data. It will provide:

- Cryptographic techniques applied to fingerprint biometrics to obtain a non-invertible and protected;
- Pseudo-identity bit-string for enrolment and subsequent verification;
- Multiple re-generation of independent unique bit-strings based on the same fingerprint;
- Revocable and multiple pseudo-identity management scheme based on these unique bit-strings;
- Highly reliable biometric fingerprint 1:1 secure verifications using these unique bit-strings;
- Detailed verification performance analysis, evaluated on very large public and private fingerprint databases;
- Comprehensive risk analysis and system security;
- Contribution to developing international standards for biometric template protection.

Its primary objective is to develop and then demonstrate that the technology and its performance in practice is sufficiently mature for deployment as a solution to large scale eID requirements. Expert groups will advise the consortium on i) data protection, privacy issues and ii) requirements of key application sectors for eID management solutions. Furthermore, a comprehensive verification test, demonstrator environment will evaluate how single fingerprint data of an individual may be used to generate several secure unique pseudo-identity bit-strings with different levels of trust. It will include revocation and issuance of an equivalent re-generated biometric identity based on the same specific fingerprint data without weakening the overall security.

### 2.2 Background and objectives

This document, created in the context of the TURBINE project, gathers the research findings resulted from WP1.1 *Requirements for privacy protection and trusted identity verification*, WP2.2 *Fusion with other finger attributes*, and WP2.3 *Protected biometrics with appropriate minutiae* to constitute a technical reservoir for possible output into relevant international standards. This standardisation work is aiming at the following targets:

#### Visibility of TURBINE and European Research Efforts on Biometric Template Protection

One of targets of the standardisation work in TRUBINE is to increase the visibility of European researches on biometric template protection by outputting TURBINE partners' innovative research work to the current international standards. Playing leading roles of research and technology innovation in Europe, the TURBINE partners (Sagem Security, Philips Research, Precise Biometrics, University of Leuven and Gjøvik University College) have been doing great competitive research work in this field in the past years which are familiar to peer researchers. And the standardisation work will further make the achievements visible to the global academic side, industries and potential customers.

#### Leading Technology Trend on Biometric Template Protection

To lead the technology trend in biometric template protection in the global scope is another target of the standardisation work in TRUBINE. By involvement in the international standardisation work,

TURBINE partners can feed innovative research results into the standards and lead the technology trend throughout the global industries. For those technology-neutral standards, by involving in the standardisation work TURBINE can influence the global technological developing directions in the field of biometric template protection and help shape a technology-compatible framework for the European partners' future technology development.

### Achieving Interoperability for Biometric Template Protection Solutions in International Standards

Emphasising industrial interoperability, the TURBINE project is targeting at fingerprint template protection solutions compatible with the existing fingerprint data format standards based on minutiae features. In the meanwhile, the TURBINE project is also targeting at technology solutions achieving interoperability with other existing / developing international biometric standards, identity management standards and information security standards. By involvement in standardisation work, above interoperability target can be better met.

The objective of this document is to provide an overview of existing international standards relevant to biometrics and template protection, the possible contributions from TRUBINE to the international standards, and the research findings resulted from TURBINE that are suitable for standardisation work.

## 2.3 Organization

This document is organised as follows: Section 3 provides an overview of current international standards relevant to biometrics and the specific standard project ISO/IEC JTC1 SC27 24725 on biometric template protection. Section 4 provides the possible contributions from TURBINE that can be output into the standard project ISO/IEC JTC1 SC27 24725. Section 5 presents the research findings resulted from TURBINE WP1.1 that are suitable for standardisation and the research findings from WP2.2 and WP2.4 as supportive technical materials for the standardisation work.

## 3. Standards Overview

---

### 3.1 Standards on Biometrics

Per TURBINE project's objective to provide security and privacy enhancing solutions for biometric authentication systems, we investigate the relevant international standards and give an overview of existing standards and ongoing standardisation work in this section.

Standards on biometrics are mainly set up to define requirements, and achieve interoperability in data formats and procedures among biometric systems. There are formal and informal standards organisations. The formal ones are usually formed by national bodies and international recognised bodies, such as the *International Organisation for Standardisation (ISO)*, the *International Electro-Technical Commission (IEC)*, the *International Communications Union (ITU)*; or formed by some government sponsored national standards bodies such as the *American National Standards Institute (ANSI)*. The informal ones, i.e., the de facto standards organisations, are usually formed by industrial consortium such as the *BioAPI Consortium*.

#### 3.1.1 ISO and ISO/IEC standards

The current ISO standards on biometrics were originated from the technical committee TC68 on Banking and Financial Services, in which the subcommittee SC2 on Security Management and General Banking Operations, including biometrics, Public Key Infrastructure (PKI), and security guidelines. Since early 1980's, joint Technical Committee One (JTC1) have been formed between ISO and IEC. Three subcommittees SC17 (Cards & Personal Identification), SC27 (IT Security Techniques) and SC37 (Biometrics, formed in 2002) are relevant to biometrics. SC37 is dedicated to biometric technologies including data formats, APIs, application profiles and testing; SC17 comprises the scope of biometrics for cards and personal identification; and the SC27 comprises the scope of biometric security and evaluation methodologies. So far some existing and developing standards include:

- ISO TC68 SC2 - 19092 (transposed from ANSI X9.84): Biometrics (2008)
- ISO/IEC JTC1 SC17 - 7816: Identification cards -Integrated circuit cards – Part 11: Personal verification through biometric methods (2004)
- ISO/IEC JTC1 SC17 - 24787: Information technology - Identification cards - On-card biometric comparison. (FCD 2009)
- ISO/IEC JTC1 SC17 - 18013: Information technology - Personal identification - ISO-compliant driving license - Part 2: Machine-readable technologies (2008)
- ISO/IEC JTC1 SC27 - 19792: Information technology - Security techniques - Security evaluation of biometrics (2010)
- ISO/IEC JTC1 SC27 - 24761: Information technology - Security techniques - Authentication context for biometrics (2009)
- ISO/IEC JTC1 SC27 - 24745: Information technology - Security techniques - Biometric template protection (2ndCD 2010)
- All ISO/IEC JTC1 SC37 standards, such as
  - ISO/IEC JTC1 SC37 - 19784: Information technology - Biometric application programming interface (Part1 (2006), Part2(2007))
  - ISO/IEC JTC1 SC37 - 19785: Information technology - Common Biometric Exchange Formats Framework (Part1,2 (2006), Part3(2007), Part4(FCD 2009))
  - ISO/IEC JTC1 SC37 - 19794: Information technology - Biometric data interchange formats (still under active development).
  - ISO/IEC JTC1 SC37 - 24714: Information technology - Biometrics - Jurisdictional and societal considerations for commercial applications (Part1 (2008), Part2(2007))

### 3.1.2 Other Standards

Other standards include:

- ANSI serial such as
  - ANSI X9.84-2003, "Biometric Information Management and Security for the Financial Services Industry", June 2003
  - ANSI/NIST-ITL 1-2000, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information", July 2000
- INCITS serial such as
  - ANSI/INCITS 398-2005, "Common Biometric Exchange Formats Framework (CBEFF)", February 7, 2005
  - ANSI/INCITS 358-2002, "The BioAPI Specification", February 13, 2002
- ICAO – Doc9303 (Part1 (2006), Part2 (2005), Part3 (2008))

### 3.2 Targeted Standard - ISO/IEC JTC1 WG5 SC27 24745 (Biometric Template Protection)

An open standard for biometric template protection is currently being taken by ISO JTC1 subcommittee 27 (SC27) workgroup 5 - *ISO/IEC JTC1 24745 on Biometric Template Protection*. This workgroup deals with identity management and privacy technologies in the area of IT security techniques and is developing a standard for cryptographic guidance to protect biometric data. This project of ISO/IEC standardisation dedicated to the topic of biometric template protection was created in the Vienna meeting held in May 2005 and Mr. Hee-Un Park was appointed as the Editor. Since then, he produced two Working Drafts: 1st WD (SC 27 N4545) and 2nd WD (SC 27 N4832). In May 2006, Mr. M.G. Chun and Mr. P.J. Lee were appointed as new Co-editors in October 2006. The 3rd WD was produced in April 2008, 4<sup>th</sup> WD in January 2009 and CD1 in June 2009. This document aims at describing the potential threats and requirements with respect to data confidentiality, integrity, availability and renewability of biometric references during storage and transmission. Furthermore, the binding between biometric data and other personally identifiable information (such as identity data, contact information, account numbers, and alike) is described and the associated privacy requirements are formulated. In accord with the project TURBINE's aim, this standards is a good option to take in TURBINE's research output and thus become the target of TURBINE's standardisation work.

## 4. Potential Contributions to Standards

---

### 4.1 Security and Privacy Requirements on Biometric Template Protection

In general, data security concerns confidentiality, integrity and availability. However, besides these security requirements for general data, biometric templates concerns additional requirements in security and privacy aspects. The TURBINE project is targeting at mechanism to emphasize the following security and privacy requirements:

- Protected templates
  - Irreversibility: impossible to retrieve or decode original biometric sample from protected template;
  - Unlinkability: Impossible to link protected templates across databases or applications.
  - Contains identification data for a specific, pre-defined purpose only.
- Renewable, revocable, and diversifiable protected templates  
Protected templates should be renewable and revocable.
- Universal approach  
Template protection should be applicable to any biometric characteristic and preferably allows fusion between different biometric modalities.
- Interoperability  
Allows integration of technology from various vendors.
- Data minimization  
Protected templates should be stored efficiently, with a minimum of information required for reliable verification.
- Architecture flexibility  
Both on-line verification and off-line verification should be supported.

and other optional requirements for specific applications scenarios such as:

- *Binary form* of the protected biometric templates for efficient comparison;
- *Fixed length* of the protected biometric templates for efficient comparison and storage management;

Till the 3<sup>rd</sup> WD of ISO/IEC JTC1 SC27 24745, the security requirements of biometric template protection were limited in data protection level and the privacy requirements are concerning only about the operator and operation level. Formalization of the above requirements and related concepts can be TURBINE's standardisation work in the ISO/IEC JTC1 SC27 24745 project on biometric template protection.

### 4.2 A General Framework for Template Protection Equipped with "Renewability"

In recent years many schemes for biometric data protection have been published in the literature. These proposals are often termed "biometric template protection" or "biometric encryption" schemes and typically address one or more of the privacy and security requirements described in the previous section. From a high-level point of view there are many similarities in the structure of these proposals, which are often difficult to recognize because most of them employ their own terminology. Therefore there is a need to describe template protection schemes using a harmonized terminology and structure. Such "standardized" structure would also help in translating the privacy and security requirements into technical properties of the various involved processes and data elements, and allow verification of the extent to which the various requirements are met. Such a general framework for biometric template protection emphasizing the requirements listed in Section 4.1 is needed for the current ISO/IEC JTC1 SC27 24745 project. On one hand, the

proposed general framework should reflect the renewability requirement of the protected templates and the concepts of pseudo identity generated from the TURBINE project; on the other hand, the proposed general framework should be compatible as much as possible with existing biometric standards such as the ISO/IEC JTC1 SC37 - 19794: Information technology - Biometric data interchange formats, and also be compatible with existing / developing biometric template protection techniques, including both renewability-equipped mechanisms (such as biometric encryption and fuzzy vault) and traditional cryptography-based data protection mechanisms, as reflected in the old ISO/IEC JTC1 SC27 24745 document 3rdWD. In the meanwhile, compatibility with identity management requirements, such as the developing standards project ISO/IEC JTC1 SC27 24760, is necessary as well.

To achieve the above goals, the components and their relationships in the framework need to be defined to accommodate the “renewability” requirement and to map all existing and emergent biometric template protection mechanism to the proposed framework in a harmonized way.

### 4.3 Technique Improvement

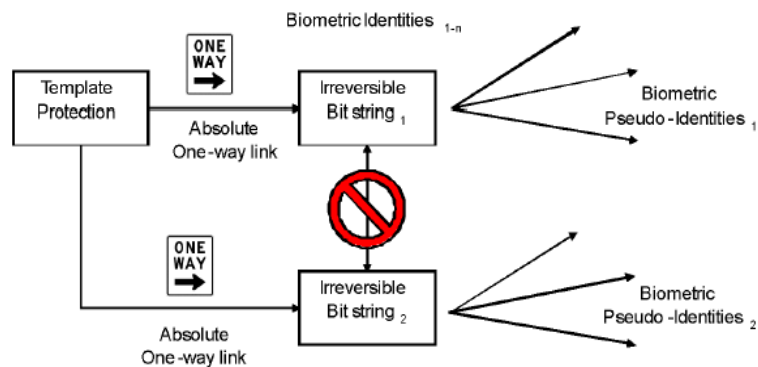
Besides the security and privacy requirements formulated in Section 4.1 and a compatible general framework planned in the Section 4.2, technique innovations need to be done to fulfil the requirements and support the proposed general framework. Particularly, to improve the biometric performance and security of the protected templates to meet the TURBINE’s biometric performance target is a key task to support the standardisation work for the proposed requirements and in the Section 4.1 and the general framework planned in the Section 4.2.

## 5. Research Findings from TURBINE

In this chapter research findings from the TURBINE project that are potentially promising for standardisation are gathered. Publications of corresponding research work from TURBINE are listed as Annex I.

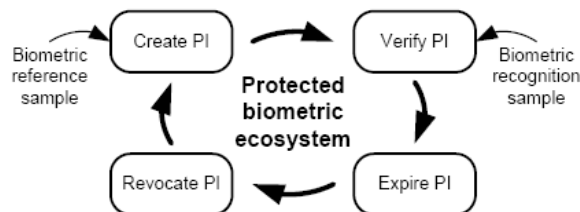
### 5.1 Security and Privacy Requirements Formulation

To describe the security requirement of renewability / revocability and the privacy requirements of irreversibility and unlinkability, the concept of “Pseudo Identities” and “Auxiliary Data” was proposed in TURBINE [1] for the protected templates in a diversified and protected form. The individual generates for each application a unique biometric identifier - the “pseudo identity”, such that in each application the client is associated with a different pseudo-identity. The client verifies his pseudo-identity prior to each transaction or consumption of the offered service. Figure 1 demonstrates the basic concept of “pseudo identities”.



**Figure 1 - Pseudo identities derived from biometric characteristics.**

Pseudo identities can be defined [2] as diversifiable, protected identity verification strings within a predefined context (i.e., the protected biometric ecosystem). A pseudo identity (PI) does not reveal any information that allows retrieval of the original biometric measurement data, biometric template or true identity of its owner by any other person than the enrolled subject. Within a protected biometric ecosystem, pseudo identities follow 4 distinct phases that are visualized in Figure 2.



**Figure 2 - Pseudo identity lifecycle in a protected biometric ecosystem.**

1. Creation (or renewal) of PIs from biometric reference data during an enrollment phase;
2. Verification of a PI based on a recognition sample;
3. Expiration of the validity of a PI;
4. Revocation of a PI if its validity is expired.

Besides PI, auxiliary data (AD) is defined [2] to serve the following purposes, depending on the employed method and algorithms:

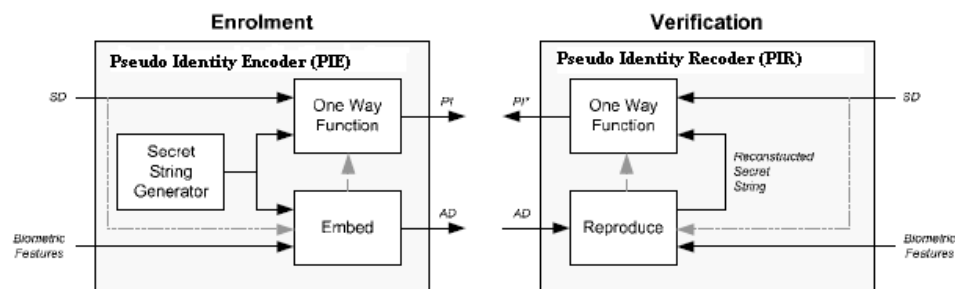
- It allows generation of multiple independent pseudo identities for the same individual within an application to provide renewable templates;
- it allows generation of independent pseudo identities across applications to prevent database cross-matching and linking;
- it allows generation of independent pseudo identities for subjects that have very similar biometric characteristics to prevent impersonation through spotting of biometric look-a-likes;
- it provides means for template data separation to enhance security and privacy; and
- it allows individualized comparison parameters to optimize the verification performance.

To illustrate the compatibility of the proposed concepts PI and AD with existing biometric template protection methods, Table 1 presents an overview of methods mapped to the concepts of PI and AD.

**Table 1 – Overview of methods to generate PI and AD**

<u>Method</u>	<u>Reference</u>	<u>Pseudo Identity (PI)</u>	<u>Auxiliary Data (AD)</u>
Helper data systems	[3]	Hash of a secret string	Helper data
Fuzzy commitment	[4]	Hash of secret string	Offset
Biometric encryption	[5]	Cryptographic key	Filter and key link
Fuzzy vault	[6]	Hash of secret string	Point set P
Shielding functions	[7]	Hash of secret string	Authentication challenge W
Fuzzy extractors	[8]	Hash of secret string	Public string P
Extended PIR	[9]	Encrypted template	n/a
2D hexagonal quantization index modulation	[10]	Hash of a secret string	Quantization errors
Cancellable biometrics	[11]	Transformed template	Transform parameters

With the proposed concepts PI and AD, a high-level implementation to generate and verify the protected template (PI and AD) can be structured as in Figure 3, where the Supplementary Data (SD) is defined to randomize biometric features as part of the embed stage for example using a password). Alternatively, if the randomization string is assumed to be public and subject dependent, this string can be part of AD.



**Figure 3 - Pseudo identity lifecycle in a protected biometric ecosystem.**

The Embed and One-Way Functions are subject to various major requirements to safeguard security and privacy. These major requirements include:

- **Renewability** – represented by sufficient entropy in the generated secret strings. This requirement is needed to (1) allow a sufficient number of diversifications of protected templates for a single person, and (2) to prevent reconstruction of the secret string from PI.

- **Irreversibility** – represented by low cross-entropy between the unprotected biometric features and the protected template, to prevent information leakage about biometric characteristics from AD.
- **Unlinkability** – represented by low cross-entropy among protected templates generated using different secret strings using equal biometric features, required to prevent cross-matching of databases and services.

More requirements of the protected templates can be found in the TURBINE publication [12].

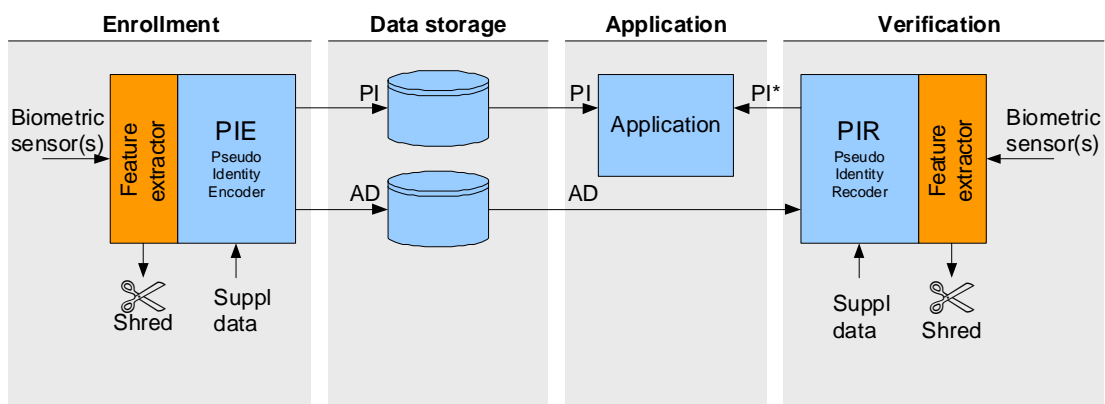
## 5.2 Reference Architecture for Template Protection

The interoperability is the key point to emphasize in TURBINE’s standardisation work. To be compatible with all the existing biometric template protection mechanisms and possible emergent mechanisms, a reference architecture for template protection is proposed in TURBINE to gain the interoperability among different technique providers. Components are designed within this reference architecture to meet the defined security and privacy requirements.

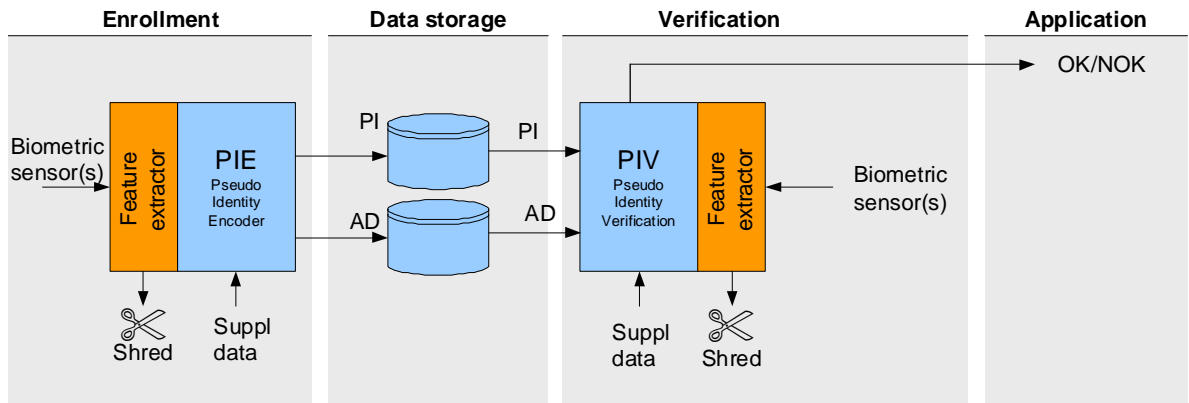
Two reference architectures are considered for the TURBINE system, i.e. the Pseudo Identity Recoder (PIR) and Pseudo Identity Verification (PIV) approach. Throughout this section we use the term features. The biometric data could be minutiae based fingerprint features, as well as (combined with) image/shape based features, which are provided by the software developed in WP2.1 and WP2.2, respectively. Refer to [2] for an elaborate description concerning the reference architectures developed within TURBINE. Software modules [13] for generation of protected biometrics have been delivered in M18. Refer to [14] for further details on usage and installation of these software modules. Also a common software API is provided in this document, both for PIR and PIV architectures.

### 5.2.1 PIR Approach

At the enrolment phase first a set of features is extracted from biometric sample(s) captured by a fingerprint sensor. If necessary the extracted features are transformed into an ordered, fixed length feature vector. The Pseudo Identity Encoder (PIE) module derives a Pseudo Identity (PI) and possibly Auxiliary Data (AD) from the transformed feature set. During the verification phase a biometric sample is captured by a fingerprint sensor. The Pseudo Identity Recoding (PIR) first transforms the extracted feature set into a fixed length and ordered vector representation. Subsequently the PIR module regenerates/recodes a pseudo identity  $PI^*$  using AD from the claimed identity which was derived during enrolment. The Pseudo Identity Comparator (PIC) module compares the recoded pseudo identity  $PI^*$  against the pseudo identity PI derived during enrolment. A person is authenticated if PI and  $PI^*$  are equal.



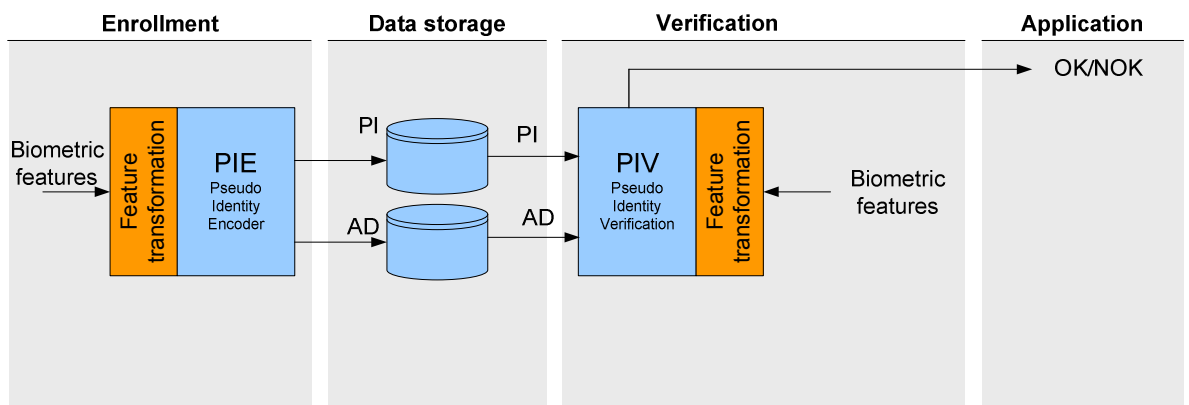
**Figure 4 - Overview of the architecture of the PIR approach for biometric template protection.**



**Figure 5 - Overview of the reference architecture of the PIV approach for biometric template protection.**

## 5.2.2 PIV Approach

The PIE module in the PIV approach is equal to the PIE from the PIR approach. In the PIV approach no PI\* is recreated at the verification phase. After a verification sample is measured and transformed into an ordered, fixed length feature vector, the PI derived during enrolment is directly verified. This solution requires integration of the PIV module and protected template on the same device, for example in a Match-On-Card system.



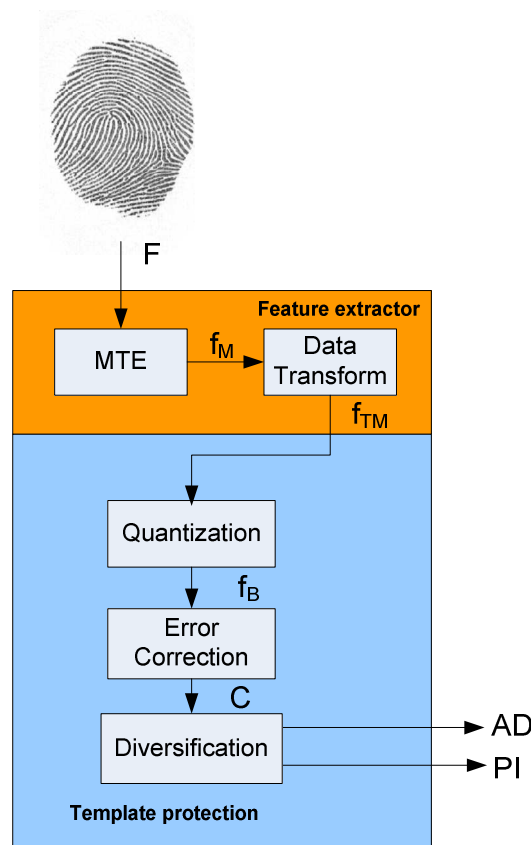
**Figure 6: TURBINE reference architecture PIV approach**

More details of the specification of this reference architecture can be found in the TURBINE publication [2] and [12].

## 5.3 Supportive Research Work for the Proposed Requirements and the Reference Architecture

### Introduction

To generate a protected template from a fingerprint image, the two-stage approach as described in paragraph 5.2.1 and [13] has been developed in WP2.3 for protection of the biometric fingerprint. Figure portrays this concept, see also [14].



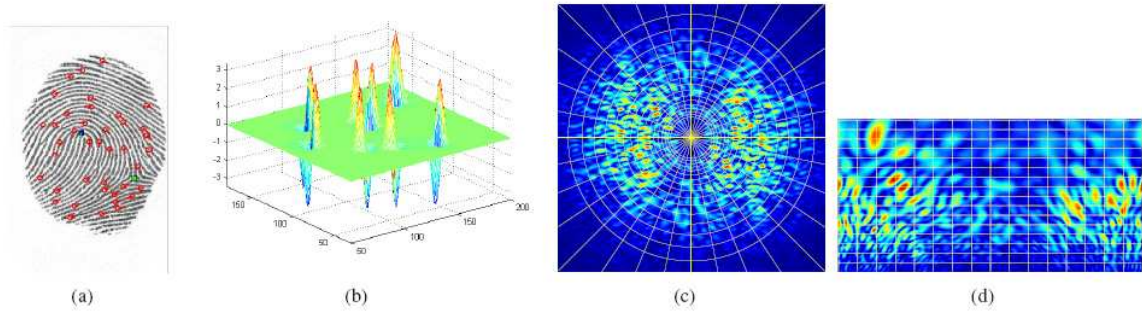
**Figure 7: Protection of fingerprint biometric**

In more detail, from a fingerprint image  $F$ , captured by a fingerprint sensor and minutiae are being extracted by module MTE (Minutiae Template Encoder), giving a template  $f_M$ . A minutiae set that has been derived from a fingerprint is an unordered collection of minutiae locations and orientations which also varies in size. Conventional minutiae data cannot be used as input of the quantization module present in the template protection stage two. This module requires an ordered and fixed length real valued feature vector. Transforming conventional minutiae templates into ordered and fixed length feature vectors enables combining a fingerprint verification system with template protection. The transformation of minutiae is accomplished in the module Data Transformation which produces a vector  $f_{TM}$ .

The second stage involves quantization, error correction and diversification to generate a protected template from the transformed minutiae vector to satisfy the security and privacy requirements mentioned in paragraph 4.1.

### Minutiae Data Transform – Spectral Minutiae Representations

The objective of the spectral minutiae representation is to represent a minutiae set as a fixed-length feature vector, which is invariant to translation, rotation and scaling [26] [27]. In Figure 8, a general procedure of the spectral minutiae representation is illustrated. Step 1: we represent minutiae points as real (or complex) valued continuous functions, illustrated in Figure 8(b). In this representation, translation, rotation and scaling may exist, depending on the fingerprint sensors that have been used and how the user has put his finger on the sensor. Step 2: a two-dimensional continuous Fourier transform is performed and only the Fourier magnitude is kept, illustrated in Figure 8(c). This representation is now translation invariant according to the shift property of the continuous Fourier transform. Step 3: the Fourier spectrum is re-mapped onto a polar-logarithmic coordinate system, illustrated in Figure 8(d). According to the scale and rotation properties of the



**Figure 8: Illustration of the general spectral minutiae representation procedure (images from the SMO case).**

**(a) a fingerprint and its minutiae; (b) representation of minutiae points as real (or complex) valued continuous functions; (c) the 2D Fourier spectrum of 'b' in a Cartesian coordinate and a polar-logarithmic sampling grid; (d) the Fourier spectrum sampled on a polar-logarithmic grid.**

two-dimensional continuous Fourier transform, the rotation and scaling become translations along the new coordinate axes. It should be noted that this representation can be computed analytically.

There are three types of spectral minutiae representations: SML, SMO and SMC. For a fingerprint with  $Z$  minutiae points, with  $(x, y, \theta)$  the coordinates and orientation,  $w$  is the weight that is decided by the minutiae quality, the SML, SMO and SMC representations are:

*Location-based Spectral Minutiae Representations (SML)*

$$|M_L(\omega_x, \omega_y; \sigma_L^2)| = \left| \exp\left(-\frac{\omega_x^2 + \omega_y^2}{2\sigma_L^2}\right) \sum_{i=1}^Z w_i \exp(-j(\omega_x x_i + \omega_y y_i)) \right|$$

*Orientation-based Spectral Minutiae Representations (SMO)*

$$|M_O(\omega_x, \omega_y; \sigma_O^2)| = \left| \exp\left(-\frac{\omega_x^2 + \omega_y^2}{2\sigma_O^2}\right) \sum_{i=1}^Z j(\omega_x \cos \theta_i + \omega_y \sin \theta_i) \cdot w_i \exp(-j(\omega_x x_i + \omega_y y_i)) \right|$$

*Complex Spectral Minutiae Representations (SMC)*

$$|M_C(\omega_x, \omega_y; \sigma_C^2)| = \left| \exp\left(-\frac{\omega_x^2 + \omega_y^2}{2\sigma_C^2}\right) \sum_{i=1}^Z w_i \exp(-j(\omega_x x_i + \omega_y y_i) + j\theta_i) \right|$$

## Template format

In order to obtain the final spectral representations, the continuous spectra SML, SMO and SMC need to be sampled on a polar-logarithmic (or polar-linear) grid. A polar mapping transforms rotation to translation in the horizontal direction, while a logarithmic mapping transforms scaling to translation in the vertical direction. We sample SML and SMO in a polar-logarithmic grid, while we sample SMC in a polar-linear grid, which can provide more samples in the higher frequency part. In the radial direction  $\lambda$ , we use  $M=128$  samples between  $\lambda_l$  and  $\lambda_h$ . In the angular direction  $\beta$ , we use  $N=256$  samples uniformly distributed between  $\beta=0$  and  $\beta=\pi$  or  $2\pi$  (because of the symmetry of the Fourier transform for real-valued functions, using the interval between 0 and  $\pi$  for SML and SMO is sufficient). Finally, the sampled spectra contain 32,768 floating point values.

## Error Correction coding

A spectral minutiae feature vector, produced from a minutiae set by applying the spectral minutiae algorithm described in paragraph has a very high dimensionality. A single spectral feature vector contains 32,768 floating point values. Therefore the degree of correlation present in a spectral

minutiae vector might be very high. In order to derive a robust bit vector from a spectral minutiae vector, as a first step, dimension reduction techniques developed in task T2.3.2 “Quantization, noise and footprint reduction” are applied on the spectral feature vectors provided at the input of the PIE and PIR modules. The applied dimension reduction technique, which involves training on a separate data set, aims to minimize the degree of correlation present in a full size feature vector and to maximize the discrimination of individuals.

Some feature quantization processes require statistics derived from offline training and provided enrolment data; other procedures may not use such statistics. Refer to [15] and [16] for possible quantization methods for generating binary strings. The binary vectors derived during enrolment and verification are most likely not equal due to noise, therefore Error Correcting Codes (ECC) is being applied to correct the corrupted bits [17]. The diversification module enables creation of multiple, independent biometric references from one feature set [17]. The output of the diversification module is a protected template, which consist of a PI and AD.

### Security analysis over Helper Data systems

In this section we give an overview of the definitions of security and privacy attributes for helper data systems that are known currently in the literature. These attributes that are briefly described in Table 2, can be divided in three classes. Attributes in the first class measure security and privacy in terms of information theoretical quantities, for instance key randomness, weak biometric privacy, strong biometric privacy and reusability. Attributes in the second class describe properties of the functions used during enrollment and authentication, for instance irreversibility and indistinguishability. Attributes in the third class might have effect on the security and privacy of the biometric data; however they depend mostly on the implementation of the anonymous biometric authentication system. This class includes transaction anonymity and identity privacy.

**Table 2 - Short overview of biometric privacy related attributes in the literature.**

Identity Privacy	Relationship between a username ID and the corresponding pseudo identity should be protected;	[22]
Key Randomness	Quantifies the randomness of the secret key to an attacker who has the protected template;	[18],[20]
Weak Biometric Privacy	Quantifies the amount of information revealed about the unprotected biometric identifier by the protected template;	[18]
Strong Biometric Privacy	Quantifies the amount of information revealed about the unprotected biometric identifier by the protected template and the secret key;	[18]
Reusability	Quantifies the amount of information revealed about the unprotected biometric by multiple related protected templates (generated from one biometric identity using different keys)	[19]
Irreversibility	Quantifies the amount of information revealed about the unprotected biometric by multiple related protected templates generated using different protection techniques;	[21]
n-Indistinguishability	Quantifies the amount of information, which exists between related protected templates used for different services, applications;	[21]
Transaction Anonymity	Transactions statistics for a particular user should be protected;	[22]

In [23] an evaluation is given concerning the achieved security and privacy when using the Quantization Index Modulation (QIM) scheme to generate protected biometric references.

### Innovation based on IBM scheme – Privacy Enhancement against Traceability

In the IBM scheme [11], the non-invertible transformation parameters need to be well kept in secret in order to achieve high irreversibility analyzed in the publication [11]. To better keeping these parameters, a security enhanced solution for enrolment and identification is proposed as follows -

one parameter  $g_t$  (distortion function) can be split into two parts ( $g_t = g_{t,in} \circ g_{t,out}$ ) and stored in the memory of the Client (sensor) with  $(h_{t,ID}^{-1} \circ g_{t,in} \circ f)$  and Server with  $(g_{t,out} \circ h_{t,ID})$  respectively. In this way, the compromise of a Client (sensor) will not disclose the full distortion function  $g_t$  which is also used during comparison (comparing  $g_{t,out}(b')$  with  $g_{t,out}(DB)$ ). Note that  $f$  is the non-invertible transformation in [11], and  $h_{t,ID}$  is a time and sensor-ID dependent bijective function, making the whole biometric data transformation secure against replay attack in timeline and across sensors. Privacy can be enhanced in this scheme in the sense that only binary comparison result is sent from the database  $DB$  to the Server, which makes the Server not able to get the information who is identified in the database; in addition, the distortion function  $g_t$  is time-dependent, which makes the attacker who has access to the Server has no information whether the same user have accessed the sensor many times. This is called untraceability. More details can be found in the TURBINE publication [24].

### Efficient Comparison-on-Card Biometric Identification Respecting Privacy

Comparison-on-Card applications using Secure Access Module (SAM) provide secure storage functionalities against eavesdropping but need computationally efficient biometric template comparison schemes for implementation. The efficiency of comparison-on-card process can thus be improved by reducing the searching scope to a limited subset of biometric templates and doing the unprotected biometric templates comparison inside the SAM over the subset. The searching scope reduction is done by finding the subset out of those quantized reference features stored inside the SAM which are similar to the quantized probe biometric features. Then the encrypted templates stored outside the SAM corresponding to the subset quantized features are sent to the SAM for comparison after decryption inside the SAM. As the biometric information of the enrolled users remain either in the SAM, or encrypted outside the SAM and decrypted only in the SAM, the scheme ensures the privacy of the registered users. More details can be found in the TURBINE publication [25].

## 6. Conclusions

---

This deliverable aims at pooling research findings promising for standardisation work from the TURBINE project. The main resources are TURBINE research tasks in WP1.1 *Requirements for privacy protection and trusted identity verification*, WP2.2 *Fusion with other finger attributes*, and WP2.3 *Protected biometrics with appropriate minutiae*.

Standardisation of TURBINE research results will increase the technological impact and visibility of TURBINE representing European biometric researches in both academic and industrial fields, help the TURBINE partners lead the technology trend in biometric identity security fields, and achieve interoperability of biometric template protection techniques with existing biometric technologies and standards.

Overview is given over existing and developing international standards on biometric identity security on their history and scopes. The standardisation work project ISO/IEC JTC1 SC27 – 24745 is targeted for our TURBINE project standardisation work. Potential contributions from TURBINE to this ISO standard consist of renewability/ revocability concept, security and privacy requirements, pseudo identity based reference architecture for template protection, and other corresponding supportive technologies.

Research findings associated with above potential contributions are gathered for standardisation work. Publications from TURBINE are listed in the Annex I of this document.

## 7. Bibliography

---

- [1] N. Delvaux, H. Chabanne, J. Bringer, B. Kindarji, P. Lindeberg, J. Mdgren, J. Breebaart, T. Akkermans, M. van der Veen, R. Vedhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, and D. Skepastianos. "Pseudo identities based on fingerprint characteristics," *Proceedings of the IEEE IHH-MSP 2008*, Harbin, China, pp. 1063-1068, 2008.
- [2] J. Breebaart, C. Busch, J. Grave, E. Kindt. "A reference architecture for biometric template protection based on pseudo identities," *Gesellschaft für Informatik (GI): BIOSIG 2008. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*. Editor: Brömme, A. Bonn: Gesellschaft für Informatik, pp 25-37, 2008.
- [3] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaer, G. J. Schrijen, A. M. Bazen, R. N. J. Veldhuis. "Practical biometric authentication with template protection," *Audio and Video-based biometric person authentication*, pp. 436-449, Springer, Berlin, Germany, 2005.
- [4] A. Juels, M. Wattenberg. "A fuzzy commitment scheme," *ACM Conference on Computer and Communications Security*, pp. 28–36, 1999.
- [5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. K. Vijaya Kumar. "Biometric encryption using image processing," *Proc. SPIE 3314*, pp. 178–188, 1998.
- [6] A. Juels, M. Wattenberg. "A fuzzy vault scheme," *Proc. IEEE Int. Symposium on Information Theory*, 2002.
- [7] J-P. M. G. Linnartz, P. Tuyls. "New shielding functions to enhance privacy and prevent misuse of biometric templates," *AVBPA*, pp. 393–402, 2003.
- [8] Y. Dodis, L. Reyzin, A. Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *Eurocrypt*, 2004.
- [9] J. Bringer, H. Chabanne, D. Pointcheval, Q. Tang. "Extended private information retrieval and its application in biometrics authentications," *CANS*, 2007.
- [10] I. Buhan, J. Doumen, P. Hartel, R. N. J. Veldhuis. "Embedding renewable cryptographic keys into continuous noisy data," *Information and communications security, 10th international conference ICICS*, Birmingham, UK, pp.294-310, 2008.
- [11] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. "Generating cancellable fingerprint templates," *IEEE trans. pattern analysis and machine intelligence*, vol.29, no.4, pp. 561-572, 2007.
- [12] J. Breebaart, B. Yang, I. Buhan-Dulman, C. Busch, "Biometric template protection: The need for open standards," *Datenschutz und Datensicherheit - DuD*, vol. 33, no. 5., pp. 299-304., May 2009.
- [13] TURBINE deliverable D1.1.1. Technical Requirements, 2008.
- [14] TURBINE deliverable D2.3.1. TURBINE SW modules for Protected Biometric, 2009.
- [15] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaer, A.H.M. Akkermans. "Biometric binary string generation with detection rate optimized bit allocation," *Computer Vision and Pattern Recognition Workshops, 2008*, pp 1-7, 2008.
- [16] E.J.C. Kelkboom, and Groot, K.T.J. de and Chen, C. and Breebaart, J. and Veldhuis, R.N.J. Pitfall of the Detection Rate Optimized Bit Allocation within template protection and a remedy. In: *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems*, 2009. BTAS '09. pp. 1-8, 2009.
- [17] E.J.C. Kelkboom, B. Gökberk, T.A.M Kevenaer, A.H.M Akkermans, M. van der Veen, "3D Face": Biometric Template Protection for 3D Face Recognition, *Lecture Notes in Computer Science, Volume 4642/2009*, pp. 566-573, 2007.
- [18] L. Ballard, S. Kamara, F. Monrose, and M. Reiter. "The practical subtleties and pitfalls in designing secure biometric key generators," *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, 2009.

- [19] X. Boyen. "Reusable cryptographic fuzzy extractors," *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS 2004)*, Washinton DC, USA, pp. 82–91, ACM, October 2004.
- [20] Q. Li, Y. Sutcu, N. Memon. "Secure sketch for biometric templates," *ASIACRYPT 2006*, Shanghai, China, vol. 4284 of Lecture Notes in Computer Science, pp. 99–113. Springer, December 2006.
- [21] K. Simoons, P. Tuyls, B. Preneel. "Privacy weakness in biometric sketches," *IEEE Symposium on Security and Privacy*, 2009.
- [22] Q. Tang, J. Bringer, H. Chabanne, D. Pointcheval. "A formal study of the privacy concerns in biometric-based remote authentication schemes," *ISPEC 2008*, no.4991 in Lecture Notes in Computer Science, pp. 56–70, Springer-Verlag, 2008.
- [23] I. Buhan, J. Breebaart, J. Merchan Guajardo, K. T. J. de Groot, E. Kelkboom, T. Akkermans. "A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem," *Proc. 4th international workshop on data privacy management (DPM'09)*, Saint malo, France, 2009.
- [24] J. Bringer, H. Chabanne, B. Kindarji. "Anonymous identification with cancelable biometrics," *Proc. of the 6th International Symposium on Image and Signal Processing and Analysis*, Salzburg, September, 2009.
- [25] J. Bringer, H. Chabanne, T.A.M. Kevenaar, B. Kindarji. "Extending Match-On-Card to local biometric identification," *BioID MultiComm2009*, LNCS 5707, pp. 178–186, 2009.
- [26] H. Xu, R.N.J. Veldhuis, A. Bazen, T. Kevenaar, T. Akkermans and B. Gokberk, "Fingerprint verification using spectral minutiae representations," *Information Forensics and Security, IEEE Transactions on*, vol.4, no.3, pp.397-409, Sept. 2009.
- [27] H. Xu and R.N.J. Veldhuis, "Spectral minutiae representations of fingerprints enhanced by quality data," *IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS '09)*, September 2009.

## 8. Annexes – Publication List from TURBINE Researches

---

- [1] N. Delvaux, H. Chabanne, J. Bringer, B. Kindarji, P. Lindeberg, J. Mdgren, J. Breebaart, T. Akkermans, M. van der Veen, R. Vedhuis, E. Kindt, K. Simoens, C. Busch, P. Bours, D. Gafurov, B. Yang, J. Stern, C. Rust, B. Cucinelli, and D. Skepastianos. "Pseudo identities based on fingerprint characteristics," *Proceedings of the IEEE IIH-MSP 2008*, Harbin, China, pp. 1063-1068, 2008.
- [2] J. Breebaart, C. Busch, J. Grave, E. Kindt. "A reference architecture for biometric template protection based on pseudo identities," *Gesellschaft für Informatik (GI): BIOSIG 2008. Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*. Editor: Brömme, A. Bonn: Gesellschaft für Informatik, pp 25-37, 2008.
- [10] I. Buhan, J. Doumen, P. Hartel, R. N. J. Veldhuis. "Embedding renewable cryptographic keys into continuous noisy data," *Information and communications security, 10th international conference ICICS*, Birmingham, UK, pp.294-310, 2008.
- [12] J. Breebaart, B. Yang, I. Buhan-Dulman, C. Busch, "Biometric template protection: The need for open standards," *Datenschutz und Datensicherheit - DuD*, vol. 33, no. 5., pp. 299-304., May 2009.
- [13] TURBINE deliverable D1.1.1. Technical Requirements, 2008.
- [14] TURBINE deliverable D2.3.1. TURBINE SW modules for Protected Biometric, 2009.
- [15] C. Chen, R.N.J. Veldhuis, T.A.M. Kevenaar, A.H.M. Akkermans. "Biometric binary string generation with detection rate optimized bit allocation," *Computer Vision and Pattern Recognition Workshops, 2008*, pp 1-7, 2008.
- [16] E.J.C. Kelkboom, and Groot, K.T.J. de and Chen, C. and Breebaart, J. and Veldhuis, R.N.J. Pitfall of the Detection Rate Optimized Bit Allocation within template protection and a remedy. In: *IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, 2009. BTAS '09*. pp. 1-8, 2009.
- [21] K. Simoens, P. Tuyls, B. Preneel. "Privacy weakness in biometric sketches," *IEEE Symposium on Security and Privacy*, 2009.
- [22] Q. Tang, J. Bringer, H. Chabanne, D. Pointcheval. "A formal study of the privacy concerns in biometric-based remote authentication schemes," *ISPEC 2008*, no.4991 in *Lecture Notes in Computer Science*, pp. 56–70, Springer-Verlag, 2008.
- [23] I. Buhan, J. Breebaart, J. Merchan Guajardo, K. T. J. de Groot, E. Kelkboom, T. Akkermans. "A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem," *Proc. 4th international workshop on data privacy management (DPM'09)*, Saint malo, France, 2009.
- [24] J. Bringer, H. Chabanne, B. Kindarji. "Anonymous identification with cancelable biometrics," *Proc. of the 6th International Symposium on Image and Signal Processing and Analysis*, Salzburg, September, 2009.
- [25] J. Bringer, H. Chabanne, T.A.M. Kevenaar, B. Kindarji. "Extending Match-On-Card to local biometric identification," *BioID MultiComm2009*, LNCS 5707, pp. 178–186, 2009.
- [26] H. Xu, R.N.J. Veldhuis, A. Bazen, T. Kevenaar, T. Akkermans and B. Gokberk, "Fingerprint verification using spectral minutiae representations," *Information Forensics and Security, IEEE Transactions on*, vol.4, no.3, pp.397-409, Sept. 2009.
- [27] H. Xu and R.N.J. Veldhuis, "Spectral minutiae representations of fingerprints enhanced by quality data," *IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS '09)*, September 2009.

Note that the indices of above publications are same as those in the Section 7 Bibliography.