Secure and Privacy Preserving Management of Biometric Templates

Vincent Alimi, Rima Belguechi, Christophe Rosenberger

Redaktør: Patrick Bours, Norwegian Information Security Laboratory (NISlab),
Gjøvik University College

Norwegian Information Security Conference
Norsk Informasjonssikkerhetskonferanse

NISK 2010

Gjøvik University College, Gjøvik
23.–24. november 2010

Program Chair

Patrick Bours	HiG

Program Committee

Kristian Gjøsteen	NTNU	Vladimir Oleshchuk	UiA
Tor Helleseth	UiB	Anders Paulshus	Conax
Erik Hjelmås	HiG	Ragnar Soleng	UiT
Audun Jøsang	UNIK	Nils Kalstad Svendsen	HiG
Martin Gilje Jaatun	SINTEF IKT	Svein Willassen	Svein Willassen AS
Stig F. Mjølnes	NTNU	Eli Winjum	FFI
Leif Nilsen	UNIK	Andre Årnes	HiG

Norwegian Information Security Conference
Norsk Informasjonssikkerhetskonferanse

NISK 2010

Gjøvik University College, Gjøvik
23-24 November 2010

Program Chair

Patrick Bours	HiG

Program Committee

Kristian Gjøsteen	NTNU
Tor Helleseth	UiB
Erik Hjelmås	HiG
Audun Jøsang	UNIK
Martin Gilje Jaatun	SINTEF IKT
Stig F. Mjølnes	NTNU
Leif Nilsen	UNIK
Vladimir Oleshchuk	UiA
Anders Paulshus	Conax
Ragnar Soleng	UiT
Nils Kalstad Svendsen	HiG
Svein Willassen	Svein Willassen AS
Eli Winjum	FFI
Andre Årnes	HiG

ISBN 978-82-519-2705-5

Redaktør: Patrick Bours, Norwegian Information Security Laboratory (NISlab), Gjøvik University College

Tapir Akademisk Forlag har som målsetting å bidra til å utvikle gode læremidler og alle typer faglitteratur. Vi representerer et bredt fagspekter, og vi gir ut ca. 100 nye titler i året. Vi samarbeider med forfattere og fagmiljøer i hele landet, og våre viktigste produktområder er:

Læremidler for høyere utdanning
Fagbøker for profesjonsmarkedet
Vitenskapelig publisering

Forlagsredaktør for denne utgivelsen:
Lasse.Postmyr@tapirforlag.no

Tapir Akademisk Forlag
7005 TRONDHEIM
Tlf.: 73 59 32 10
Faks: 73 59 32 04
E-post: post@tapirforlag.no
www.tapirforlag.no

Preface

Welcome to NISK 2010, the third edition of the Norwegian Information Security Conference. After the initial NISK conference in Agder and its follow up in Trondheim, it will now take place in Gjøvik on the 23^{rd} and 24^{th} of November. As before the conference will take place in combination with NIK and NOKOBIT. NISK2010 is sponsored by NISnet, the resource network of Norwegian Information Security researchers funded by the Norwegian Research Council.

This year we had 27 high quality submissions from 8 different institutes. Of those one was withdrawn and one came in too late. The remaining 25 were reviewed by 2 members of the Program Committee each and from their feedback 14 papers were selected for presentation. This means that the acceptance rate of 56% is very close the the 58% from last year. All 14 papers will get a 30 minutes timeslot for presenting the ideas. Out of the 14 papers, 8 are authored or co-authored by PhD students and 1 is co-authored by master students.

We are glad to announce that Dr. Mike Bond from the Computer Laboratory at the University of Cambridge accepted the invitation as a keynote speaker. The title of his presentation is *Chip and Empiricism: Breaking EMV, with proof*. In May 2010 Mike Bond presented the controversial paper *Chip and PIN is broken*, which he co-authored with Steven J. Murdoch, Saar Drimer, and Ross Anderson, at USENIX Security. The paper described how an EMV card can be used to make purchases at Point-of-Sale without knowing the correct PIN. During the subsequent publicity, demonstrations of the technique deployed against the live banking system aired on various European television channels.

I would like to thank all the members of the Program Committee for their valuable input in the reviewing process. Furthermore I would like to thank the organizers of NIK, Erik Hjelmås and of NOKOBIT, Tom Røise for the pleasant cooperation and last but certainly not least I would like to thank Kari Lauritzen for all the help with the practical organization of the three conferences.

Table of Content

NISK 2010

Secure and Privacy Preserving Management of Biometric Templates

Vincent ALIMI
Laboratoire GREYC: ENSICAEN – Université de CAEN – CNRS
6 boulevard Maréchal Juin, F-14020 CAEN (France)
vincent.alimi@ensicaen.fr

Rima BELGUECHI
École Nationale Supérieure d'Informatique ESI, Alger, Algeria
r_belguechi@esi.dz

Christophe ROSENBERGER
Laboratoire GREYC: ENSICAEN – Université de CAEN – CNRS
6 boulevard Maréchal Juin, F-14020 CAEN (France)
christophe.rosenberger@ensicaen.fr

Abstract

Privacyand security are one of the most important challenges in biometrics. We propose in this paper an architecture for the secure storage and verification of the biometric template. We propose to use at the same time a trusted architecture based on Global Platform and an algorithmic solution for providing a cancelable biometric template. We illustrate this new technique on fingerprints. In the experimental results, we put into obviousness the benefit of the proposed architecture.

1 Introduction

Secure and privacy preserving management of our digital identities in the constantly evolving numerical world is of paramount importance for citizens, industries, social groups, and governments. Numerous applications are emerging related to physical access control (buildings, restricted areas …), logical access points (bank accounts, tax payments …) or identity documents (passport, national identity card…). In order to achieve more secure systems, biometric technologies are employed in an increasing manner in order to verify the identity of a user (to perform an authentication) or to find out his/her identity (identification tasks). The major reason for this widespread use of biometrics is that this technology provides the strongest proof of the physical presence of a person. The variety of biometric characteristics available can be classified in three broad categories: Biological characteristics such as, DNA, cardiac signals [1], Electroencephalogram signals [2]... Behavioral characteristics such as keystroke dynamics [3], voice... Morphological characteristics such as fingerprints, face, iris, or hand veins [4].

However, with more and more applications using biometrics, new privacy and security risks arise. For example, personal (biometric) information could be tracked from one application to another by cross-matching between biometric databases, thus compromising privacy. A crucial issue is the potential misuse of collected biometric data. Questions like "What can I do if my biometric data has been stolen or misused?" require urgent attention not only to reassure users with regards to privacy intrusion but also to prevent misuse and improve accuracy. Moreover, since standard biometric templates are permanently associated with an individual, they could not be used any more in case they are compromised. Since they cannot be replaced, they are also inherently non revocable. This

This paper was presented at the NISK-10 conference.

makes “classical” biometric systems inappropriate for privacy and security critical applications. Therefore, these major issues of biometric systems that guarantee the rules of privacy protection should be solved urgently.

Figure 1: Illustrations of biometric modalities (a fingerprint image and a hand veins image)

Recently, different architectures have been proposed by academics and industries [5] in order to guarantee some security issues such as the storage of applications and data in a secure way in different devices such as mobile phones or smart cards. This trusted architecture is the ideal support for storing biometric templates for security reasons and also because this can be done in a post-personalization way. Over the last decade, a new innovative multidisciplinary research field has emerged, that combines biometrics and cryptography, and that has the capability to guarantee biometric data privacy in an algorithmic way. The resulting innovative hybrid systems have the following important properties: they confer to biometric characteristics the needed capabilities of revocability, privacy, and diversity, and provide cryptographic systems with a strong link to the user through biometrics.

The objective of this paper is to describe how these two complementary technologies could contribute to solve some security and privacy issues concerning the use of biometrics for the authentication of an user for any kind of transaction. The paper is organized as follows. The next part focuses on the state of the art of trusted architectures and the description of Global Platform that is the one that retained our attention. We then present the biohashing techniques that permit to revoke the biometric template of an individual in case of attack or after a pre-defined period (like certificates). Some experimental results are given and put into obviousness the advantages of the proposed techniques. We finally conclude this study and give some perspectives.

2 Trusted Architecture

Smart cards programming languages appeared in the mid 90s and with them the first multi-applications cards. These technologies are known as MULTOS, Windows for Smart Cards, ZeitControl, SmartCard .NET and the most widespread: Java Card. Java Card is an adaptation of the well-known Java technology to the smart card constraints. Java Card is an open language and it explains its great success. Based on a virtual machine environment, it is very portable (“Write Once, Run Everywhere”) and allows several applications to be installed and ran on the same card. But this technology also has drawbacks. Indeed, the cohabitation of applications raises some questions. How and when load the applications? Shall applications loading be secured? How to isolate applications each from others? What

the life cycle of a single application on the card? How to determine the privileges of an application? … Answers to these issues have been provided by the GlobalPlatform technology. The following section describes it and the benefits of implementing it for biometric in general and for our system in particular.

The GlobalPlatform consortium

GlobalPlatform (formerly named Visa Open Platform) is an organization that has been established in 1999 by leading companies from the payment and communications industries, the government sector and the vendor community, and is the first to promote a global infrastructure for smart card implementation across multiple industries. Its goal is to reduce barriers hindering the growth of cross-industry, multiple application smart cards. The smart card issuers will continue to have the freedom to choose from a variety of cards, terminals and back-end systems.
The GlobalPlatform specifications cover the entire smart card infrastructure: smart cards, devices and systems. Written consistently, this set of specifications allows developing multi-applications and multi-actor smart cards systems. It specifies the technical models that meet the business models requirements.

GlobalPlatform and biometrics

In a white paper published in 2009 [7], the GlobalPlatform consortium presented for the first time the "GlobalPlatform value proposition for biometric match-on-card verification". We study in this section how GlobalPlatform meets the requirements for biometrics.

In a match-on-card solution, it is absolutely necessary to establish a chain of trust between all components of the system and at every phase of the process. The system components are the enrollment station, the identity management system, the smart card management system and the on-card application. The phases implied in the chain of trust are the enrollment process and the user verification. Those requirements are met by the set of specifications that maintain the GlobalPlatform committees (GlobalPlatform System Specifications), the GlobalPlatform Device Specifications and the GlobalPlatform Card Specifications. Those specifications take place at every stages as shown in Figure 2.

The system specifications are perfectly adapted to the enrollment process as they allow the secure delivery of critical data between entities and establishment of management responsibilities.

During the enrollment process, a trusted device must be used to capture a user's biometric data. The capacity to trust this device is offered by the device specifications, more precisely by GDP/STIP[2]. In [7], we find a very good definition of GDP/STIP objective: "Its aim is to define an open architecture and software infrastructure for trusted terminals as well as open specifications for the management of the lifecycle of these trusted devices".

[2] GDP/STIP stands for GlobalPlatform Device / Small Terminal Interoperability Platform.

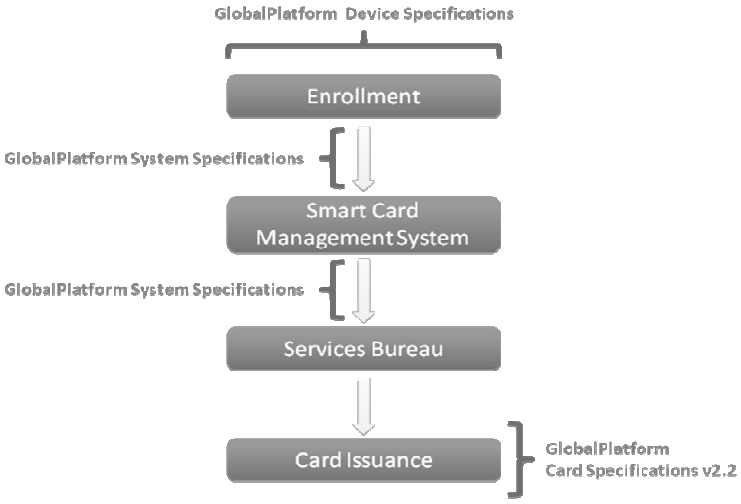

Figure 2: GlobalPlatform technology applied to biometric match-on-card enrollment

The GlobalPlatform card specifications are involved in the user verification process. They constitute an essential link in the chain of trust. We will see below how a GlobalPlatform compliant smart card prevents sensitive data to be tampered, makes it possible to establish secure communications and multi-application management.

The GlobalPlatform card specification [6] defines the behavior of a GlobalPlatform Card. The GlobalPlatform card architecture (see Figure 4) is comprised of a number of logical and physical components that provide application interoperability and security, in an issuer controlled environment. For example, it is important for the actors of a biometric match-on-card verification solution – with thousands of cards and several card manufacturers – to have a common "language" and protocols for managing card content.

At the bottom of the architecture, we encounter the smart card microprocessor. The Runtime Environment is responsible for providing an abstraction layer between the GlobalPlatform card architecture and the underlying hardware and software technologies. A typical runtime environment consists of three main components [5, 6]:

- a Smart Card Operating System (SCOS),
- a Virtual Machine (VM),
- an Application Programming Interface (API, Java Card or MULTOS).

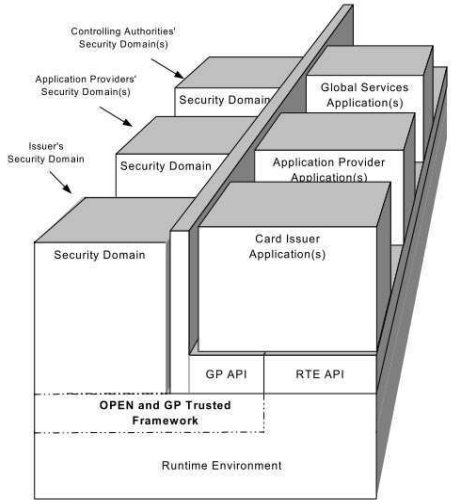

Figure 4: GlobalPlatform Card Architecture
(source: GlobalPlatform Card Specifications [6])

The Trusted Framework provides inter-applications communication services between applications. The main responsibilities of the GlobalPlatform Environment (OPEN) are to provide an API to applications (GlobalPlatform API), command dispatch, application selection and card content management. Security Domains (SD) act as the on-card representatives of off-card authorities. It allows its owner to control an application in a secure way without sharing any keys or compromising its security architecture. Security Domains support security services such as cryptographic functions, keys handling and secure communications. There are three main types of Security Domain, reflecting the three types of off-card authority recognized by a card: Issuer Security Domain, Supplementary Security Domain and Controlling Security Domain. The Issuer Security Domain (ISD) is the first application installed on a card. It is mainly used to perform all issuer related card content management. For example, the ISD holds the issuer's keys and performs cryptographic operations when card content changes occur. The Supplementary (SSD) or Application Provider Security Domain (APSD) is a secured environment where application providers are allowed to download, install and maintain applications following their own life cycle. The Controlling Authority Security Domain (CASD) is a special type of SSD. It is the on-card representative of the Controlling Authority. Thus, its role is to enforce the security policy on all application code loaded to the card.

In this section, we studied how the set of GlobalPlatform specifications make them suitable for a match-on-card verification solution. In the next section, we will expose our system.

3 Biohashing

Although biometric technology offers a possible solution to the problem of authentication in the identity management systems, it should be kept in mind that a variety of threat exist

at various points in the biometric subsystem chain. Many of possible attacks were identified and documented by Ratha et al. [9]. The eight potential attack points are marked in Figure 5 and are elaborated below.

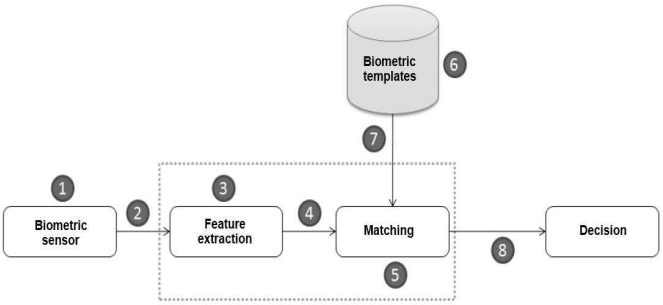

Figure 5: Locations of possible attacks in a biometric system

(1). Attack at the sensor. It is mostly due to the presentation of a spoof biometric trait. As an example, authors in [10], use easily gummy finger to masquerade as a legitimate user. This is principally due to the fact that biometric data are not considered to be secret. So, the user verification can be successful only when user's characteristics are fresh and have been collected from the user being authenticated. This implies that biometric input device must be trusted.
(2,4,7). Attack on the communication channels between modules. Insecure communication channels allow an adversary to lunch replay or hill-climbing attacks. If none cryptographic measure is taken, he also can intercept and modify biometric data.
(3,5,8). Attack on the software module. The runtime program at a module can be modified such that it always outputs the values desired by the adversary. Such attacks are known as Trojan-horse attacks
(6). Attacks on the stored templates. An attacker could attempt to capture a reference template, substitute a template to create a false reference, or more spectacularly, an attacker could compromise the database by stealing all its records.

The template attack is considered as the most potentially damaging one. This means that if a template record is compromised, original biometric data leaks out, which may lead to reconstruction and additional (identity) fraud. Moreover, biometric systems may violate user's privacy or anonymity. Indeed, biometric characteristics are highly sensitive data that may contain personal information. In addition, biometric systems link all user actions to a single identity so a person could be tracked from one application to another just by cross-matching. Another issue that is often overlooked is fallback. What can I do if my biometric data has been stolen or misused? Unlike password or token, the biometric template cannot be canceled or revoked. In view of these threats, a few desirable properties regarding biometric system security are as follows:

- Integrity: Forging fake identity should be infeasible.
- Confidentiality: Original biometric data should be kept secret.
- Privacy: Database cross-matching should not reveal any information.
- Revocability: Revocation should be easy.

- Loss detection: One of the most complicated issues with biometric deployment is how to detect and recover from the loss of biometric data.

So, privacy, security and comfort of the users will depend on the quality of (1) supporting architecture and (2) data-protection mechanisms. In Tab.1, we try to analyze vectors needed to meet high security requirements for a biometric system:

		Integrity	Confidentiality	Privacy	Revocability	Loss detection
Supporting architecture	Liveness detection	X				
	Tamper Resistance	X	X	X		X
	Secure Communication	X	X			
	Trusted Enrolment	X	X			
Data protection mechanism	Clear Template					
	Encrypted Template		Not sufficient	Not sufficient		
	Protected Template		X	X	X	

Table 1: Possible solutions to secure the management of biometric systems

From Table 1, we deduce that the five desirable properties can be reached if we combine: liveness detection, tamper resistance device like smartcards, secure communication, trusted enrollment and protected template. While the first four vectors can be handled by the Global Platform standard, the protection of the biometric template is a recent research area which addresses the problem by a software manner. In the following section, we make a brief overview of the main published techniques.

Template protection schemes

Due to the intraclass variability in the acquired biometric signal, one cannot store a biometric template in an encrypted form and then perform the matching in the encrypted domain. Hence, standard encryption techniques are not useful for securing biometric templates. So, the idea of template protection schemes aims to secure the template in a software manner where confidentiality and revocability properties will be granted. The proposed methods generally fall into two categories:

- Biometric cryptosystems.
- Feature transformation functions.

In biometric cryptosystems, a helper data as a secret key k is combined with the template to lock the biometric set. Here, error correcting codes were designed as an alternative to deal with the intra-variation problem. Figure 6 illustrates a possible cryptosystem scheme:

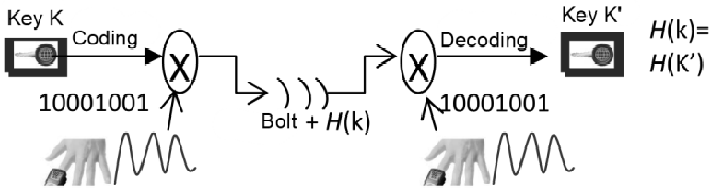

Figure 6: Principle of fuzzy commitment scheme

Figure 6 presents a method proposed by Juels and Wattenberg [11], called fuzzy commitment. During the enrollment step, a word associated to a code $c \in \{0,1\}^n$ is computed given the Key **K** belonging of the user U. The biometric template for the user is represented given a sequence x containing n bits. Only the couple $(c \otimes x, H(k))$ will be saved, H being a hashing function. During the verification step, the user U gives its biometric signal x'. To verify the commitment $(c \otimes x, H(k))$, the value $(c \otimes x \otimes x')$ is computed in order to derive the value of the key **K'**. The user U is authenticated if $H(k) = H(k')$. Even if this approach does not necessitate the storage of the biometric template, it is limited to biometric data having a binary representation. In 2002, Juels and Sudan [12] modified this approach in order to be used for partial representations with the name of fuzzy vault where the polynomial interpolation principle has been used. A secret (Key **K**) is a polynomial function P of degree d. During the enrollment step, the system computes one fuzzy vault V with P and the reference biometric template. The user is authenticated when it is possible to get back P from V and the fresh biometric data. The shortcoming of the fuzzy vault is the absence of any **revocability scenario**.

In parallel, in the feature transform approach, a transformation function F is applied to the biometric template T and only the transformed template F(T) is stored in the database. Ideally, F is a one-way function. Ratha et al. [13] proposed three different transformations for fingerprints (Cartesian, polar, and functional). These transformations are one-way transformations as it is not possible (or practically feasible) to obtain the original biometric data from the transformed data. However, the administration of revocability is not easy and the performance is largely decreased compared to baseline system. Using tokenized random numbers for biometric discretization is another solution proposed by a group of researchers in [6]. An advantage of this approach is to obtain a cancelable biometric data. To re-issue the user identity, a specific new token needs to be given. The authors denote this model as BioHashing. For our biometric system, we use this principle for the fingerprint modality. Our interest for BioHashing is explained by its revocability property, so we can issue a new user credential from the same biometric trait periodically or after revocation demand as it is done for certificates. The use of fingerprint is related to the supremacy of this modality over the biometric market.

A biometric cancelable system

We illustrate the cancelable biometric we developed. First, the general process is described. Secondly, the computational details of the biometric template are given. The principle of this cancelable method is to generate a biocode from a biometric feature and a salt value (random value in order to change the biocode after revocation). The salt value has to be

stored in a secure element (USB disk, smartcard...). The generated biocode is composed of binary elements. Figure 7 illustrates the principle of BioHashing.

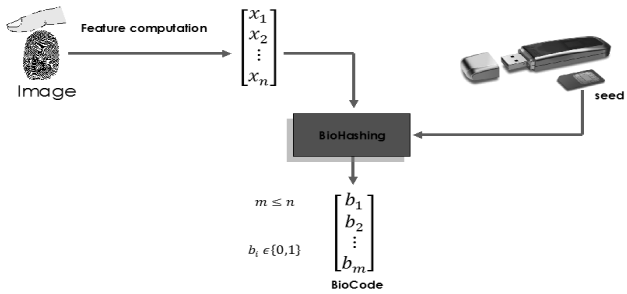

Figure 7: General principle of the BioHashing technique

BioHashing

In general, the process of BioHashing (see Figure 7) has two stages. In the first stage, some features (f_1,f_2,…,f_n) are derived from the raw biometric signal. The biometric feature vector is called FingerCode [16]. In the second stage, features are mapped to a binary descriptor $b \in \{0,1\}^m$, where m is the length of the bit-string code. Different biometric signals exploit different techniques in the first process, but the focus of our analysis is discretization, the process of BioHashing, consisting of four steps:

1) Generate a set of pseudo-random vectors Δ. In practice, a random number sequence r could be generated from a seed stored on a physical device (such as a USB token or a smartcard) through a random number generator. The seed is different among different users. For testing, random bit/number algorithms are publicly available such as ad hoc scheme.

2) Apply Gram-Schmidt process to transform the basis Δ into an orthonormal set of matrices $r_{\perp i}$, $i = 1..m$.

3) Compute the inner product between the biometric feature f and $r_{\perp i}$, $(\langle f \mid r_{\perp i} \rangle)$, $i = 1,...,m$. This projection results in an error tolerant representation.

4) Compute an m-bit BioHash denoted as b ($b \in 2^m$),

$$b_i = \begin{cases} 0 \text{ if } \langle f \mid r_{\perp i} \rangle \leq \tau \\ 1 \text{ if } \langle f \mid r_{\perp i} \rangle > \tau \end{cases}$$

where τ is a preset threshold.

The resulting bitstring b named BioCode is compared using Hamming distance. The security of the process is assured if the BioCode is non invertible. Note that the user must provide his Biocode and the seed value to be authenticated.

4 Experimental Results

We present in this section some experimental results on images from the FVC2002 fingerprint benchmark database [15]. Figure 8 presents the Receiver Operating Curve (ROC) curve of the initial system using only the fingercode (without any **BioHashing**) on this database. We obtain an EER (Equal Error Rate) value of 4%. When the BioHashing technique is applied, the EER reduces to 0%. This is shown in Figure 8.

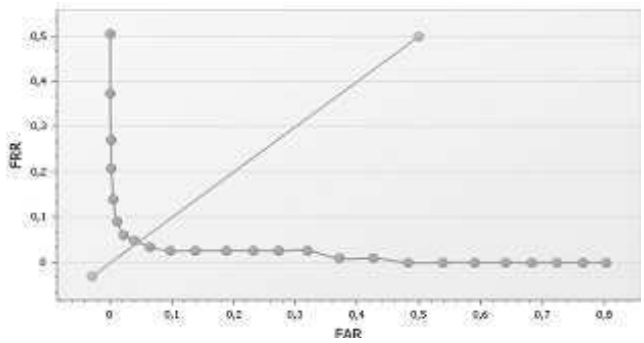

Figure 8: Performance of the biometric system based on the fingercode without BioHashing

Now, we illustrate the robustness of the system based on BioHashing when it is attacked. Figure 9 shows the performance when the impostor has the biometric reference but not the seed value. In this case, the EER value is also 0%, meaning that the impostor cannot be authenticated. The use of BioHashing improves the performance of the initial biometric system because the seed value can be considered as supplementary information for the authentication of an individual. Figure 11 presents the worst case when the impostor has access to the Biocode and obtains the seed value. Of course, the impostor does not have the Fingercode of the user. In this case, the EER value is 9.7%. The best parameters of the system achieve an EER of 6.8%. To support our claim of revocability, we assign n different keys to each individual of the database. The resulting n BioCodes should be different. In our experiment, we achieve a FAR (False Acceptance Rate) of 0% which proves the revocability of this method. It is important to mention, that the match-on-card implementation of this biometric authentication technique does not decrease the performance of the system at any way contrary to many others methods.

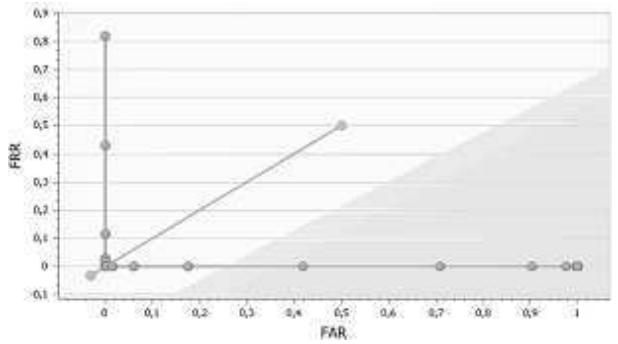

Figure 9: Performance of the biometric system based on the BioHashing in the case when the impostor has the biometric reference but not the seed value

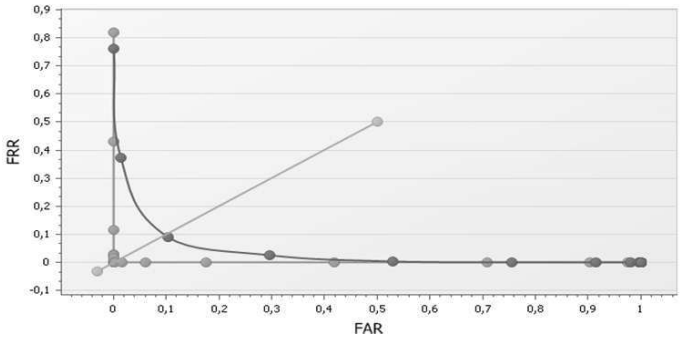

Figure 11: Performance of the biometric system based on the proposed BioHashing in the worse case when the impostor has the biometric reference and the seed value

5 Conclusions And Perspectives

We proposed in this paper a secure architecture to store cancelable biometric templates. We showed that GlobalPlatform is a good candidate as trusted architecture to store private data such as biometric templates. For privacy aspects, cancelable biometrics is a good algorithmic candidate to solve this problem. Note that we also put into obviousness that the taking into account these constraints permits us to improve the efficiency of the authentication process. Our future works will concern the processing of other biometric modalities such as palm vein or face and the improvement of the Biohashing technique in term of robustness.

REFERENCES

[1] K. Phua et al., Heart sound as a biometric, Pattern Recognition 2007

[2] R. Palaniappan, Electroencephalogram Signals from Imagined Activities: A Novel Biometric Identifier for a Small Population. E. Corchado et al. (Eds.): IDEAL, LNCS 4224, pp. 604 – 611, © Springer-Verlag Berlin Heidelberg 2006.

[3] R. Giot, M. El-Abed, C. Rosenberger, GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems. IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington DC USA, Sept. 28-30, 2009.
[4] P.-O. Ladoux, C. Rosenberger, B. Dorizzi, Hand Vein Verification System based on SIFT matching. The 3rd IAPR/IEEE International Conference on Biometrics (ICB), M. Tistarelli and M.S. Nixon (Eds.): LNCS 5558, pp.1297–1305, © Springer-Verlag Berlin Heidelberg 2009.
[5] K. Markantonakis and K. Mayes, "An overview of the GlobalPlatform smart card specification," Information Security Technical Report: Smart Card Security, vol. 8, no. 1, pp. 17–29, 2003, elsevier Science Ltd (ISSN:1363-4127).
[6] GlobalPlatform, GlobalPlatform Card Specification Version 2.2, 2006.
[7] GlobalPlatform, The GlobalPlatform Value Proposition for Biometric Match-on-Card Verification, 2009.
[8] GlobalPlatform, GlobalPlatform Overview, 2004.
[9] N.K. Ratha, J.H. Connelle, R. Bolle. Enhancing Security and Privacy in Biometrics-Based Authentication System, IBM Systems J., vol. 40, pp.614-634, 2001.
[10] T. Matsumoto, H.Matsumoto, K.Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. Proc. of SPIE, vol. 4677, pp. 275-289, 2002.
[11] A. Juels and M. Wattenberg, A fuzzy commitment scheme, Proceedings of the 6th ACM conference on Computer and communications security, pp.28–36, 1999.
[12] A. Juels and M. Sudan, A fuzzy vault scheme, Proc. IEEE Int. Symp. Information Theory, 2002.
[13] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Trans on PAMI, Vol. 29, pp. 561-572, 2007
[14] A.B.J. Teoh, D. Ngo, A. Goh, BioHashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognition, 2004.
[15] FVC 2002, http://bias.csr.unibo.it/fvc2002/
[16] A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, Filterbank-based fingerprint matching, IEEE Trans. Image Process, Vol 5, pp. 846–859, 2000