One-Time Biometrics for Online Banking and Electronic Payment Authentication

Aude Plateaux, Patrick Lacharme, Christophe Rosenberger, Audun Jøsang

One-time biometrics for Online Banking and Electronic Payment Authentication

Aude Plateaux, Patrick Lacharme, Christophe Rosenberger
ENSICAEN, GREYC, F-14032 Caen, France

aude.plateaux@ensicaen.fr, patrick.lacharme@ensicaen.fr
christophe.rosenberger@ensicaen.fr

Audun Jøsang
Department of Informatics, University of Oslo, 0316 Oslo, Norway

audun.josang@mn.uio.no

***Abstract*—Online banking and electronic payment systems on the Internet are becoming increasingly advanced. On the machine level, transactions take place between client and server hosts through a secure channel protected with SSL/TLS. User authentication is typically based on two or more factors. Nevertheless, the development of various malwares and social engineering attacks transform the user's PC in an untrusted device and thereby making user authentication vulnerable. This paper investigates how user authentication with biometrics can be made more robust in the online banking context by using a specific device called OffPAD. This context requires that authentication is realized by the bank and not only by the user (or by the personal device) contrary to standard banking systems. More precisely, a new protocol for the generation of one-time passwords from biometric data is presented, ensuring the security and privacy of the entire transaction. Experimental results show an excellent performance considering with regard to false positives. The security analysis of our protocol also illustrates the benefits in terms of strengthened security.**

***Keywords*-e-payment, biometrics, online banking security, strong authentication.**

I. Introduction

Electronic commerce on the Internet is more and more used for online payment and online banking. In the same time, the fraud for these transactions is a major problem for financial institutions [11], [3]. Indeed, although the online payment only represents a small percentage of transactions, it concentrates a major loss for banks [19]. Many directives are related to online payments, as for instance, the European directive 2000/31/EC on e-commerce security [6], whereas the Directive on Payment Services, [7], provides an european wide single market for payments and a legal platform for SEPA (Single Euro Payment Area, [8]). The 3D-Secure protocol is the payment protocol proposed by the industry, developed to reduce the fraud in online payment.

In the usual case of e-commerce, the customer wants to purchase an online service, with a credit card, through a website. At a high level, the transaction generally begins with an authentication and a secure connection between the customer's client host and the service provider (SP) host, using a protocol such as SSL/TLS. In a second time, the user sends to the SP bank, through the SP host, his/her bank information: Personal Authentication Number (PAN), Card Verification Value (CVX2) and expiry date. SSL/TLS protocols enable to secure transaction between user's client host and the SP host. Nevertheless, there is no direct user's authentication in this scheme.

Security challenges in e-commerce are numerous, particularly related to user authentication, because the merchant and the cardholder are not in the same place during the transaction. So-called strong authentication is typically based on two-factor authentication. For example, an additional secret, sent by mobile phone, as for the 3D-Secure protocol [27] or an additional device as a CAP reader [12], [10] are required for electronic payments and online banking. The user's authentication system is traditionally realized by the user's bank (because the financial risk falls on the bank). Authentication should also take into account man-in-the-middle attacks (such as described in [3]). However, this paper is centered on user's authentication and such attacks are out of scope.

This paper presents an alternative method for user's authentication based on biometrics. The proposed system generates one-time passwords from fingerprints. The biometric data is not directly stored in the device and the generated password is different for each transaction in order to avoid replay attack.

The paper is organized as follows. Section 2 briefly presents state-of-the-art authentication solutions for e-payment. We define in Section 3 the security and privacy issues that the proposed solution should address. In Section 4, we present the OffPAD concept, a secure device to ensure secure Machine to Machine (M2M) transactions. We present in Sections the proposed authentication protocol. Some experimental results and security analysis are given in Section 6. Finally, we conclude and give some perspectives of this study.

978-1-4673-2480-9/13/$31.00

II. E-PAYMENT ARCHITECTURES

The Secure Electronic Transactions (SET, [24]) protocol, developed by VISA [1], and MasterCard [2], was a protocol for securing e-payment transactions by credit card. User authentication in SET was based on a public-key certificate installed on the client computer. VISA and MasterCard realised that the management of certificates was too complex for customers, so a simpler 3D-Secure protocol designed by VISA in 2001 was proposed as a solution to replace SET.

The 3D-Secure protocol [27] is the current authentication and payment architecture for credit cards on the web. It was first adopted by VISA, then other financial organizations developed their own implementations of VISA's 3D-Secure licensed architecture, such as MasterCard with its MasterCard SecureCode, American Express with SafeKey. A comparison between 3D-Secure and MasterCard SecureCode is proposed in [21]. The 3D-Secure protocol is composed of nine steps exchanged between five actors (Fig.1):

A. The user sends to the SP his/her purchase intention, with his/her bank information: PAN (Personal Account Number), expiration date, CVV2 (Card Verification Value). These data are intended for a dedicated module called MPI (Merchant Plug In) implemented into the merchant website.

B. MPI queries the directory server with the VEReq (Verify Enrollment Request) message.

C. The directory server checks the SP identity, the card number and the user's bank and recovers the ACS (Access Control Server) managing the card.

D. The message VERes (Verify Enrollment result) contains the response of message. The ACS checks if the users's bank is enrolled in the 3D-Secure program and sends the cardholder authentication URL to the MPI.

E. MPI sends the PAReq (Payer authentication request) message to the given URL. This message contains the details of the authorized purchase. MPI also opens on the client computer a pop-up window to the ACS.

F. The user provides the necessary information for authentication from the bank.

G. ACS sends to MPI a confirmation of user authentication through PARes message.

H. MPI records PARes message as confirmation of user authentication by ACS.

I. SP authenticates to the bank. The bank verifies the nature of the transaction from the user's bank and confirms the payment authorization from the SP. The SP gets his/her payment and the users's bank stores payment information to ensure non-repudiation of the transaction.

The main security flaw of 3D-Secure implementations,

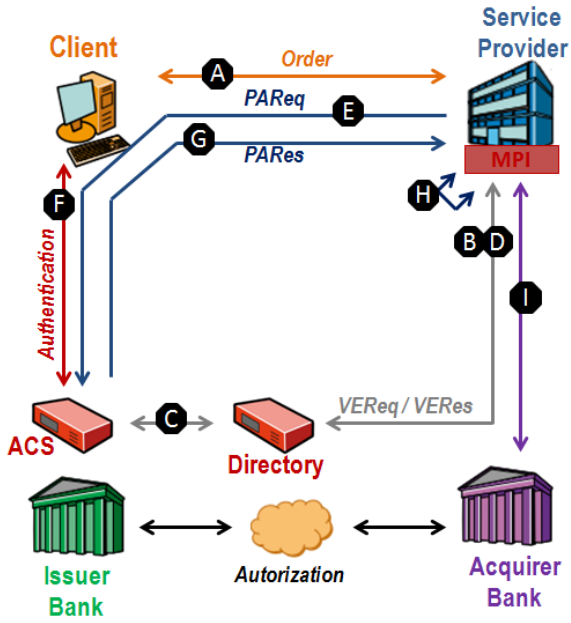

Figure 1. The 3D-Secure protocol

underlined in [19], concerns user authentication (step F). Some banks have used in the past the date of birth or other trivial secrets. Many banks have replaced these solutions by a strong authentication mechanism (e.g. challenge is sent to user's mobile phone) which then is a two-factor authentication scheme (based on the possession of the mobile phone and the knowledge of the PIN code for the logical access to it). However we argue that this user authentication scheme has significant vulnerabilities. We therefore propose a new approach based on biometrics which eliminates these vulnerabilities.

User authentication solutions, as CAP readers, TAN generators or the lightweight system proposed in [17], are Knowledge and Possession based approaches. We argue that only biometrics can direct authenticate users, whereas solutions based on knowledge and possession only authenticate users indirectly. The main reason is related to the particular relationship between the user and its authenticator. There are f course specific problems related to biometrics, such as mentioned below:

- A biometric data is very sensitive as it cannot be revoked in general. Its encryption is necessary but not sufficient (as the data should be decrypted for the matching process in general and as the lifetime of this data is very high). For these reasons, using central storage of biometric data is problematic.
- The matching process could make errors for genuine users but also impostors could be falsely accepted. This is not the case for password verification as long as the

correct password is typed (but there is no proof that it has been typed by the genuine user).
- Biometric data could be intercepted during its transmission. This could lead to security problems, such as replay attacks and privacy attacks based on linkability. For these reasons, the biometric data should be cancelable and dynamic (changing at each transaction).

In this paper, we propose a new solution that solves these problems. To achieve a security and privacy compliant solution, we combine two elements: the first one is a specific device owned by the user called OffPAD, and the second is a protocol using biometrics and cancelable algorithms. In the next section, we list the security and privacy requirements of the proposed solution.

III. Security and privacy requirements

In electronic payments, four main actors are present: The **user** C, who has an OffPAD, wants to purchase an online service with a credit card, through the website of a **service provider SP**. The user has an **issuer bank** and the SP has an **acquirer bank**. In this paper, we also call these payment providers: *user's bank* and *SP bank*. A fifth actor is often involved. It is the trusted party as a third-party cashier or the Directory used in 3D-Secure. The role of this fifth actor is various but generally allows to authenticate the banks. The proposed protocol is concentrated on user authentication and the user's registration with the SP.

During an online payment, numerous personal data are involved and must be protected against several threats, [4]. In order to preserve privacy and security properties, a list of ten requirements R_i is defined. These requirements should be taken into account during the user authentication/registration step in the e-payment architecture:

- R_1: **Confidentiality of transactions** requires that each exchanged data must be encrypted in order to protect these data against external entities.
- R_2: **Integrity of transmitted information** allows the accuracy of the content and so the non-alteration of data during transmission or storage.
- R_3: **User authentication** by a trusted party ensures the identity of the customer. Depending on the situation, the authentication can be realized thanks to a biometric data.
- R_4: **Authentication of the user's device** ensures the device is valid within the application. This authentication can be realized thanks to an identifier of the device.
- R_5: **Proof that the device belongs to the user** ensures the device prevents device replacement attacks.
- R_6: **SP authentication** by the user or by a trusted party ensures the identity of the SP.
- R_7: **Bank authentication** by a trusted party ensures the identity of SP bank and customer's bank.
- R_8: **Unlinkability** of realized transactions prevents linking different transactions of the same customer.
- R_9: **Confidentiality of customer information** CI (data minimization principle) ensures only authorized persons access to this information. This requires the user's biometric data are unknown to the banks and SP.
- R_{10}: **Data sovereignty** means that personal data associated with the customer can only be processed with his/her control and consent.

In the next section, we present the OffPAD concept as secure device for ensuring the security of sensitive operations.

IV. OffPAD concept

The PAD (Personal Authentication Device) is described by Jøsang and Pope [13] as a secure device external to the client computer platform. The PAD is the conceptual predecessor to the OffPAD. The OffPAD (Offline Personal Authentication Device) described by Klevjer et al. [16] and Varmedal et al. [26] is an enhanced version of the PAD, where an essential characteristic is to guarantee offline security (Machine to Machine communications). The OffPAD represents local user-centric identity management because it enables secure and user friendly management of digital identities and credentials locally on the user side. The OffPAD supports authentication of both user and service provider identities (i.e. mutual authentication) and can in addition support data authentication. For access to the OffPAD, the user must unlock the device by using e.g. a PIN, pass phrase, biometrics or other adequate authentication credentials. A possible OffPAD design is illustrated in Figure 2.

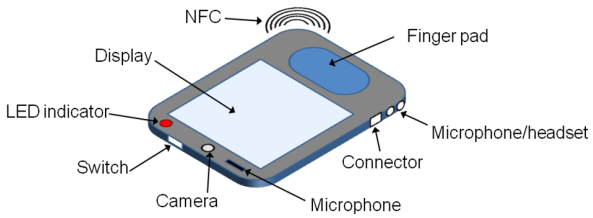

Figure 2. OffPAD concept [26].

The OffPAD is a trusted device, meaning that it is assumed to function as intended and to be adequately protected against relevant attacks. The OffPAD has limited connectivity to client platforms. These communication channels must therefore be carefully controlled, e.g. by sanitizing the received data. Protection against attacks resulting from physical theft is to have traditional access control based on PIN and biometrics, combined with some level of physical tamper resistance. However, it is not necessary that the OffPAD operating system and applications are free from vulnerabilities that are typically

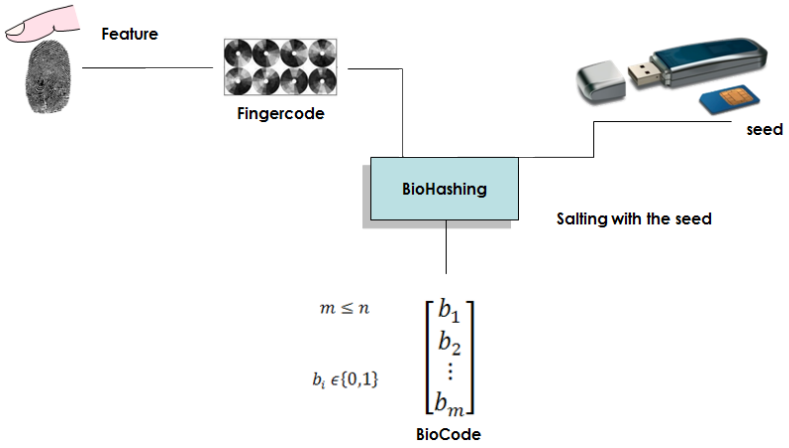

Figure 3. BioHashing scheme

found in online systems, because it is assumed that attackers will not be able to exploit such vulnerabilities since the OffPAD is offline most of the time. In that sense, a specific software bug which would have been a vulnerability in an online system is strictly speaking not a vulnerability in the OffPAD because it can not be exploited. The OffPAD may have several interfaces for communication. Microphone and camera may be used for voice and face recognition, and a fingerprint reader may be used for both authenticating to the device and elsewhere. The requirement of being offline does not exclude electronic communication with the OffPAD, but means that the communication follows controlled formats and takes place in short, restricted time periods. This decoupling from networks improves security of the device, as it is less vulnerable to outside attacks.

Any specific electronic communication should normally be disconnected, and should only be connected whenever it is needed for authentication or for management of the device. NFC with a backup USB connection is a suitable for OffPAD connectivity. This limits the threat of a man-in-the-middle attack when connecting an OffPAD to a computer. The first connection to the OffPAD builds upon the concept of Trust-On-First-Use (TOFU). On first use, there is no cryptographic way to verify the connection between the device and the client platform, the trust must simply be based on the physically observed set-up. On the first connection, some kind of pairing between the device and computer occurs, so that the subsequent connections can be verified to be between the same device and computer.

We use this secure device for online banking and electronic payment following an original protocol with biometrics. The following section explains the Biohashing algorithm used in the proposed protocol. Then, the section VI details this new original protocol.

V. BioHashing algorithm

The BioHashing algorithm transforms a real-valued vector of length n (i.e. the FingerCode, resulting from a feature extraction method) into a binary vector of length $m \leq n$ (i.e. the BioCode), as first defined by Teoh *et al.* in [25].

It consists of projecting the FingerCode on an orthogonal basis defined by a random seed (considered here as a secret), to generate the BioCode. The template transformation uses the following algorithm, where the inputs are the random seed and the FingerCode F and the output is the BioCode B:

1) For $i = 1, \ldots, m$, $m \leq n$ pseudorandom vectors v_i of length n are generated (from the random seed) and are gathered in a pseudorandom matrix.
2) The Gram-Schmidt algorithm is applied on the m vectors v_i of the matrix, for the generation of n orthonormal vectors $V_1, \ldots, V_m$.
3) For $i = 1, \ldots, m$, m scalar products $p_i =< F, V_i >$ are computed using the FingerCode F and the m orthonormal vectors V_i .
4) The m-bit biocode $B = (B_0, \ldots, B_m)$ is finally obtained, using the following quantization process:

$$B_i = \begin{cases} 0 & \text{if } p_i < t \\ 1 & \text{if } p_i \geq t, \end{cases}$$

where t is a given threshold, generally equal to 0.

When used for authentication the *Reference BioCode* (computed from the FingerCode after enrollment and after exhibiting the secret) is compared with the *Capture BioCode* (computed from the FingerCode computed after a new capture with the secret) with the Hamming distance. If this value is lower than a specified threshold set by the system administrator, the identity of the user is verified.

Roughly speaking, the first part of the algorithm, including the scalar products with the orthonormal vectors, is used for the performance requirements and the last step of the algorithm is used for the non-invertibility requirements of the BioHashing algorithm. As mentioned before, the random seed guarantees the diversity and revocability properties.

The user authentication protocol applies multiple times the BioHashing algorithm which we detailed in the next section.

VI. Proposed authentication protocol

The proposed authentication protocol uses biometric data that must be protected through the capture with the OffPAD device and template protection algorithms. Biometric template protection schemes are a group of technologies, included in privacy enhancing technologies, used to enhance both privacy and security of biometric data. Therefore, any template protection approach should allow to revoke a biometric data in case of interception, and should be carefully designed, with a strong security analysis. Among the different solutions in the literature, template protection can be achieved using biometric cryptosystems [15], [14], [9], [20] or by transforming the biometric feature data [22], [5], [25], [23]. As detailed in the next section, BioHashing is one popular scheme that belongs to this second category and allows to revoke a biometric template.

The proposed protocol is detailed with fingerprints but could be used for any other biometric modality (face, iris...). As we use biometrics, two main steps are required: enrollment and authentication.

1) Enrollment: This step has for objective to collect Alice's reference template. In our case, the template is given by a BioCode called *Reference BioCode* computed from a FingerCode (feature vector computed on the fingerprint) and a secret (user's secret concatenated with the serial number of the OffPAD device). User's secret could be a password or a random value stored in the OffPAD device (of course, it is protected by the biometric authentication to the device). Once the *Reference BioCode* has been computed, it is sent to the Alice's *Issuer Bank* through a SSL channel. Concerning an organizational point of view, this step could be done in a branch after identity checking by a physical person. Figure 4 details the enrollment process. There is no privacy issue to store the *Reference BioCode* by the *Issuer Bank* as this template is cancelable and as the BioHashing process is invertible.

2) Authentication: During an electronic payment, the *Issuer Bank* has to authenticate Alice (e.g. 3D-Secure process). A challenge is sent to Alice (number displayed on the computer or directly sent to her OffPAD). Alice has to provide her fingerprint and her password (that is not known by the *Issuer Bank*). A *Capture BioCode* is computed given the FingerCode on the capture biometric data, the password and the OffPAD serial number. The *Challenge Capture Biocode* is computed by applying the BioHashing algorithm on the *Capture BioCode* with the challenge sent by the *Issuer Bank* as secret. The *Issuer Bank* computes also the *Challenge Reference Biocode* by applying the BioHashing algorithm on the *Reference BioCode* with the challenge. The Hamming distance is used to make the comparison of these two Challenge BioCodes and if the distance is lower than a predefined threshold, Alice is authenticated. Figure 5 details the whole process.

3) Discussion: The challenge sent by the *Issuer bank* allows us to define a One Time Biometrics authentication solution. We assume in this solution that the OffPAD is a secure device. In this solution, the *Issuer bank* controls the decision on Alice's authentication.

VII. Analysis of the proposed method

In this section, we analyze the proposed authentication protocol considering two aspects: performance analysis (considering biometric errors) and security and privacy issues.

A. Performance analysis

In this section, we analyze the performance of the protocol to avoid false rejection and false impostor. We start by defining the experimental protocol.

1) Experimental protocol: In this study, we used three fingerprint databases, each one is composed of 800 images from 100 individuals with 8 samples from each user:

- FVC2002 benchmark database DB2: the image resolution is 296×560 pixels with an optical sensor "FX2000" by Biometrika ;
- FVC2004 benchmark database DB1: the image resolution is 640×480 pixels with an optical Sensor "V300" by CrossMatch ;
- FVC2004 benchmark database DB3: the image resolution is 300×480 pixels with a thermal sweeping Sensor "FingerChip FCD4B14CB" by Atmel.

Figure 6 presents one image from each database. We can see that fingerprints are quite different and representative of the different types of fingerprint (acquired with sensors using different technologies).

These databases have been used for competitions (Fingerprint Verification competition) in 2002 and 2004. Table 1 presents the performance of the best algorithms on these databases[1]. The Equal Error Rate (EER) computes the compromise error rate when genuine users have been falsely rejected and impostor falsely accepted. ZeroFMR

[1] http://bias.csr.unibo.it/fvc2002

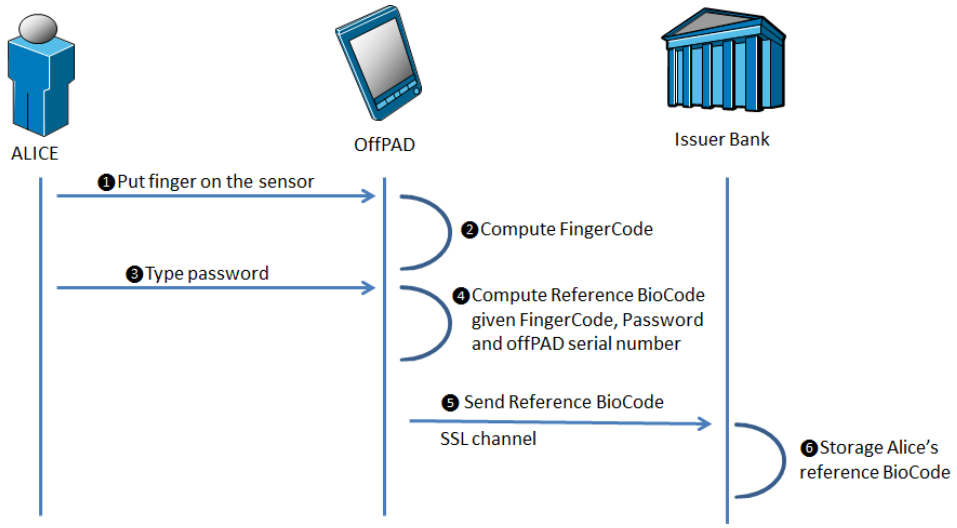

Figure 4. Enrollment step

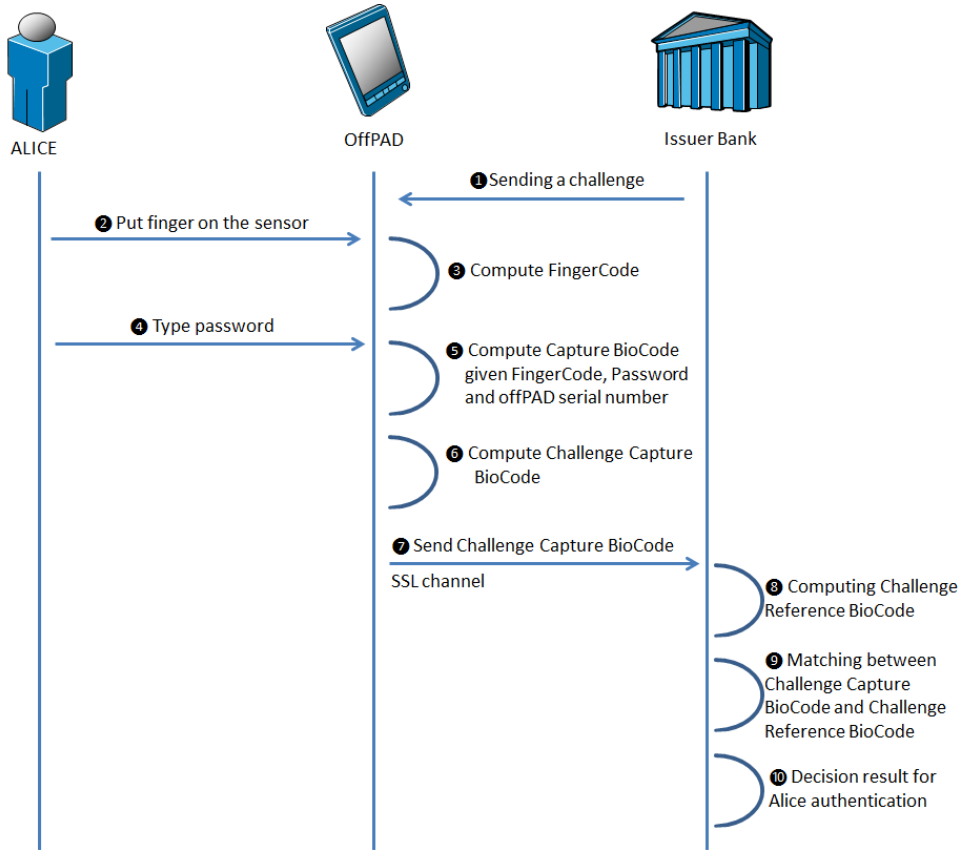

Figure 5. Authentication step

(a) (b) (c)

Figure 6. One fingerprint example from each database: (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3

is the value of False Non Match Rate (FNMR) when no impostor is falsely accepted. These values define the complexity of each database and give some elements of the performance what we can expect on these databases.

$Databases$	EER	$ZeroFMR$
$FVC2002\ DB2$	0.14%	0.29%
$FVC2004\ DB1$	0.61%	1.93%
$FVC2004\ DB3$	1.18%	4.89%

Table I
PERFORMANCE OF THE BEST ALGORITHM FOR EACH DATABASE (SEE HTTP://BIAS.CSR.UNIBO.IT/FVC2002)

As FingerCode, we used Gabor features (GABOR) [18] of size n=512 (16 scales and 16 orientations) as template. These feature are very well known and permit a good texture analysis of a fingerprint. For each user, we used the first FingerCode sample as reference template. Others are used for testing the proposed scheme. BioCodes are of size m=256 bits. In order to quantify the performance of the One Time Biometrics approach, we computed 1000 comparisons (with the Hamming distance) between the challenge Reference BioCode and challenge Capture BioCode for each user. We obtained 100.000 intraclass and interclass scores for the performance analysis of the proposed scheme.

2) Experimental results: We applied the previous protocol to the proposed authentication solution. On the three databases, we reach an EER value very close to 0%. In order to illustrate this efficiency, we show in Figure 7 the distribution of intraclass and interclass scores for each database. We clearly see that there is no overlap between the two distributions and a threshold near 60 (meaning maximal 60 different bits between the capture and Reference BioCodes is tolerated) could be used. In the last column of Table 2, we present the EER value by considering an impostor has in his/her possession the OffPAD device and the user password (worst case). In this case, the impostor can apply the Zero effort attack by providing his/her biometric data to impersonate the genuine user. We tested 100.000 attacks for each database and this attack is successful from 16% to 25% of the cases. In classical approaches (two-factor authentication), this attack is always successful.

$Database$	$EERwithoutattack$	$EERwithattack$
$FVC2002\ DB2$	0%	25.85%
$FVC2004\ DB1$	0.00093%	23.95%
$FVC2004\ DB3$	0.00023%	16.12%

Table II
PERFORMANCE OF THE PROPOSED ALGORITHM FOR EACH DATABASE

B. Security and privacy analysis

The proposed protocol is more respectful of the users' privacy than that of 3D-Secure protocol. We propose an analysis of the proposed protocol in this section.

1) Data security and authentication: The secure channel between actors and the encryption schemes ensure the confidentiality of exchanged data and the data integrity during the protocol. Consequently, the requirements R_1 and R_2 are ensured. Entities authentication is also realized through SSL for the SP (R_6) and the banks (R_7), whereas user authentication (R_3) is realized thanks to the strong authentication through Biohashing algorithm. Moreover, thanks to the challenges during user authentication, this authentication is an One Time Biometrics authentication solution. Consequently, the different transactions of a same user cannot be linked. The requirement R_8 is thus guaranteed. The device is also authenticated by its serial number and a proof of the user's device ownership is provided. Consequently, the requirements R_4 and R_5 are ensured. Moreover, for the user authentication solution, the user only needs to produce what he/she is (biometric data) and what is known (password).

2) Privacy analysis: During our authentication process, several sensitive information items are exchanged and stored, such as biometric data and password. Their storage should not be centralized. However, thanks to the use of the BioHashing algorithm, the template is cancelable. Thus, the knowledge of the BioCode does not given knowledge concerning a user's personal information. In our case, the knowledge of the Reference BioCode does not involve the knowledge of the biometric data, the fingerprint. Only the relevant and necessary data are sent and stored. Thus, the minimization principle (R_9) is also respected. Moreover, for each user's authentication, the user must present his/her finger and give his/her password. These actions involve the user who gives his/her consent to use this data which he/she can control thanks to the computations of the Capture BioCode and the storage of the Reference BioCode. The data sovereignty principle (R_{10}) is consequently respected.

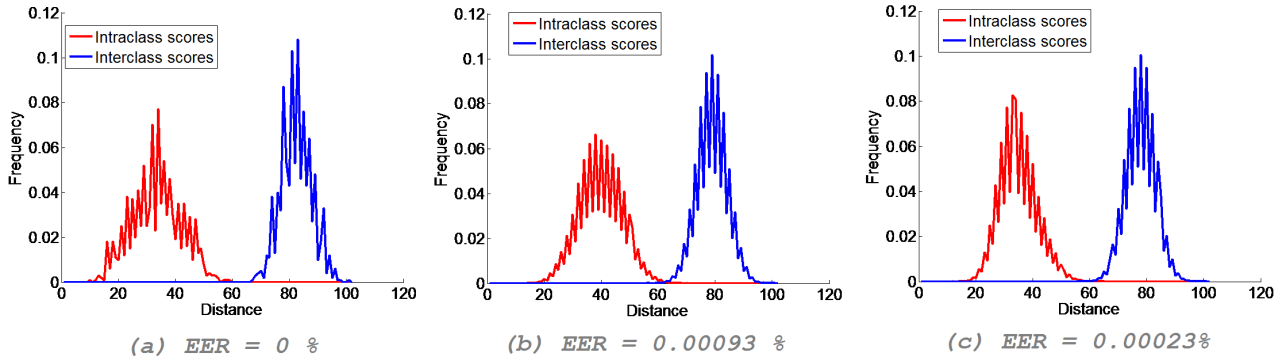

Figure 7. Distribution of intraclass and interclass scores for each database: (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3

VIII. Conclusion and perspectives

The proposed solution uses an extra device, which has a non negligible cost. Nevertheless, we consider the financial risk of on-line banking or payment is important and strongly increases. Consequently, this additional device is not a porblem for a real world deployment. In this paper, a new authentication protocol called "One Time Biometrics" for online banking and electronic payment authentication. We protocol consists of two main components. The first component is a specific device called OffPAD that ensures many security and privacy issues. The second component is the use of a biometric template protection algorithm to make possible the storage of a biometric data in a centralized way by the Issuer Bank. A challenge-based protocol is then proposed to prevent replay attacks. The user authentication scheme is usable for users as they do not have to remember different passwords. The protocol demonstrates very good performances on three benchmark fingerprint databases and good properties considering security and privacy issues.

Future perspectives of this study are numerous. We plan to use multiple biometric data in order to avoid the use of a password in the proposed protocol, and we also plan to design a biometric data authenticaiton protocol.

IX. Acknowledgment

The authors would like to thank the Eurostars program for assistance to the project, as well as for financial support. http://www.eurostars-eureka.eu/

References

[1] Visa corporate, 1958. http://corporate.visa.com/index.shtml.

[2] Mastercard worldwide, 1966. http://www.mastercard.com/.

[3] Manal Adham, Amir Azodi, Yvo Desmedt, and Ioannis Karaolis. How to attack two-factor authentication internet banking. In *Financial Cryptography*, 2013.

[4] G. Antoniou and L. Batten. E-commerce: protecting purchaser privacy to enforce trust. *Electronic commerce research*, 11(4):421–456, 2011.

[5] R.M. Bolle, J.H. Connell, and N.K. Ratha. Biometric perils and patches. *Pattern Recognition*, 35(12):2727–2738, 2002.

[6] European Commission. Directive 2000/31/ec of the european parliament and of the council of 8 june 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('directive on electronic commerce'), 2000.

[7] European Commission. Directive 2007/64/ec of the european parliament and of the council of 13 november 2007 on payment services in the internal market amending directives 97/7/ec, 2002/65/ec, 2005/60/ec and 2006/48/ec and repealing directive 97/5/ec, 2007.

[8] European Payments Council. Sepa - single euro payment area, 2007. http://www.sepafrance.fr/.

[9] J. Daugman. New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 37(5):1167–1175, October 2007.

[10] S. Drimer, S. Murdoch, and R. Anderson R. Optimised to fail: Card readers for online banking. *Financial Cryptography and Data Security*, pages 184–200, 2009.

[11] Y. Espelid, L.H. Netland, A. Klingsheim, and K. Hole. A proof of concept attack against norwegian internet banking systems. *Financial Cryptography and Data Security*, pages 197–201, 2008.

[12] MasterCard International. Chip authentication program functional architecture, September, 2004.

[13] Audun Jøsang and Simon Pope. User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference*, page 77. Citeseer, 2005.

[14] A. Juels and M. Sudan. A fuzzy vault scheme. In *ISIT*, page 408, 2002.

[15] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[16] Henning Klevjer, Kent Are Varmedal, and Audun Jøsang. Extended http digest access authentication. In *Policies and Research in Identity Management*, pages 83–96. Springer, 2013.

[17] Shujun Li, Ahmad-Reza Sadeghi, Soeren Heisrath, Roland Schmitz, and Junaid Jameel Ahmad. hPIN/hTAN: A lightweight and low-cost e-banking solution against untrusted computers. In *Financial Cryptography*, 2011.

[18] B. S. Manjunath and W.Y. Ma. Texture features for browsing and retrieval of image data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18:37–42, 1996.

[19] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. *Financial Cryptography and Data Security*, pages 336–342, 2010.

[20] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. Scifi - a system for secure face identification. In *IEEE Symposium on Security and Privacy*, 2010.

[21] V. Pasupathinathan, J. Pieprzyk, H. Wang, and J.Y. Cho. Formal analysis of card-based payment systems in mobile devices. In *Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54*, pages 213–220. Australian Computer Society, Inc., 2006.

[22] N.K. Ratha, J.H. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication system. *IBM Systems J.*, 37(11):2245–2255, 2001.

[23] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Information Security*, 3, 2011.

[24] S.E.T. Secure electronic transaction specification. *Book 1: Business Description. Version*, 1, 2002.

[25] A.B.J. Teoh, D. Ngo, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 40, 2004.

[26] Kent Are Varmedal, Henning Klevjer, Joakim Hovlandsvåg, Audun Jøsang, Johann Vincent, and Laurent Miralabé. The offpad: Requirements and usage. In *Network and System Security*, pages 80–93. Springer, 2013.

[27] Visa. 3D secure protocol specification, core functions, July 16, 2002.