Biométrie à usage unique pour la monétique

Aude Plateaux (aude.plateaux@ensicaen.fr)*
Patrick Lacharme (patrick.lacharme@ensicaen.fr)*
Christophe Rosenberger (christophe.rosenberger@ensicaen.fr)*
Audun Jøsang (audun.josang@mn.uio.no) †

Abstract: Les paiements sur l'Internet et les services bancaires en ligne font désormais partis de notre quotidien. L'authentification de l'utilisateur est généralement basée sur un système à deux facteurs. Néanmoins, le développement des logiciels malveillants et d'attaques diverses font de l'ordinateur un outil non sécurisé et rendent l'utilisation d'un mot de passe trop faible. Cet article examine l'utilisation de la biométrie pour sécuriser l'authentification de l'utilisateur dans le domaine bancaire en ligne et propose l'emploi d'un objet spécifique, nommé OffPAD. Cet objet ne contient pas lui même de données biométrique, l'hypothèse étudiée porte sur un système centralisé. Plus précisément, un nouveau protocole d'authentification à l'aide d'une génération d'un mot de passe à usage unique à partir de données biométriques est présenté et permet d'assurer la sécurité de la transaction et de protéger la vie privée de l'utilisateur. Les résultats expérimentaux montrent une excellente performance et une analyse de sécurité est présentée afin d'illustrer les avantages de la solution proposée.

Keywords: e-paiement, biométrie, sécurité bancaire, authentification forte.

1 Introduction

La fraude sur les opérations bancaires croit et devient un problème majeur pour les institutions financières [AADK13]. En effet, même si le paiement en ligne ne représente qu'un petit pourcentage des transactions bancaires, la fraude représente une grande perte pour les banques [MA10]. De nombreuses directives sont liées aux paiements en ligne, comme par exemple la directive européenne 2000/31/CE ou encore la directive sur les services de paiement [Com07] qui fournit un large marché européen unique pour les paiements, ainsi que la plate-forme juridique du SEPA (Single Euro Payment Area). Des protocoles sont alors mis en place afin de réduire la fraude dans le paiement en ligne, comme le protocole 3D-Secure proposé par l'industrie. Dans le cas habituel du e-commerce, le client souhaite acheter un service en ligne avec une carte de crédit, par le biais d'un site marchand. À un niveau élevé, l'opération commence généralement par une authentification et une connexion sécurisée entre l'ordinateur du client et le fournisseur de services (SP), en utilisant par exemple, le protocole SSL/TLS. Dans un second temps, le client fournit à la banque de SP, via ce SP, ses renseignements bancaires : le numéro personnel d'identification (PAN), la valeur de vérification (CVX2) et la date d'expiration de sa carte. Alors que les protocoles de type SSL/TLS permettent de sécuriser la transaction entre l'ordinateur du client et le fournisseur de services, il n'y a pas d'authentification directe de l'utilisateur.

∗. ENSICAEN, Laboratoire GREYC, 17 rue Claude Bloch, 14000 Caen, France
†. Department of Informatics, University of Oslo, 0316 Oslo, Norway

Les problèmes de sécurité dans l'e-commerce sont nombreux, en particulier avec les usurpations d'identité et l'authentification de l'utilisateur. Il est alors possible de renforcer la sécurité de ces protocoles par une authentification à deux facteurs, en utilisant par exemple un secret supplémentaire envoyé sur le téléphone mobile du client, comme le fait 3D-Secure.

Cet article présente une méthode alternative pour l'authentification de l'utilisateur basée sur la biométrie. Le système proposé génère un mot de passe à usage unique à partir des empreintes digitales. Les données biométriques ne sont pas directement stockées dans l'appareil, car on considère que les banques souhaitent elles même authentifier leur client. L'objectif est de sécuriser un tel système, ainsi, le mot de passe généré est différent pour chaque transaction afin d'éviter l'attaque par rejeu. Le papier est organisé de la manière suivante. La section 2 est consacrée à un état de l'art sur les solutions d'authentification existantes pour les paiements en ligne. Nous définissons dans la section 3 les exigences de sécurité et de protection de la vie privée auxquelles doit répondre la solution. Dans la section 4, nous présentons le concept OffPAD, un dispositif sécurisé pour assurer la sécurité des transactions M2M (Machine to Machine). Nous présentons dans la section 5 le protocole d'authentification proposé. Enfin, avant de conclure et d'avancer les perspectives de cette étude, la section 6 nous présente les résultats expérimentaux, ainsi qu'une analyse de la proposition en fonction des exigences définies.

2 Architectures de e-paiement

Le protocole SET (Secure Electronic Transactions, [S.E02]), développé par VISA et MasterCard, est un protocole de sécurisation des transactions de paiement électronique par carte de crédit. Dans ce protocole, l'authentification de l'utilisateur est réalisée à l'aide d'un certificat installé sur l'ordinateur du client et contrôlé par la banque du commerçant. Bien que ce protocole soit particulièrement respectueux de la vie privé du client, il a été remplacé par le protocole 3D-Secure du fait de la complexité entraînée par la gestion d'un certificat. Le protocole 3D-Secure développé par VISA en 2001, est ainsi l'actuelle architecture d'authentification et de paiement utilisé sur Internet. Le protocole 3D-Secure est composé de neuf étapes échangés entre cinq acteurs. La principale faille de sécurité des implémentations 3D-Secure, soulignée dans [MA10], a été corrigée par de nombreuses banques. L'authentification du client (Étape 7) à l'aide de sa date de naissance (ou d'autres secrets triviaux) est depuis remplacée par une authentification forte, à savoir l'utilisation d'un mot de passe à usage unique, un OTP (One Time Password), envoyé au téléphone mobile de l'utilisateur. Cependant, bien qu'une authentification à deux facteurs soit désormais utilisée, nous clamons dans cet article que ce schéma n'est pas suffisamment sécurisé et nous proposons ainsi une approche originale utilisant de la biométrie.

3 Exigences de sécurité et de protection de la vie privée

Dans les paiements électroniques, de nombreuses données personnelles sont impliquées et doivent être protégées [AB11]. Quatre acteurs sont principalement présents : Le **client C**, qui possède un OffPAD, veut acheter un service en ligne avec sa carte de crédit par l'intermédiaire du site marchand d'un **fournisseur de service SP**. Le client a un fournisseur de paiement, la **banque émettrice**, de même que le SP avec la **banque acquéreur**. Un cinquième acteur est également souvent impliqué. Il s'agit d'un tiers de confiance,

comme le Directory utilisé dans le protocole 3D-Secure. Le rôle de ce cinquième acteur n'est pas fixe, mais permet généralement d'authentifier les banques. Le protocole proposé se concentre sur l'authentification du client et l'enregistrement du client auprès du SP. Afin d'assurer les principes de protection de la vie privée et la sécurité lors de telles transaction, une liste de dix exigences E_i a été établie. Ces exigences doivent être prises en compte lors de l'étape d'authentification/d'enregistrement du client d'une architecture de e-paiement :

- E_1 : La **confidentialité des transactions** implique que chaque donnée échangée doit être chiffrée afin de protéger ces données contre les entités extérieures.
- E_2 : L'**intégrité des données transmises** permet d'assurer l'exactitude des données et leur non-altération lors de leur transmission ou leur stockage.
- E_3 : L'**authentification du client** par un tiers de confiance assure l'identité du client. En fonction de la situation, l'authentification peut être réalisée à l'aide de données biométriques.
- E_4 : L'**authentification de l'appareil possédé par le client** assure la validité de l'outil avec la bonne application. Cette authentification peut être réalisée à l'aide d'un identifiant de l'outil.
- E_5 : La **preuve de l'appartenance de l'outil au client** assure que l'outil est bien celui du client authentifié.
- E_6 : L'**authentification du SP** par le client ou un tiers de confiance assure l'identité du SP.
- E_7 : L'**authentification des banques** par une partie de confiance assure l'identité de la banque du SP et de la banque du client.
- E_8 : La **non-associabilité** des transactions réalisées permet de ne pas lier les différentes transactions d'un même client.
- E_9 : La **confidentialité des données du client** (ou principe de minimisation des données) assure que seulement les personnes autorisées ont accès à ses informations. Cette exigence inclut le fait que les données biométriques du client ne soient connues ni par les banques, ni par le SP.
- E_{10} : Le **principe de souveraineté des données** implique l'utilisation des données personnelles du client avec son consentement et son contrôle.

4 Concept OffPAD

Le PAD (Personal Authentication Device) est décrit par Jøsang et Pope dans [JP05] comme un dispositif externe sécurisé pour la plate-forme de l'ordinateur du client. Le PAD est le prédécesseur conceptuel d'OffPAD (Offline Personal Authentication Device). Ce dernier est décrit par Klevjer et col. dans [KVJ13] et par Varmedal et col. dans [VKH+13]. Il s'agit d'une version améliorée de PAD, où une caractéristique essentielle est de garantir la sécurité hors ligne. OffPAD représente la gestion locale d'identité centrée sur l'utilisateur. En effet, il permet une gestion facilitée et sécurisée des identités numériques et des informations d'identification du côté de l'utilisateur. OffPAD prend en charge à la fois l'authentification de l'utilisateur et celle du fournisseur de services (authentification mutuelle). De plus, il est capable d'appuyer l'authentification des données. Pour accéder à un OffPAD, l'utilisateur doit déverrouiller l'appareil en utilisant par exemple un code PIN, une passe-phrase, une donnée biométrique ou d'autres informations d'authentifica-

tion appropriées. Une conception possible d'un OffPAD est illustrée par la figure 1.

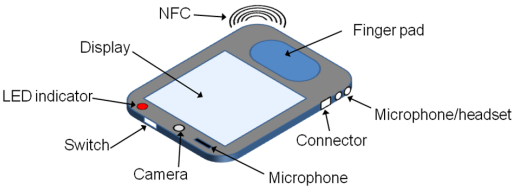

Figure 1: Concept OffPAD

OffPAD est un appareil de confiance doté d'un élément sécurisé. Il a également des connectivités limitées aux plates-formes des clients. Ces canaux de communication doivent donc être soigneusement contrôlés. Le contrôle d'accès traditionnel via code PIN et biométrie, est combiné à un certain niveau de résistance à l'effraction physique qui le protège également contre les attaques résultant d'un vol physique. L'OffPAD peut avoir plusieurs interfaces de communication. Le micro et l'appareil photo peuvent être utilisés pour la voix et la reconnaissance faciale, et un lecteur d'empreintes digitales peut être utilisé à la fois pour l'authentification de l'appareil. L'obligation d'être déconnecté n'exclut cependant pas la communication électronique avec le OffPAD. Ce découplage des réseaux étant moins vulnérable aux agressions extérieures, il permet d'améliorer la sécurité sur l'appareil. Nous utilisons cet outil sécurisé pour notre protocole original lors d'un paiement bancaire électronique. Celui-ci est détaillé dans la section suivante.

5 Protocole d'authentification proposé

Le protocole d'authentification proposé utilise des données biométriques devant être protégées grâce à l'outil OffPAD et des algorithmes de protection du modèle. Ces algorithmes de protection pour des modèles biométriques sont des groupes de technologies incluant les technologies permettant de protéger la vie privée des clients et d'assurer la sécurité du modèle. Par conséquent, toute approche de protection doit offrir la possibilité de révoquer un ensemble de données biométriques dans le cas d'interception, et doit être conçue avec une forte analyse de sécurité. Au vue des différentes solutions présentes dans la littérature, cette protection peut être réalisée en utilisant des systèmes biométriques cryptographiques [JW99] ou en transformant la caractéristique biométrique [RCB01]. Le BioHashing est un protocole bien-connu qui appartient à cette seconde catégorie et qui permet de révoquer un modèle biométrique.

5.1 Algorithme de BioHashing

L'algorithme de BioHashing transforme un vecteur de valeur réelle et de taille n (le FingerCode résultant de la méthode d'extraction) en un vecteur binaire de taille $m \leq n$ (le BioCode). Teoh *et al.* sont les premiers à l'avoir défini dans [TNG04].

Lorsqu'il est appliqué dans un contexte d'authentification, le *BioCode référent* (calculé à partir du FingerCode après l'enregistrement et après avoir présenté le secret) est comparé au *BioCode capturé* (calculé à partir du FingerCode obtenu après une nouvelle capture avec le secret) avec la distance de Hamming. Si cette valeur est inférieure au seuil déterminé

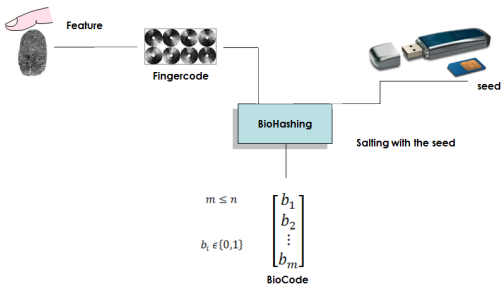

Figure 2: Schéma de BioHashing

par l'administrateur du système, l'identité de l'utilisateur est vérifiée. Ainsi, la première partie de l'algorithme, y compris les produits scalaires avec les vecteurs orthonormés, est utilisée pour les besoins de performance, alors que la dernière étape de l'algorithme est utilisée pour assurer la non-inversibilité de l'algorithme de BioHashing. Comme expliqué dans la suite, l'utilisation d'une graine aléatoire garantit les propriétés de diversité et de révocabilité. Le protocole d'authentification applique alors plusieurs fois l'algorithme de BioHashing, nous le détaillons dans la section suivante.

5.2 Détails du protocole

Le protocole proposé est détaillé avec les empreintes digitales mais peut tout à fait être utilisé avec d'autres modalités biométriques (visage, iris ...). Comme nous utilisons la biométrie, deux grandes étapes sont nécessaires : l'enregistrement et l'authentification.

5.2.1 Enregistrement

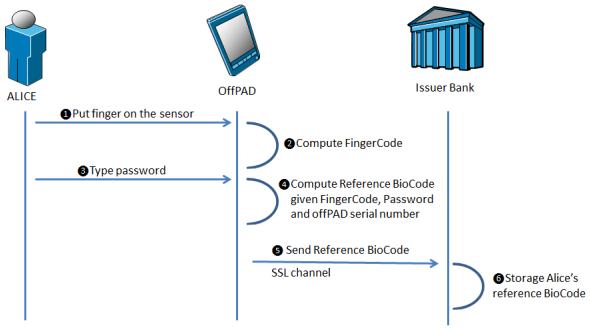

Figure 3: Étape d'enregistrement

Cette étape a pour objectif de recueillir le modèle de référence d'Alice. Dans notre cas, le modèle est donné par un BioCode appelé *BioCode capturé* calculé à partir d'un FingerCode (vecteur caractéristique calculé à partir de l'empreinte digitale) et un secret (le secret de l'utilisateur concaténé avec le numéro de série de l'appareil OffPAD). Le secret de l'utilisateur peut être un mot de passe ou une valeur aléatoire stockée dans le

dispositif OffPAD. Une fois le *BioCode référent* calculé, il est envoyé à la *banque émetteur d'Alice* via un canal SSL. D'un point de vue organisationnel, cette étape peut être réalisée après vérification de l'identité par la personne physique . La Figure 3 détaille le processus d'enregistrement. Le stockage de ce *BioCode référent* par la *banque émettrice* n'est pas un problème en termes de protection de la vie privée étant donné que ce modèle est révocable et que le processus de BioHashing est inversible.

5.2.2 Authentification

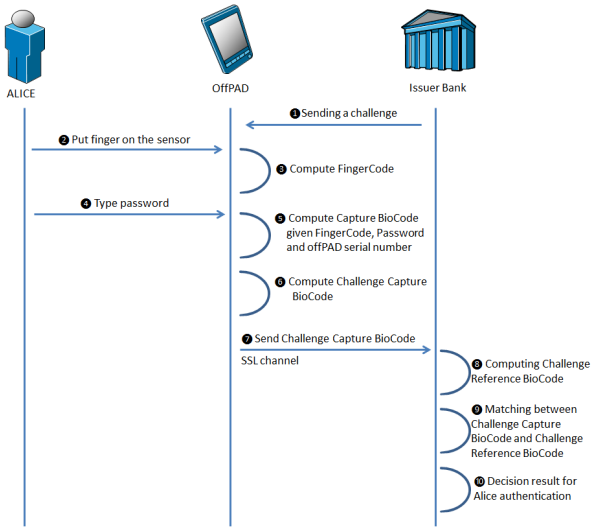

Figure 4: Étape d'authentification

Lors d'un paiement électronique, la *banque émettrice* doit authentifier Alice (par exemple via le protocole 3D-Secure). Un défi est alors envoyé à Alice (numéro affiché sur l'ordinateur ou directement envoyée à son OffPAD). Alice doit ensuite fournir ses empreintes et son mot de passe (qui n'est pas connu par la *banque émettrice*). Un *BioCode capturé* est calculé à partir du FingerCode calculé lui-même en utilisant la capture des données biométriques, le mot de passe et le numéro de série OffPAD. Le *BioCode capturé relatif au défi* est alors calculé en appliquant l'algorithme de BioHashing sur le *BioCode référent*, avec le challenge envoyé par la *banque émettrice* comme secret. La *banque émettrice* calcule également le *BioCode référent relatif au défi* en appliquant l'algorithme de BioHashing sur le *BioCode référent*. La distance de Hamming est utilisé pour effectuer la comparaison de ces deux BioCodes relatifs au défi. Si cette distance est inférieure à un seuil prédéfini, Alice est authentifiée. La Figure 4 détaille l'ensemble du processus. Le défi envoyé par la *banque émettrice* nous permet de définir une solution d'authentification biométrique à usage unique. Nous supposons dans cette solution que l'OffPAD est un dispositif sécurisé et que la *banque émettrice* contrôle la décision sur l'authentification d'Alice.

5.3 Analyse de performance

Dans cette section, nous analysons les performances du protocole à éviter de faux rejets et de fausses acceptations.

5.3.1 Protocole expérimental

Nous avons utilisé trois bases de données d'empreintes digitales, chacune est composée de 800 images de plus de 100 personnes avec 8 échantillons de chaque utilisateur :

- FVC2002 base de données de référence DB2 : la résolution de l'image est 296×560 pixels avec un capteur optique "FX2000" par Biometrika ;
- FVC2004 base de données de référence DB1 : la résolution de l'image est 640×480 pixels avec un capteur optique "V300" par CrossMatch ;
- FVC2004 base de données de référence DB3 : la résolution de l'image est 300×480 pixels avec un capteur de balayage thermique "FingerChip FCD4B14CB" par Atmel.

Ces bases de données ont été utilisées pour les compétitions (concurrence de vérification d'empreintes digitales) en 2002 et 2004. Le tableau 1 présente les performances des meilleurs algorithmes sur ces bases de données. Le taux d'erreur égal (EER) calcule le taux où les erreurs entre les utilisateurs légitimes rejetés à tort et les imposteurs acceptés à tort sont égales. ZeroFMR est la valeur du taux de faux rejets (FNMR, False Non Match Rate). Ces valeurs définissent la complexité de chaque base de données et donnent quelques éléments de performance que nous pouvons attendre de ces bases de données.

BdD	EER	ZeroFMR
FVC2002 DB2	0.14%	0.29%
FVC2004 DB1	0.61%	1.93%
FVC2004 DB3	1.18%	4.89%

Table 1: Performance du meilleur algorithme pour chaque base de données

Comme FingerCode, nous avons utilisé le modèle de Gabor (GABOR) [MM96] de taille $n = 512$ (16 niveaux et 16 orientations). Ces caractéristiques sont très bien connues et permettent une bonne analyse de la texture d'une empreinte digitale. Pour chaque utilisateur, nous avons utilisé le premier échantillon de FingerCode comme modèle de référence. D'autres sont utilisés pour tester le schéma proposé. Les BioCodes sont de taille $m = 256$ bits. Afin de quantifier la performance de notre approche, nous avons calculé $1,000$ comparaisons (avec la distance de Hamming) pour chaque utilisateur entre le BioCode référent relatif au défi et le BioCode capturé relatif au défi. Nous avons obtenu 100.000 scores intra et interclasses pour l'analyse des performances du système proposé.

5.3.2 Résultats expérimentaux

Nous avons appliqué le protocole précédent à la solution d'authentification proposée. Sur les trois bases de données, nous arrivons à une valeur de EER très proche de 0 %. Afin d'illustrer cette efficacité, nous montrons, par la figure 5, la distribution des scores intra et interclasses pour chaque base de données. Nous remarquons clairement qu'il n'y a pas de chevauchement entre les deux distributions et qu'un seuil proche de 60 (ce qui signifie que le nombre de bits différent maximum toléré entre le BioCode capturé et le

référent capture et le BioCode de référence est 60) pourrait être utilisé. Dans la dernière colonne du tableau 2, nous présentons la valeur de l'EER en considérant qu'un imposteur a en sa possession l'appareil OffPAD et le mot de passe de l'utilisateur (le pire des cas). Dans ce cas, l'imposteur peut appliquer l'attaque "zéro effort" en fournissant ses données biométriques afin de se faire passer pour le véritable utilisateur. Nous avons testé 100.000 attaques pour chaque base de données et cette attaque est réussie dans 16% à 25% des cas. Dans les approches classiques (authentification à deux facteurs), cette attaque est toujours couronnée de succès.

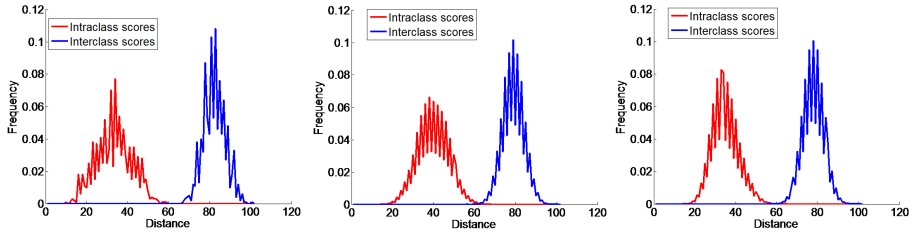

Figure 5: Distribution des scores intra et interclass pour chaque base de données : (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3

BdD	EER sans attaque	EER avec attaque
FVC2002 DB2	0%	25.85%
FVC2004 DB1	0.00093%	23.95%
FVC2004 DB3	0.00023%	16.12%

Table 2: Performance de l'algorithme proposé pour chaque base de données

5.4 Analyse de sécurité et protection de la vie privée

Le protocole proposé est plus respectueux de la vie privée des utilisateurs que le protocole l'authentification du client de 3D-Secure. Nous proposons une analyse du protocole proposé dans cette section.

5.4.1 Sécurité et authentification des données

Le canal sécurisé entre les acteurs, ainsi que les systèmes de chiffrement permettent de garantir la confidentialité des données échangées et l'intégrité des données au cours des transactions. Par conséquent, les exigences E_1 et E_2 sont assurées. L'authentification des entités est également réalisée via le protocole SSL pour la SP (E_6) et les banques (E_7), et par l' authentification forte avec l'algorithme BioHashing pour le client (E_3). De plus, grâce aux défis au cours de l'authentification du client, cette authentification est une solution d'authentification biométrique à usage unique. Par conséquent, les différentes opérations d'un même client ne peuvent être liées. L'exigence E_8 est ainsi garantie. Le dispositif est également authentifié par son numéro de série et une preuve de la propriété de l'appareil du client est fourni. Les exigences E_4 et E_5 peuvent ainsi être assurées. En outre, pour la solution d'authentification du client, le client a uniquement besoin d'utiliser ce qu'il est (données biométriques) et ce qu'il connaît (mot de passe).

5.4.2 Analyse de protection de la vie privée

Au cours de notre processus d'authentification, plusieurs informations sensibles sont échangées et stockées, telles que les données biométriques et le mot de passe du client. Leur stockage ne doit pas être centralisé. Cependant, grâce à l'utilisation de l'algorithme de BioHashing, le modèle est révocable et la connaissance du BioCode n'entraîne donc pas de connaissance concernant les renseignements personnels d'un client. Dans notre cas, la connaissance du BioCode référent n'implique pas la connaissance des données biométriques, les empreintes digitales. Seules les données pertinentes et nécessaires sont envoyées et stockées. Ainsi, le principe de minimisation (E_9) est respecté. De plus, pour chaque authentification d'un client, celui-ci doit présenter son doigt et donner son mot de passe. Ces actions concernent donc le client qui donne sa permission sur l'utilisation de ces données et peut les contrôler grâce aux calculs du BioCode capturé et du stockage du BioCode référent. Le principe de la souveraineté des données (E_{10}) est donc également respecté.

6 Conclusion et perspectives

Nous avons présenté dans cet article un nouveau protocole d'authentification appelé "Biométrie à usage unique" destiné au service bancaire en ligne et à l'authentification lors d'un paiement électronique. Nous avons utilisé deux principales composantes pour cela. La première est un dispositif spécifique, appelé OffPAD, qui assure de nombreuses propriétés en termes de sécurité et de protection de la vie privée. La seconde composante est l'utilisation d'un algorithme de protection du modèle biométrique afin de rendre possible le stockage d'une telle donnée de façon centralisé par la banque émettrice. Un protocole basé sur un défi est ensuite proposé afin d'éviter l'attaque par rejeu. Nous montrons de très bonnes performances sur les trois bases de données de référence d'empreintes digitales et de bonnes propriétés prenant en compte les exigences en termes de sécurité et de protection de la vie privée. Les perspectives de cette étude sont nombreuses. Nous prévoyons d'utiliser plusieurs données biométriques afin d'éviter l'utilisation d'un mot de passe dans le protocole proposé. De plus, un tel protocole pourrait être utilisé dans d'autres cas d'étude. Notons enfin qu'il est possible de rajouter un mécanisme de protection contre les attaques de type *man in the browser* grâce à l'OffPAD.

7 Remerciements

Les auteurs voudraient remercier le programme Eurostars pour l'aide apportée au projet, ainsi que son soutien financier.
`http://www.eurostars-eureka.eu/`

Références

[AADK13] Manal Adham, Amir Azodi, Yvo Desmedt, and Ioannis Karaolis. How to attack two-factor authentication internet banking. In *Financial Cryptography*, 2013.

[AB11] G. Antoniou and L. Batten. E-commerce : protecting purchaser privacy to enforce trust. *Electronic commerce research*, 11(4) :421–456, 2011.

[BCR02] R.M. Bolle, J.H. Connell, and N.K. Ratha. Biometric perils and patches. *Pattern Recognition*, 35(12) :2727–2738, 2002.

[Com00] 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.

[Com07] 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.

[Cou07] European Payments Council. Sepa - single euro payment area, 2007. http ://www.sepafrance.fr/.

[Dau07] J. Daugman. New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B : Cybernetics*, 37(5) :1167–1175, October 2007.

[DMR09] 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.

[ENKH08] 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.

[Int04] MasterCard International. Chip authentication program functional architecture, September, 2004.

[JP05] Audun Jøsang and Simon Pope. User centric identity management. In *AusCERT Asia Pacific Information Technology Security Conference*, page 77. Citeseer, 2005.

[JS02] A. Juels and M. Sudan. A fuzzy vault scheme. In *ISIT*, page 408, 2002.

[JW99] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36, 1999.

[KVJ13] 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.

[LSH+11] 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.

[MA10] 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.

[MC66] Mastercard worldwide, 1966. http ://www.mastercard.com/.

[MM96] 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.

[OPJM10] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. Scifi - a system for secure face identification. In *IEEE Symposium on Security and Privacy*, 2010.

[RCB01] 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.

[RU11] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Information Security*, 3, 2011.

[S.E02] S.E.T. Secure electronic transaction specification. *Book 1 : Business Description. Version*, 1, 2002.

[TNG04] A.B.J. Teoh, D. Ngo, and A. Goh. Biohashing : two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 40, 2004.

[Vis58] Visa corporate, 1958. http ://corporate.visa.com/index.shtml.

[Vis02] Visa. 3D secure protocol specification, core functions, July 16, 2002.

[VKH+13] 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.