HAL
open science

Un pass de transport anonyme et intraçable pour mobile NFC

Ghada Arfaoui, Guillaume Dabosville, Sébastien Gambs, Patrick Lacharme, Jean-François Lalande

To cite this version:

Ghada Arfaoui, Guillaume Dabosville, Sébastien Gambs, Patrick Lacharme, Jean-François Lalande. Un pass de transport anonyme et intraçable pour mobile NFC. Atelier sur la Protection de la Vie Privée 2014, Jun 2014, Cabourg, France. hal-01009516

HAL Id: hal-01009516

https://inria.hal.science/hal-01009516v1

Submitted on 18 Jun 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Un pass de transport anonyme et intraçable pour mobile NFC

G. Arfaoui[1,6], G. Dabosville[2], S. Gambs[3], P. Lacharme[4], J.-F. Lalande[3,5]

[1] *Orange Labs, 14066 Caen*
[2] *Oberthur Technologies, 92700 Colombes*
[3] *SUPELEC/Inria/Univ. Rennes 1, IRISA (UMR 6074), 35042 Cesson Sévigné*
[4] *Laboratoire GREYC (Unicaen, Ensicaen, CNRS), UMR 6072, 14032 Caen*
[5] *INSA Centre Val de Loire, Univ. Orléans, LIFO EA 4022, 18022 Bourges*

Résumé

Cet article présente un titre de transport anonyme et non traçable pour mobile NFC [1]. L'anonymat et la non-traçabilité sont obtenus grâce à un algorithme de signature de groupe utilisé dans un protocole répartissant les calculs entre la carte SIM et le mobile lui-même. La solution obtenue respecte la contrainte pratique des standards de transport actuels qui est que la validation du titre doit être réalisée en moins de 300 ms.

1 Introduction

Avec le déploiement de la technologie NFC dans les smartphones, les services sur mobile telles que le paiement, les cartes de fidélité ou la gestion des titres de transport deviennent de plus en plus fréquents dans notre quotidien [1, 2, 3, 4]. Cependant du point de vue de la vie privée, la plupart de ces applications utilisent ou génèrent de données personnelles sur lesquelles les utilisateurs de ces services n'ont pas de réel contrôle. Ceci est d'autant plus inquiétant que la plupart des smartphones sont à l'heure actuelle vulnérables à des menaces de sécurité comme par exemple l'écoute des communications échangées entre le module NFC du téléphone et un fournisseur de service.

Pour contrecarrer ces risques, il est fondamental de concevoir des versions respectueuses de la vie privée de ces services sans contact. Un simple pseudonyme n'est en général pas suffisant pour garantir l'anonymat d'un utilisateur car les corrélations spatiales et temporelles que possèdent certaines données générées peuvent permettre de briser cet anonymat. Ces services doivent donc aussi garantir la non-traçabilité des utilisateurs. Toutefois afin de pouvoir réconcilier les impératifs de vie privée avec le fait de pouvoir retrouver l'identité d'un utilisateur dans le cas d'une fraude, une solution est d'implémenter une forme d'anonymat révocable (plutôt qu'un anonymat total) qui laisserait la possibilité de dé-anonymiser un utilisateur à partir des traces laissées par ses actions dans des circonstances exceptionnelles, telles que suite à une injonction judiciaire.

1. Ces travaux ont été financés par le projet ANR LYRICS (ANR-11-INS-0013).

Certaines primitives cryptographiques, comme les signatures de groupe [5], permettent d'obtenir un tel anonymat. Bien que ces primitives soient relativement coûteuses, elles sont maintenant à portée des smartphones dont la puissance de calcul devient de plus en plus importante. De plus, ces appareils possèdent une puce qui peut être considérée comme un élément sécurisé comme la carte UICC/SIM [6], et qui permet de stocker et de manipuler de manière sécurisée les clés et autres données.

Dans cet article, nous proposons une solution permettant d'implémenter un pass de transport anonyme et non-traçable, qui se base sur un protocole cryptographique réparti entre un mobile NFC et un élément sécurisé (SIM). De plus, la solution proposée permet la détection de fraude, la levée exceptionnelle de l'anonymat, et respecte les contraintes opérationnelles des services de transport, dont en particulier une validation du titre de transport en moins de 300 ms.

2 Spécification et état de l'art

En 2007, le standard CALYPSO [7] (norme ISO 24014-1 :2007) spécifie les détails de la transaction, de l'achat à l'utilisation de tickets électroniques pour les services de transport sans contact. Un système de ticket ou d'abonnement pour les transports consiste en plusieurs phases. La première phase consiste pour l'utilisateur à installer et personnaliser l'application de transport sur son mobile en fonction de son identité et de manière certifiée (comme le fait d'être étudiant afin d'obtenir une réduction). La seconde phase est l'achat d'un produit lui-même. Par exemple, dans le cas d'un abonnement mensuel cette phase concerne le chargement de ce produit dans l'élément sécurisé du smartphone, éventuellement accompagné des attributs correspondant au produit. Ces attributs ne sont cependant pas vérifiés durant cette phase car le produit pourrait être transféré à une autre personne. La troisième phase consiste à valider l'abonnement lors de l'utilisation du système de transport. Pendant cette phase, l'utilisateur fait interagir son smartphone avec une borne d'entrée qui valide l'abonnement en contrôlant l'authenticité du produit et en autorisant ou non l'entrée à l'utilisateur. Il est possible aussi de maintenir une liste des abonnements révoqués ainsi qu'un mécanisme d'*anti passback* qui prévient la réutilisation d'un même titre de transport sur une courte période. La dernière phase, qui est optionnelle et peut se dérouler à n'importe quel moment pendant le trajet, consiste à contrôler et vérifier la validité du titre de transport pendant le voyage (cette fonctionnalité n'est pas décrite dans cet article).

Plusieurs exemples de titres de transport se voulant comme étant plus respectueux de la vie privée que leurs homologues classiques ont été déployés en Allemagne, au Chili ou à Hong Kong [8, 9, 10]. Les garanties en terme de vie privée offerts par ces systèmes sont très limités car ils sont tous basés sur un pseudonyme, ce qui n'offre donc aucune protection contre la traçabilité des utilisateurs. On trouve aussi dans la littérature plusieurs propositions de solutions de services de ticketing ou d'abonnement respectant la vie privée des utilisateurs qui se basent sur la cryptographie. Cependant là aussi la plupart d'entre eux n'empêchent pas la traçabilité des utilisateurs [11, 12, 13] ou alors ne respectent pas les contraintes pratique de 300 ms pour la phase de validation [14, 15] comme ceux basés sur le protocole de Brands [16, 17] ou sur les signatures de groupe BBS (Boneh-Boyen-Shacham).

En résumé, les objectifs qu'un tel service doit remplir sont multiples puisqu'elle doit combiner des propriétés de sécurité comme l'intégrité et la résistance à la contrefaçon du titre avec de propriétés de respect de la vie privée telles que l'anonymat révocable et la non-traçabilité de l'utilisateur tout en répondant aux impératifs d'efficacité du système, notamment lors de la phase de validation [18]. Au meilleur de nos connaissances, il n'existe à l'heure actuelle aucun système (déployé ou non) qui remplit l'ensemble de ces contraintes.

3 Survol du protocole

Les signatures de groupe ont été introduites par Chaum et van Heyst en 1991 [5] afin de permettre l'anonymat du signataire de telle manière que la signature puisse être vérifiée comme ayant réalisée par un membre valide du groupe mais sans pouvoir identifier son identité précise. Une variante, appelée signature de liste, fournit la non-chaînabilité des signatures sauf si certaines conditions sont remplies, auquel cas il devient possible de chaîner les signatures comme provenant du même membre du groupe mais toujours sans pouvoir dévoiler son identité [19, 20]. Une technique similaire appelée *Direct Anonymous Attestation* (DAA) [21, 22] fournit un anonymat révocable en modélisant le signataire comme deux entités distinctes : une avec une forte puissance de calcul mais dont l'environnement est relativement peu sécurisé et une autre avec des capacités de calcul plus limitées mais située dans un environnement de confiance. Cette approche est particulièrement bien adaptée au contexte des smartphones et le protocole conçu s'inspire directement de ces techniques.

Durant la première phase, l'utilisateur s'enregistre auprès d'une autorité d'enregistrement. Cette autorité pourra aussi agir plus tard comme autorité d'ouverture afin de permettre la levée de l'anonymat de l'utilisateur. Lors de cet enregistrement, deux groupes cycliques additifs sur une courbe elliptique G_1 et G_2 sont choisis dont les paramètres sont rendus publiques. L'utilisateur calcule alors deux mises en gage (C_1, C_2) sur sa clé privée sk_u tels que $C_1 = [sk_u]g_1$ et $C_2 = [sk_u]g_2$ où $g_1 \in G_1$ et $g_2 \in G_2$ sont choisis aléatoirement. L'utilisateur envoie alors ces deux mises en gage à l'autorité. Cette autorité vérifie alors que $e(C_1, C_2) = e(g_1, g_2)$ où e est un couplage bilinéaire de $G_1 \times G_2$ dans un groupe cyclique multiplicatif. Si c'est le cas, cette autorité envoie à l'utilisateur une signature μ de C_1 et stocke le triplet (C_1, C_2, μ) dans une base de données sécurisée.

L'utilisateur peut ensuite s'inscrire auprès de l'autorité de transport en lui envoyant le couple (C_1, μ) où la signature μ est vérifiée avec la clé publique de l'autorité d'enregistrement. L'autorité de transport crée ensuite un certificat CL de type Camenish-Lysyanskaya [22] sur la clé privée de l'utilisateur puis stocke le couple (ID_{user}, C_1) dans sa propre base de données. Si besoin, cette base de données pourra être utilisée en conjonction de celle de l'autorité d'enregistrement afin de lever l'anonymat de l'utilisateur ou de révoquer son titre de transport.

Durant la phase de validation, l'utilisateur doit prouver que son titre de transport est valide mais sans fournir son identité. Un protocole challenge/réponse est ensuite invoqué où le validateur envoie un challenge aléatoire ainsi qu'une donnée fixe à l'utilisateur. Cette donnée fixe peut être par exemple une valeur qui est constante pour un intervalle de temps donné et qui sera utilisée

afin d'assurer le système anti passback. L'utilisateur retourne ensuite une signature de groupe du challenge au validateur qui vérifie si cette signature est valide et non révoquée. Cette signature est composée de plusieurs informations calculées à partir de la clé privée de l'utilisateur sk_u, du certificat CL, ainsi que du challenge et de la donnée anti passback envoyés par le validateur. Une partie de cette signature est pré-calculée dans le smartphone car elle ne demande pas la connaissance des données envoyées par le validateur, alors que le reste de la signature est effectuée par la SIM. C'est justement grâce à ce découpage qu'il est possible de faire la validation en moins de 300 ms.

Finalement, le mécanisme de révocation de l'anonymat permet à l'autorité de transport de retrouver l'identité de l'utilisateur. Cette révocation ne peut se faire qu'avec le consentement de l'autorité d'ouverture. Pour réaliser cette révocation, l'autorité de transport envoie la signature à l'autorité d'ouverture qui retrouve le triplet (C_1, C_2, μ) correspondant stocké dans sa base de données à l'aide d'un calcul de couplage sur la signature. L'autorité d'ouverture retourne alors la donnée C_1 de l'utilisateur à l'autorité de transport qui peut ainsi retrouver l'identité de l'utilisateur.

4 Implémentation

L'architecture générale de notre application est illustrée dans la figure 1. Dans notre implémentation actuelle, l'autorité de transport est une application Tomcat déployée sur un serveur web. Le validateur est simulé par une application Java connectée à un lecteur NFC (protocole ISO 14443B). La cardlet est embarquée dans une carte à puce qui supporte des applications Javacard, elle-même embarquée sur un smartphone Galaxy S3 standard, fonctionnant sous Android 4.1.2.

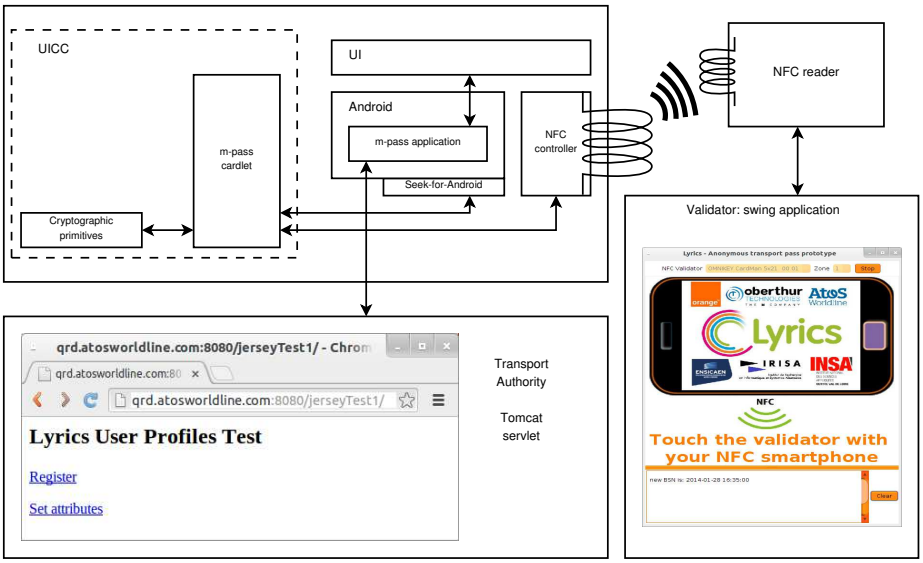

FIGURE 1 – Architecture générale du prototype

Phase du protocole	Temps mesuré
Sélection de la cardlet	12 ms
Signature de la cardlet	140 ms
Vérification	34 ms
Temps de transaction total	186 ms

Table 1 – Temps d'exécution du prototype

La carte à puce utilisée dans le prototype est une Javacard se basant sur des APIs permettant de réaliser de manière efficace des calculs d'arithmétique entière et modulaire, mais aussi des multiplications scalaires et des additions de points de courbes elliptiques, afin d'accélérer la phase de validation du titre, comme présenté dans la table 1. La vérification de la signature est ici très rapide car elle est effectuée sur un PC standard : le temps de validation total, incluant l'anti passback, est de 186 ms, respectant la contrainte des 300 ms. La validation du titre peut même être effectué mobile éteint, la carte SIM étant alimentée par le champ magnétique de la connexion NFC.

5 Conclusion

Dans cet article, nous avons proposé une solution pour mobile NFC permettant d'implémenter un pass de transport assurant des propriétés de vie privée telles que l'anonymat et la non-traçabilité. Cette solution se base sur un protocole cryptographique permettant de valider son titre de transport sans risquer d'être identifié ou tracé. L'implémentation actuelle du prototype fonctionne en moins de 300 ms ce qui démontre la faisabilité de l'approche.

Références

[1] Stefano Levialdi Ghiron, Serena Sposato, Carlo Maria Medaglia et Alice Moroni : NFC ticketing : A prototype and usability test of an NFC-based virtual ticketing application. *In 2009 First International Workshop on Near Field Communication*, pages 45–50, Hagenberg, Austria, février 2009. IEEE Computer Society.

[2] Gerald Madlmayr et Peter Kleebauer : Secure communication between web browsers and NFC targets by the example of an e-ticketing system. *In* Giuseppe Psaila et Roland Wagner, éditeurs : *9th International Conference on E-Commerce and Web Technologie*, pages 1–10, Turin, Italy, septembre 2008. Springer Berlin / Heidelberg.

[3] Smart Card Alliance : Proximity mobile payments : Leveraging NFC and the contactless financial payments infrastructure, 2007.

[4] Ann Cavoukian : Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private. Rapport technique, Information and Privacy Commissioner, Ontario, Canada, 2011.

[5] David Chaum et Eugène van Heyst : Group signatures. *In* Donald W. Davies, éditeur : *EUROCRYPT*, volume 547 de *Lecture Notes in Computer Science*, pages 257–265, Brighton, UK, 1991. Springer.

[6] Business Wire : Oberthur technologies' dragonfly NFC SIM card certified by mastercard and visa, May 2013.

[7] Calypso Networks Association : Calypso handbook v1.1, 2010.

[8] M. Pirker et D. Slamanig : A framework for privacy-preserving mobile payment on security enhanced arm trustzone platforms. *In 11th International Conference on Trust, Security and Privacy in Computing and Communications*, pages 1155–1160, Liverpool, United Kingdom, June 2012. IEEE Computer Society.

[9] Business Wire : Oberthur technologies' contactless payment solution selected by movistar chile and banco santander chile, September 2013.

[10] Sony Corp. Info : Mobile payment services using nfc sims equipped with sony felica™ technology to begin in hong kong, October 2013.

[11] Sandeep Tamrakar, Jan-Erik Ekberg et N. Asokan : Identity verification schemes for public transport ticketing with nfc phones. *In The sixth ACM workshop on Scalable trusted computing*, STC '11, pages 37–48, Chicago, IL, USA, 2011. ACM.

[12] Sandeep Tamrakar et Jan-Erik Ekberg : Tapping and tripping with nfc. *In* Michael Huth, N. Asokan, Srdjan Čapkun, Ivan Flechais et Lizzie Coles-Kemp, éditeurs : *Trust and Trustworthy Computing*, volume 7904 de *Lecture Notes in Computer Science*, pages 115–132. Springer Berlin Heidelberg, London, United Kingdom, 2013.

[13] Jan-Erik Ekberg et Sandeep Tamrakar : Mass transit ticketing with NFC mobile phones. *In* Liqun Chen, Moti Yung et Liehuang Zhu, éditeurs : *Trusted Systems*, volume 7222 de *Lecture Notes in Computer Science*, pages 48–65. Springer Berlin Heidelberg, Beijing, China, 2012.

[14] David Derler, Klaus Potzmader, Johannes Winter et Kurt Dietrich : Anonymous ticketing for NFC-enabled mobile phones. *In* Liqun Chen, Moti Yung et Liehuang Zhu, éditeurs : *The Third International Conference on Trusted Systems*, volume 7222, pages 66–83, Beijing, China, 2011. Springer Berlin Heidelberg.

[15] Andreu Pere Isern-Deyà, Arnau Vives-Guasch, Macià Mut Puigserver, Magdalena Payeras-Capellà et Jordi Castellà-Roca : A secure automatic fare collection system for time-based or distance-based services with revocable anonymity for users. *The Computer Journal*, 56(10):1198–1215, avril 2012.

[16] Stefan Brands : *Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy.* MIT Press, Cambridge, 2000.

[17] Ariel Glenn, Ian Goldberg, Frédéric Légaré et Anton Stiglic : A description of protocols for private credentials. *IACR Cryptology ePrint Archive*, 2001:82, 2001.

[18] Macià Mut-Puigserver, M. Magdalena Payeras-Capellà, Josep-Lluís Ferrer-Gomila, Arnau Vives-Guasch et Jordi Castellà-Roca : A survey of electronic ticketing applied to transport. *Computers & Security*, 31(8):925–939, novembre 2012.

[19] Sébastien Canard et Jacques Traoré : List signature schemes and application to electronic voting. *In International Workshop on Coding and Cryptography (WCC'03)*, Versaille, France, 2003.

[20] Sébastien Canard, Berry Schoenmakers, Martijn Stam et Jacques Traoré : List signature schemes. *Discrete Applied Mathematics*, 154(2):189–201, 2006.

[21] Ernie Brickell, Jan Camenisch et Liqun Chen : Direct anonymous attestation. *In ACM Conference on Computer and Communications Security*, CCS '04, pages 132–145, Washington, DC, USA, 2004. ACM.

[22] Jan Camenisch et Anna Lysyanskaya : Signature schemes and anonymous credentials from bilinear maps. *In* Matt Franklin, éditeur : *Advances in Cryptology - CRYPTO 2004*, volume 3152 de *Lecture Notes in Computer Science*, pages 56–72. Springer Berlin Heidelberg, 2004.