Contrôler la divulgation de ses données de transport

Jacques Traoré
Orange Labs
07 novembre2016

Agenda

- Contexte
- Problématique et verrous à lever
- Outils cryptographiques
- Résultats obtenus
- Démonstrateurs
- Conclusion

1 Contexte

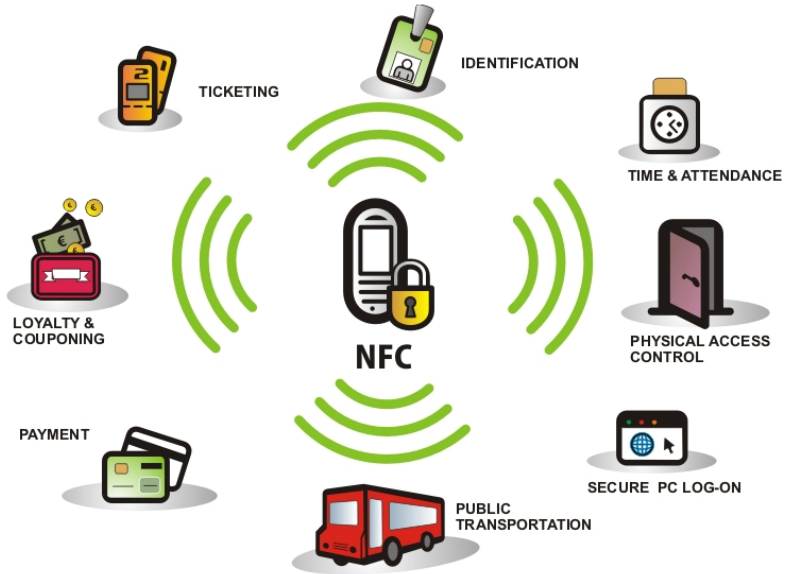
Services Mobiles sans Contact

Contexte

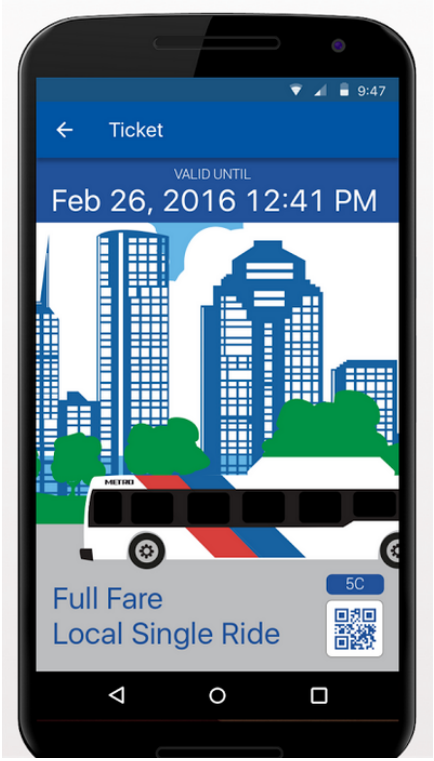
- Développement croissant des services mobiles sans contact (SMC) qui posent des risques importants en termes de possibilités de traçage et de protection de la vie privée.
- Révision et **renforcement de la directive européenne** sur la protection des données personnelles.

Problématique à résoudre

- Permettre à un individu d'utiliser des services mobiles sans contact tout en lui offrant des garanties fortes en termes de sécurité et de protection de la vie privée.
- Respecter les principes fondamentaux en matière de protection de la vie privée : **minimisation des données** et **souveraineté des données**.



Contexte



- Juniper: 32 billion purchases of transit, event and other tickets by 2019

- **Île-de-France:** « Valérie Pécresse annonce la fin du ticket de métro parisien d'ici **2021** »*

- EU General Data Protection Regulation ⇒ **data minimization**

- MoBIB card – Belgian **Big Brother award 2012**

- "Hong Kong e-payment firm admits **selling customer data**" (ZDNet 07/2012)

***Source**://www.nextinpact.com/news/99961

Dématérialisation des titres de transport

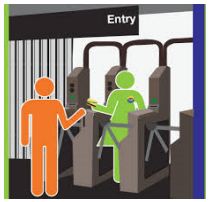
- Carte d'abonnement : 

- Carnet de tickets : 
- Porte-monnaie électronique dédié : (Londres, Washington,…) 

- Porte-monnaie électronique "universel" : (Séoul, Hong-Kong,…) 

Cahier des charges

- Exigences de sécurité / privacy :
  - Inforgeabilité du titre de transport
  - Anti pass-back (respect des conditions d'utilisation de la carte)
  - Minimisation des données



- Exigences fonctionnelles :
  - validation du titre de transport : **< 300 ms**
  - fonctionnement du service batterie off ou mobile éteint
  - Statistiques possibles (nbre de rames de métro à prévoir)
  - Post-paiement des titres de transport* (facturation selon la consommation)

*see Valérie Pécresse recent statement to the press: « des Navigo « anonymes » et une facturation selon la consommation » **Source**: http://www.nextinpact.com/news/99961

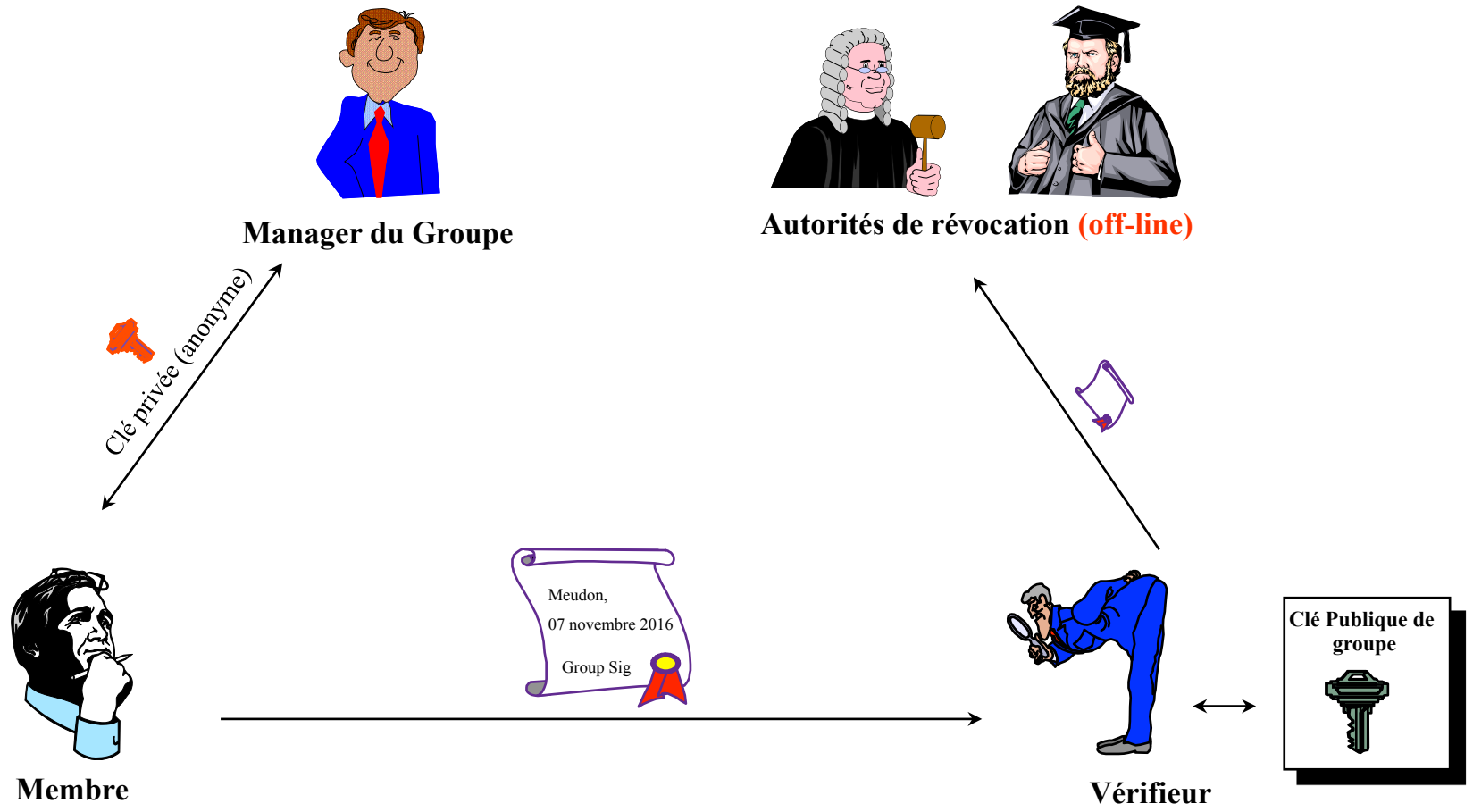
2 Les outils

Signatures de groupe

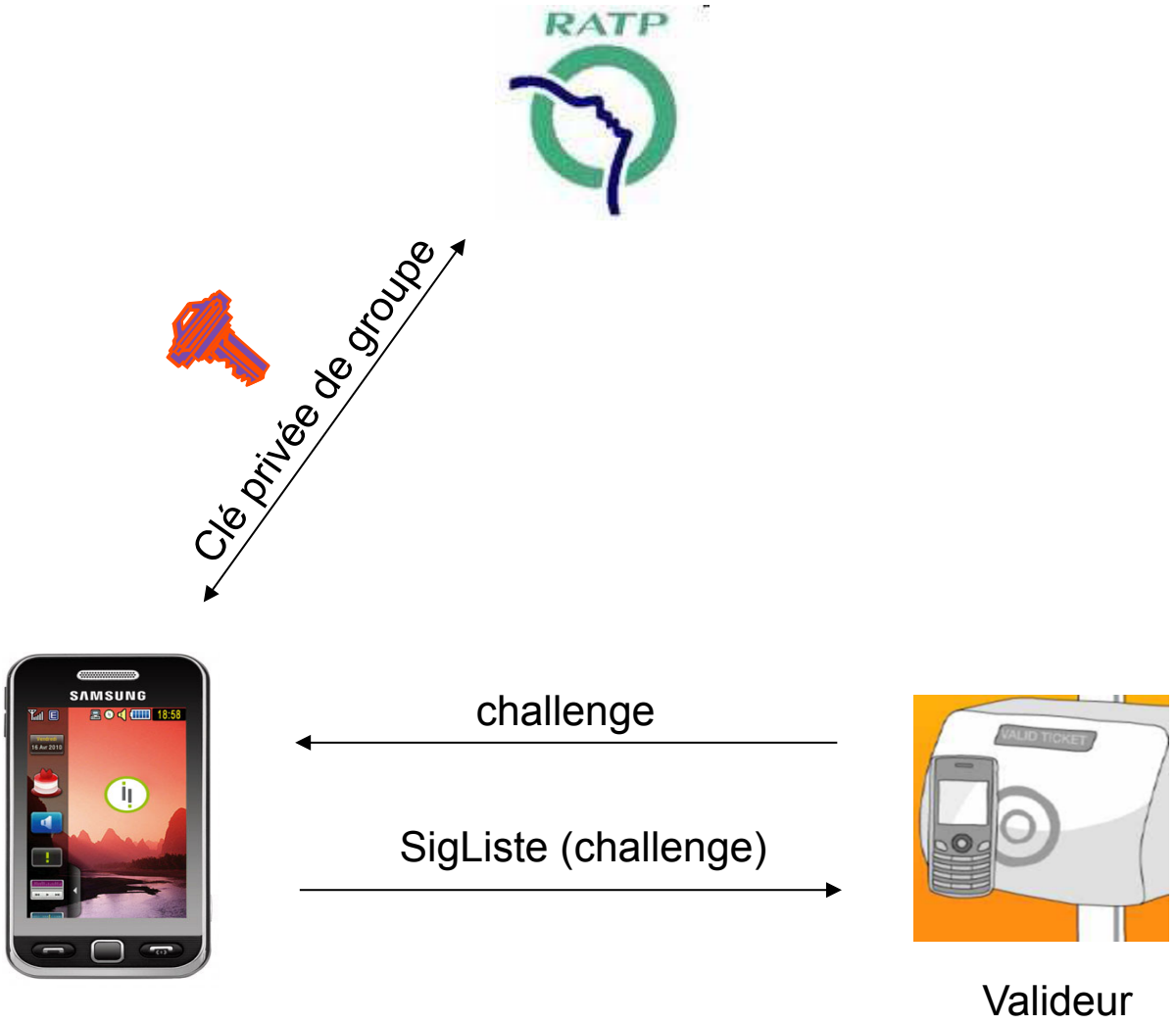
- concept introduit par Chaum et van Heyst en **1991**
- mécanismes normalisés à l'ISO SC27 WG2
- en résumé:
  - chaque membre du groupe peut signer des messages au nom du groupe
  - n'importe qui peut vérifier la validité d'une signature
  - les signatures de groupe sont anonymes et intraçables
  - seule une autorité de confiance a le pouvoir de révoquer l'anonymat de l'auteur d'une signature

- variante : signatures de liste = signatures anonymes mais traçables

Principe de fonctionnement



Application au Passe Navigo Anonyme



Verrous et Innovations

Principaux verrous

- Limitation des capacités de calcul des SIM NFC qui restreint la possibilité d'utiliser l'arsenal complet de la « cryptographie pour la privacy » :
  - La génération d'une signature RSA 2048 bits nécessite 2s
  - La génération d'une signature de groupe nécessite plus de 20 s !!!
- Difficulté d'implémenter des mécanismes permettant de révoquer l'anonymat d'un individu en cas d'utilisation frauduleuse qui « passe à l'échelle ».

Innovation

- Développement de méthodes cryptographiques pour le respect de la vie privée adaptées aux capacités restreintes des SIM NFC : de 20 s à moins de 300 ms !
  - Optimisation des protocoles de signatures de groupe et de leurs variantes
  - Pré-calculs effectués par la carte SIM
  - Délégation des calculs non-sensibles effectués par la SIM au téléphone mobile

SIM, sécurisée mais peu puissante

Mobile, puissant mais peu sécurisé

Lecteur NFC

3 Démonstrateurs

Passe Navigo Anonyme

- Le **passe LYRICS** consiste en un passe de transport, intégré à un mobile/ SIM NFC, anonyme et intraçable lors de son usage :

- Le service proposé est conforme au cahier des charges établi par les opérateurs de transports en commun :
  - contrôle de la validité du titre de transport effectué en moins de 300 ms
  - fonctionne y compris lorsque le mobile est éteint ou lorsque sa batterie est déchargée
  - mise en oeuvre d'un dispositif anti pass-back

- Mécanismes cryptographiques sous-jacents en cours de normalisation à l'ISO SC27 WG?

Porte-monnaie électroniques

- **Oyster Card intraçable** :
  - porte-monnaie électronique dédié, intégré à une SIM NFC
  - système **prouvé sûr** (PETS 2015, Financial Crypto 2016)
  - **pratique** : transactions anonymes et intraçables, inférieures à 300 ms
  - **user-friendly** : post-paiement, fonctionne y compris lorsque le mobile est éteint ou que sa batterie est déchargée

- **TrustID Wallet :**
  - porte-monnaie électronique universel, intégré à une SIM NFC
  - système **prouvé sûr** (PKC 2015, ACNS 2015)
  - **pratique** : transactions anonymes et intraçables, complètement off-line, inférieures à **500 ms**
  - **user-friendly** : pas d'appoint, ni de rendu de monnaie, fonctionne y compris lorsque le mobile est éteint ou que sa batterie est déchargée
  - résolution d'un problème ouvert en cryptographie depuis 30 ans

Retombées - Valorisation

- **Dissémination :**
  - NFC World Congress 2013
  - Salon Cartes 2012 et 2013
  - Nombreux articles dans la presse spécialisée sur le projet Lyrics et sa solution de « passe de transport anonyme » : Capital, 01net, WebWire, etc.
- **Normalisation :** adoption de certains de nos mécanismes cryptographiques pour la privacy à l'ISO :
  - ISO/IEC 20008-2 - Anonymous digital signatures – Part 2: Mechanisms using a group public key
  - ISO/IEC 18370 - Blind digital signatures
- **Publications** de nos résultats dans les conférences majeures en cryptographie appliquée et privacy (PKC, ACNS, PETS, Financial Crypto, SAC, etc.).
- **Retombées :**
  - contribution à l'émergence de nouveaux services sûrs et respectueux de la vie privée
  - diffusion plus large des résultats grâce à la participation de NEC et Microsoft

Annexes

Fiche signalétique

- **LYRICS : L**ightweight privac**Y**-enhancing c**R**yptography for mob**I**le **C**ontactless **S**ervices
- Labellisé par trois pôles de compétitivité (TES, SCS et System@tic)
- **Consortium** : Orange Labs (chef de file), Atos Worldline, Oberthur Technologies, Microsoft, NEC Corporation, *CryptoExperts*, ENSICAEN, INSA Centre Val de Loire, Université de Nanterre et Université de Rennes 1
- Durée : 40 mois (février 2012 – mai 2015)
- Coût : environ **2620 K€** (montant de l'aide 913 k€)
- Site Web : http://projet.lyrics.orange-labs.fr/

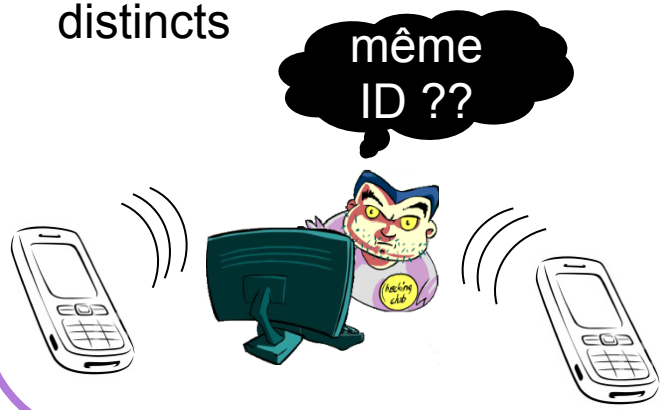
Anonymat et intraçabilité

Respect de la vie privée (dans notre contexte)

anonymat ⟷ intraçabilité

- étant donné une signature
- il est impossible en pratique de déterminer quel membre du groupe l'a émise

- étant donné deux signatures
- il est impossible en pratique de déterminer si elles ont été émises par le même membre ou par deux membres distincts

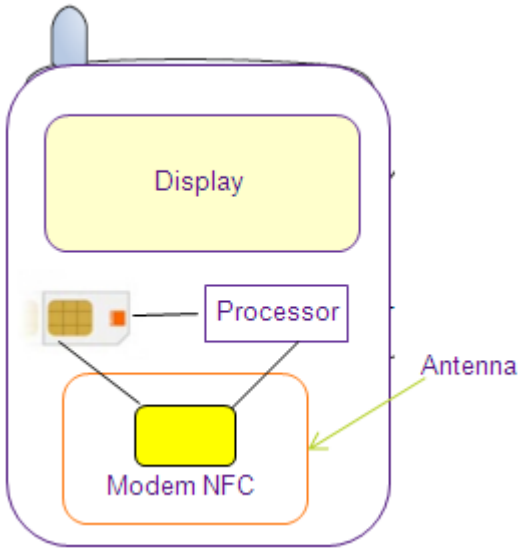


Verrous techniques

- Librairies cryptographiques embarquées sur cartes SIM
  - Seuls les algorithmes classiques de la cryptographie sont fournis nativement :
    - cryptographie symétrique (3DES, AES)
    - cryptographie asymétrique (RSA, DSA, ECDSA)

- Implémentation de nouveaux algorithmes cryptographiques
  - Les développeurs n'ont pas accès aux API mathématiques de bas niveau
    - arithmétique modulaire
    - opérations sur courbes elliptiques
  - Collaboration avec les encarteurs est nécessaire
  - Evolution de JavaCard

- Performances des cartes SIM
  - La génération d'une signature RSA 2048 bits nécessite 2s
  - La génération d'une signature de groupe nécessite plus de 20 s !!!
  - La validation d'un titre de transport doit être réalisée **en moins de 300 ms !**



SIM/UICC centric solution

Optimisations des signatures de groupe

- Comment passer de 20s à moins de 300 ms ?