



**SOLUTIONS
COMMUNICANTES
SECURISEES**
PÔLE DE COMPETITIVITE MONDIAL



LYRICS

SÉCURITÉ ET RESPECT DE LA VIE PRIVÉE DANS LE CONTEXTE DES SERVICES MOBILES SANS CONTACT

> LES OBJECTIFS

L'objectif principal du projet LYRICS est de permettre aux utilisateurs de mobiles NFC d'utiliser en toute sécurité des services dématérialisés sans contact tout en garantissant le respect de leur vie privée. Cet objectif sera réalisé dans le contexte de l'appropriation sociale d'innovations technologiques et de services.

> LES AVANTAGES

Dématérialisation et utilisation sécurisée de pièces justificatives utilisées dans la vie de tous les jours comme les tickets électroniques, les cartes d'abonnement, les cartes de crédit / de fidélité, les badges d'accès, les permis de conduire, etc



Les smartphones vont dans un avenir proche permettre de gérer les transactions de la vie quotidienne (transport, paiement, etc.) grâce à la technologie sans contact NFC (Near Field Communication). Le projet Lyrics vise à fournir des solutions de protection de la vie privée pour l'utilisation de ces services sans contact.

> LES LIVRABLES

- Fournir une architecture globale ouverte pour des services sans contact préservant la vie privée;
- Concevoir et spécifier des mécanismes cryptographiques innovants, à bas coûts, et préservant la vie privée des utilisateurs;
- Implanter ces algorithmes cryptographiques sur des smartphones munis de puces NFC;
- Réaliser un démonstrateur d'un service mobile sans contact mettant en œuvre ces technologies de protection de la vie privée.



SOLUTIONS COMMUNICANTES SECURISEES

PÔLE DE COMPETITIVITE MONDIAL



> LES BRIQUES TECHNOLOGIQUES

Conception d'un ensemble de mécanismes cryptographiques innovants, adaptés aux contraintes (mémoire, puissance de calcul) des smartphones et des cartes SIM munis de la technologie NFC. Ces mécanismes permettront aux utilisateurs de minimiser les données personnelles transmises lors de transactions sans contact, et de répondre ainsi au principe fondamental de minimisation des données.

> LES MARCHÉS VISÉS

Les marchés adressés par le projet LYRICS sont extrêmement variés.

Les mécanismes cryptographiques implémentés de façon robuste et efficace dans la carte SIM du smartphone permettront de transformer ce dernier en véritable moyen pour prouver, de façon dématérialisée et respectueuse de la vie privée, des faits et/ou des droits (j'ai plus de 18 ans et j'ai un billet valide par exemple). On peut imaginer qu'à terme tout ce qui est carte, autorisation ou billet aura disparu physiquement de notre quotidien pour être inséré dans la carte SIM de notre smartphone.

> ILS PARLENT DU PROJET



« Nine companies and academic institutions, including France Telecom, Microsoft and NEC, have formed a consortium to develop a means of providing anonymous authentication for users of smartphones using contactless services. The consortium, called LYRICS (Lightweight privacy-enhancing cRyptography for mobile Contactless Services) wants to research technology that could confirm access privileges while protecting the anonymity of users and devices. LYRICS intends to provide an open, general-purpose architecture for privacy-preserving contactless services and a set of cryptographic mechanisms for implementing and deploying these services on NFC-enabled mobile phones. »

*Extrait de l'article « Lyrics consortium formed to research anonymous contactless authentication »
MOBILE EUROPE - 26 March 2012*

> LE CONSORTIUM

- Porteur du projet : Orange Labs
- Entreprises : Atos Worldline, Microsoft, NEC Corporation, Oberthur Technologies.
- Recherche / Académiques : ENSI de Bourges, ENSI de Caen, IRISA (Université de Rennes 1), MoDyCo (Université de Paris X).

> PROJET FINANCÉ PAR

