

La communication NFC progresse

Beaucoup de smartphones modernes sont équipés de la technologie NFC (Near Field Communication). La NFC ou communication « en champ proche » c.-à-d. à courte distance, permet de transmettre des informations entre un téléphone et d'autres appareils NFC tels que des téléphones, des systèmes de paiement ou de contrôle d'accès NFC. Mais il est possible, grâce à la NFC, de partager, par exemple, des adresses mail, des contacts, des numéros de téléphone, des fichiers de musique, des vidéos ou des photos.

Selon le bureau d'études de marché américain ABI Research, le nombre d'appareils utilisés dépassera en 2015 les 500 millions. Le bureau d'analyse Gartner pense que la NFC ne sera banalisée qu'en 2016. Il devrait y avoir à cette date un marché de 448 millions d'utilisateurs qui paieraient collectivement 617 milliards de dollars via la NFC. De nombreux fournisseurs éminents d'accès mobile dans le monde, réunis au sein de l'organisation mondiale GSM Association (GSMA), ont déclaré soutenir l'utilisation de la technologie NFC. La GSMA attend, pour 2015, 110 milliards d'euros de paiements via des puces NFC implantées dans des mobiles. Bref, les attentes autour de la NFC sont élevées. C'est pourquoi, entre autres, un certain nombre d'éminents acteurs s'étaient précédemment groupés dans un forum NFC. Il faut ainsi des fabricants de puces NFC; les opérateurs de téléphonie mobile doivent adapter leurs réseaux, et il faut aussi des fabricants de matériels et des créateurs de logiciels. Bref, une équipe hétéroclite d'environ 170 intervenants ayant pour objectif de promouvoir l'utilisation de la technologie NFC dans l'électronique grand public et les appareils et PC mobiles. Vers 2004, le forum NFC, qui regroupe entre autres Philips, Sony, NXP, Nokia mais aussi VISA et Mastercard, a développé et normalisé la technologie Near Field Communication. Ces dernières années, ils ont été rejoints par les fabricants de systèmes de contrôle d'accès, mais nous en parlerons par la suite. La puce NFC apparaît sous différentes formes. Il existe des puces individuelles montées dans les appareils. À la demande de la GSMA, il a été développé en outre la possibilité d'intégrer une puce NFC à une carte SIM. Ceci permet d'augmenter la sécurité. Le but de

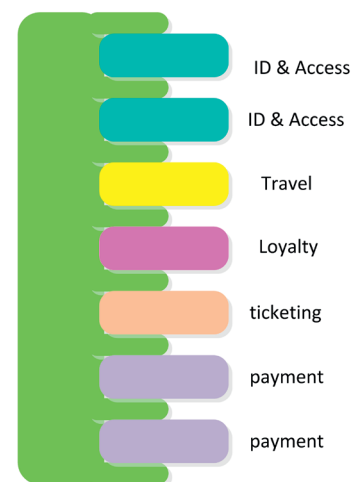
la puce NFC est d'assurer une communication bidirectionnelle sans contact entre deux appareils qui ne sont pas éloignés l'un de l'autre de plus de 10 cm. NFC utilise la bande de fréquence ISM à 13,56 MHz et possède une vitesse de 212 kilobits par seconde. La puce NFC peut fonctionner dans trois états différents:

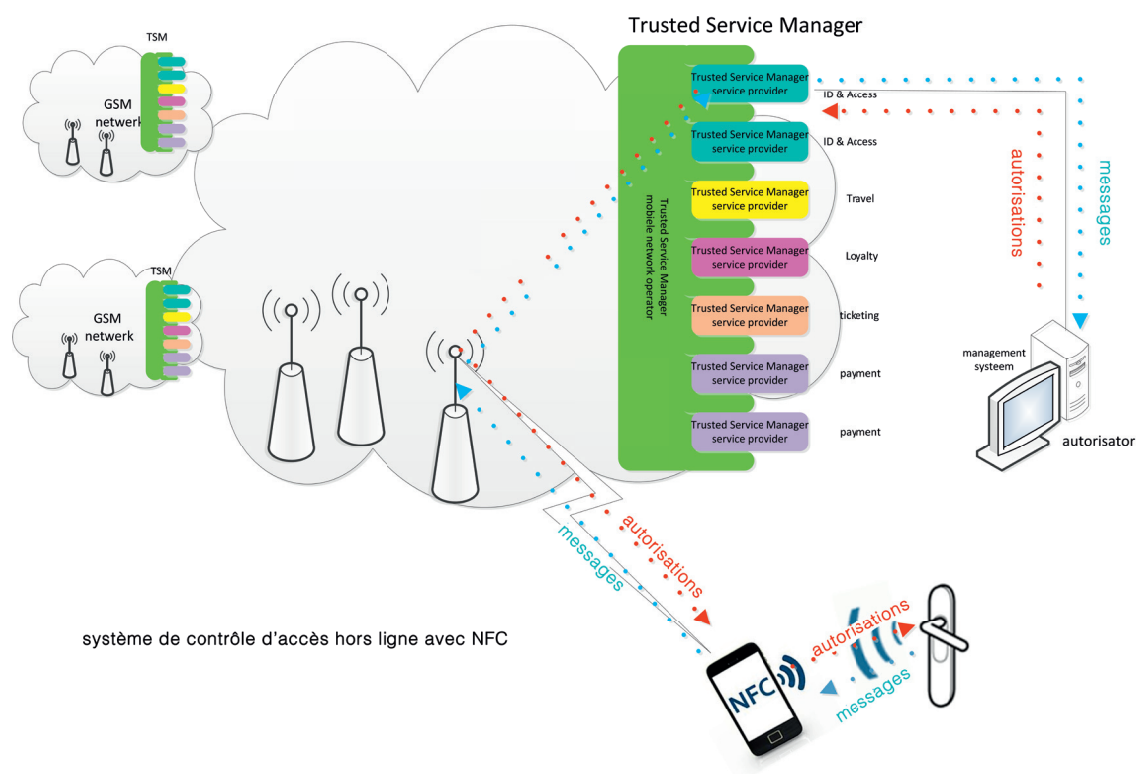
- mode émulation carte dans lequel la puce NFC se comporte comme une carte à puce sans contact,
- le mode lecture/écriture dans lequel l'appareil NFC se comporte comme un lecteur capable de lire ou d'écrire sur des tags NFC,
- mode poste à poste dans lequel il est possible pour deux appareils NFC de communiquer (par exemple, échange de cartes de visite ou autre transmission restreinte de données).

Comme décrit ci-dessus, la puce NFC peut se comporter comme une carte à puce sans contact. Le logiciel permet à la puce NFC d'émuler une carte MIFARE. MIFARE est la carte à puce sans contact la plus utilisée au monde et une marque commerciale de NXP Semiconductors. La technologie est basée sur la norme ISO 14443 Type A 13.56 MHz pour carte à puce sans contact. MIFARE accepte de nombreux dialectes tels qu'Ultra, Classic / Standard, Plus, DESFire, ProX, SmartMX, DESFire EV1. Les plus utilisés d'entre eux sont Classic, DESFire et DESFire EV1. MIFARE est utilisé dans plus d'un milliard de cartes à puce et dix millions de lecteurs. Les sociétés de cartes de crédit telles que VISA et Mastercard utilisent ainsi la norme MIFARE DESFire EV1 et la puce OV fonctionne avec MIFARE Classic. De nombreux systèmes de contrôle d'accès fonctionnent sur la base de MI-

FARE Classic. Pour que la technologie de carte MIFARE fonctionne convenablement en NFC, il est indispensable de définir une norme. Partant de ce principe, le groupe MIFARE4mobile Industry Group, composé de sept acteurs de renom de la scène NFC, a décidé de développer la norme MIFARE-4Mobile. L'un des objectifs de cette norme MIFARE4Mobile est de mettre au point des spécifications pouvant être utilisées pour la gestion des applications à base de puces MIFARE dans les appareils mobiles tels que les smartphones. MIFARE4Mobile offre aux fabricants d'appareils et opérateurs de mobiles, et donc aussi aux développeurs d'applications, un seul interlocuteur technologique (API) pour l'utilisation de la communication NFC. MIFARE4Mobile est compatible avec trois dialectes MIFARE: Classic, DESFire et DESFire EV1.

Trusted Service Manager





système de contrôle d'accès hors ligne avec NFC

Le Trusted Service Manager

Comme déjà dit, il faut pour faire fonctionner la NFC, des modifications au niveau des réseaux GSM. Pour que l'écosystème NFC fonctionne convenablement, il faut une assise mondiale. Les réseaux GSM doivent ainsi être équipés d'un « Trusted Service Manager (TSM) » et il doit y avoir une possibilité d'itinérance entre réseaux. Un certain nombre de fabricants de TSM sont présents au sein du forum NFC précité. Ils jouent un rôle important car le TSM est un élément crucial de l'écosystème NFC. Le TSM est un intermédiaire neutre, facilitant les relations entre le prestataire de services et les opérateurs de réseau mobile. Le TSM permet aux prestataires de services de distribuer et de gérer à distance leurs services, présents sur la puce NFC en tant que logiciels. Le TSM facilite la distribution et la gestion des applications qui se trouvent sur un élément du GSM. Les fonctions les plus importantes d'un TSM sont les suivantes:

- interconnecter les opérateurs de réseau et les prestataires de services,
- faciliter la sécurité de bout en bout,
- gérer le cycle de vie,
- développer de nouveaux utilisateurs,
- faciliter le téléchargement d'applications

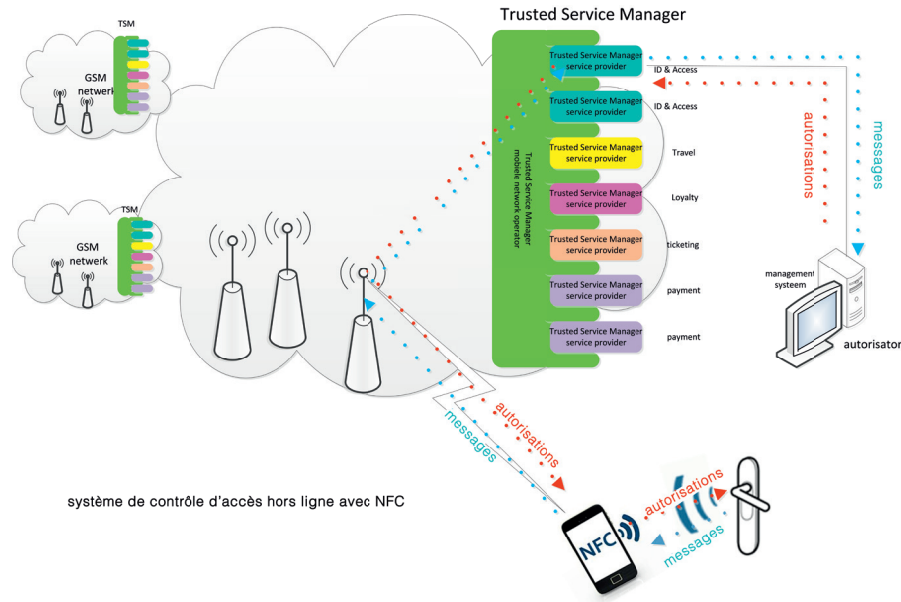
- Over-The-Air (par voie hertzienne),
- personnaliser les applications Over-the-air (ou OTA),
- activer/désactiver des services,
- mettre à jour l'interface utilisateur,
- gérer la base de données NFC du client,
- mettre à jour des compteurs de paiement et de journalisation (logging),
- faciliter les services à valeur ajoutée tels que la billetterie, le contrôle d'accès, le paiement etc.

Sur le plan de la composition interne, un TSM comprend un domaine réservé au prestataire de services et un autre réservé à l'opérateur de réseau. Plusieurs prestataires de services peuvent être raccordés aux TSM de différents opérateurs de réseau est donc essentielle. En outre, plus il y a de TSM interconnectés, mieux l'écosystème NFC fonctionne.

Systèmes de contrôle d'accès

La gestion des accès est impérative dans de nombreuses situations : Les immeubles de bureaux, les centres de données et les parkings n'en sont que quelques exemples. L'objectif principal d'une bonne gestion des accès est l'organisation adéquate et convi-

viale de l'accessibilité à un terrain, un bâtiment ou un local. L'attribution et la gestion de clés sont souvent source de tracas. La NFC peut représenter une solution dans ce cas. Une puce NFC peut, via une liaison sans fil Over-The-Air (ou OTA) être commutée en mode émulation carte, grâce auquel la puce NFC se comporte comme une carte intelligente sans contact, et MIFARE4Mobile permet d'assurer la compatibilité de MIFARE Classic, DESFire et DESFire EV1. La technologie NFC peut être utilisée pour un contrôle d'accès en ligne ou hors ligne. Les systèmes hors ligne sont des contrôles d'accès fonctionnant de manière indépendante, l'autorisation étant donnée par le lecteur hors ligne. Les lecteurs hors ligne ont leur propre intelligence et accordent l'accès de façon autonome, sur la base d'autorisations intégrées. Le lecteur hors ligne comprend alors l'unité de lecture par elle-même, une batterie fournissant les tensions d'alimentation, ainsi qu'une unité de traitement simplifiée. Les lecteurs hors ligne existent en différents modèles : intégré à la garniture de porte, lecteur de carte indépendant, mais aussi comme serrure encastrée. Avec les lecteurs hors ligne il n'est pas nécessaire d'installer une liaison câblée complémentaire; les frais de câ-



blage sont donc inexistantes (alim. 230 V et données). Avec de nombreux systèmes de contrôle d'accès, les autorisations relatives à tous les détenteurs de carte sont inscrites sur le badge à l'aide d'un logiciel. Ceci se fait souvent via un lecteur dit « de mise à jour ». Lorsque le badge est présenté à un lecteur hors ligne, la carte est lue en totalité et les autorisations sont stockées dans la mémoire du lecteur. Les autorisations sont ainsi diffusées sur tous les lecteurs hors ligne du système. Cette même plage de communication, permet aux lecteurs hors ligne d'envoyer des messages au système de gestion. (il y a lieu d'intégrer à ce niveau non seulement des messages de connexion et d'état, mais aussi de batterie faible.) Ne pas oublier qu'avec un système hors ligne, les badges d'accès doivent malgré tout être distribués et gérés. Comme dit précédemment il est possible de donner l'ordre à la puce NFC d'un téléphone compatible NFC, via l'écosystème NFC, de se comporter comme un badge d'accès pour système hors ligne. Les utilisateurs NFC peuvent ainsi obtenir l'accès via leur téléphone mobile.

Systèmes en ligne

Outre les systèmes de contrôle d'accès hors ligne il existe aussi des systèmes en ligne. Ces systèmes se caractérisent par la présence d'une unité centrale de traitement (système de gestion) qui permet de gérer toutes les portes de manière centralisée, à l'aide d'une programmation. La commande de déverrouillage est initiée à partir du système de gestion et traitée en fin de compte

localement au niveau d'une porte. Avec ce type de système, les cartes sont équipées d'un codage, souvent le numéro de série de la puce et/ou un numéro lié au fabricant, et parfois en outre des clés cryptées. Les numéros et clés peuvent être inscrits sur le badge d'accès à l'aide du système de gestion. Les autorisations sont transmises par le système de gestion à l'intelligence déportée au niveau de la porte. Cette intelligence déportée vérifie si la personne présentant le badge est autorisée à accéder au local et si oui, elle accorde l'accès. Avec les applications NFC, les données nécessaires sont transcrites via le système de gestion et une liaison OTA sur une puce NFC compatible MIFARE4Mobile. Dans ce scénario, la puce NFC se comporte comme une carte MIFARE avec le codage et les clés exigées, de manière à obtenir l'accès.

Avantages de la communication NFC

Les horaires de travail sont de plus en plus flexibles, les contrats de travail sont moins précis et le travail est sous-traité à des travailleurs indépendants. La demande d'une autorisation d'accès souple et sécurisée, devient de ce fait de plus en plus actuelle. L'utilisation de la technologie NFC peut jouer ici un rôle crucial. Via la liaison OTA, il est possible, en effet, d'émettre et/ou d'annuler une clé virtuelle. Cette clé virtuelle permet au possesseur du téléphone NFC d'obtenir l'accès au lieu souhaité. L'écosystème NFC assure un fonctionnement des solutions quel que soit le fournisseur d'accès.

Évolution du marché

Selon le bureau d'études de marché securityinfowatch, le marché du contrôle d'accès à base de technologie NFC se développe très rapidement. Blake Kozak (Senior Analyst auprès du bureau d'étude de marché IHS Technology) déclare que l'adoption des services hors ligne va dominer le marché. Les grands acteurs traditionnels du contrôle d'accès tels que HID, KABA, ASSA-ABLOY et SALTO sont prêts pour la NFC, à savoir que les trois derniers ont avancé à grands pas dans la technologie NFC. Ainsi, KABA, crée avec sa division Legic le service TSM IDConnect, ASSA-ABLOY, avec sa norme SEOS, a continué à standardiser le traitement des clés NFC, et SALTO dispose de nombreux systèmes NFC, sans couplage TSM. À présent qu'Apple a équipé son très populaire iPhone 6 de NFC, et que les opérateurs des réseaux placent dans ces derniers des TSM, le marché évoluera encore plus rapidement.

(Par Ronald Eygendaal)

Sources :

- <http://www.securityinfowatch.com/article/1117765/access-control-experts-talk-nfc-hosted-solutions-and-interoperability-at-asis?page=3>
- <http://www.sourcesecurity.com/news/articles/co-5188-ga.12743.html>
- <http://www.hidglobal.com/blog/could-mobile-phone-signal-end-pocketful-keys-and-cards>