

NEAR FIELD COMMUNICATION RUKT OP...

Deuren openen met je mobiel

Veel moderne smartphones zijn voorzien van NFC (Near Field Communication)-technologie. Met NFC kan men informatie overbrengen tussen een telefoon en andere NFC-apparaten, zoals andere telefoons, NFC-betaalsystemen en toegangscontrolesystemen. Maar ook kan men met behulp van NFC bijvoorbeeld webadressen, contacten, telefoonnummers, muziektracks, video's of foto's delen.

Volgens het Amerikaanse onderzoeksbureau ABI Research zal het aantal gebruikte NFC-apparaten in 2014 de 500 miljoen overstijgen. Analistenbureau Gartner denkt dat NFC pas gemeengoed begint te worden in 2016. In dat jaar zou er een markt moeten zijn van 448 miljoen gebruikers die gezamenlijk 617 miljard dollar betalen via NFC. Vele belangrijke mobiele providers in de wereld, verenigd in de koepelorganisatie GSM Association (GSMA), hebben verklaard achter het gebruik van de NFC-technologie te staan. De GSMA verwacht in 2015 110 miljard euro aan betalingen via NFC-chips in mobieltjes. De verwachtingen van NFC zijn hooggespannen. Mede daarom hebben een aantal vooraanstaande spelers zich in het verleden gebundeld in het NFC Forum. Zo zijn fabrikanten voor NFC-chips nodig, dienen GSM operators hun netwerken aan te passen en is de ondersteuning van hard- en softwarefabrikanten vereist. Kortom: het NFC Forum is een bont gezelschap van ongeveer 170 partijen die als doel hebben het gebruik van NFC-technologie in consumentenelektronica, mobiele apparaten en pc's te bevorderen. Onder andere Philips, Sony, NXP, Nokia maar ook VISA en Mastercard zijn lid. Rond 2004 heeft het NFC Forum de Near Field Communication-technologie ontwikkeld en gestandaardiseerd. De laatste jaren zijn de daar de fabrikanten van toegangscontrolesystemen

bijgekomen, hierover later meer. De NFC-chip kent verschillende verschijningsvormen. Zo bestaan er aparte chips die in de toestellen gebouwd worden. Daarnaast is op verzoek van de GSMA de mogelijkheid ontwikkeld om een NFC-chip te integreren in een SIM-kaart. Hierdoor ontstaat een verhoogde security. Doel van de NFC-chip is contactloze tweewegcommunicatie tussen twee apparaten die niet meer dan 10 cm van elkaar verwijderd zijn. NFC maakt gebruik van de ISM-frequentieband op 13,56 MHz en heeft een snelheid van 212 kilobit per seconde. Een NFC-chip kan in drie verschillende standen werken:

- Kaartemulatie-mode waar de NFC-chip zich gedraagt als een contactloze smart-card,
- Reader/Writer-mode waar het NFC-device zich gedraagt als een reader en NFC-tags kan lezen of beschrijven
- Peer-to-peer-mode waarbij het mogelijk is om te communiceren tussen twee NFC-apparaten (bijvoorbeeld uitwisselen van visitekaartjes of andere kleine dataoverdracht).

Zoals beschreven kan een NFC-chip zich gedragen als een contactloze smart-card. Software maakt het mogelijk dat een NFC-chip een MIFARE-kaart kan emuleren. MIFARE is de meest gebruikte contactloze chipkaart ter wereld en een handelsmerk van NXP Semiconductors. De technologie is gebaseerd op de



Ronald Eygendaal. Ronald is werkzaam als senior security consultant bij KPN Trusted Services en is sinds 1990 actief in informatiebeveiliging, elektronische & technisch beveiliging, fraude detectie & bestrijding en bewaking & beveiliging in het bijzonder. Hij is bestuurslid bij de Vereniging Beveiligingsprofessionals Nederland (VBN). Ronald is te bereiken via ronald@eygendaals.nl.

ISO 14443 Type A 13.56 MHz contactlozechipkaartstandaard. MIFARE kent vele dialecten zoals; Ultra, Classic / Standard, Plus, DESFire, ProX, SmartMX, DESFire EV1. De meest gebruikte daarvan zijn Classic, DESFire en DESFire EV1. MIFARE wordt gebruikt in meer dan één miljard chipkaarten en tien miljoen lezers. Zo maken creditcardmaatschappijen zoals VISA en Mastercard gebruik van de MIFARE DESFire EV1 standaard en werkt de OV-chip met de MIFARE Classic. Talloze toegangscontrolesystemen werken op basis van MIFARE Classic. Om MIFARE-kaarttechnologie goed te laten samenwerken met NFC is het definiëren van een standaard noodzakelijk. Vanuit deze optiek heeft de MIFARE4mobile Industry Group, welke bestaat uit zeven toonaangevende spelers in de NFC-arena, besloten de MIFARE4Mobile standaard te ontwikkelen. Een van de doelen van de MIFARE4Mobile-standaard is te komen tot specificaties welke gebruikt kunnen worden voor het beheer van toepassingen die MIFARE-chips gebruiken in mobiele apparaten, zoals smartphones. MIFARE4Mobile biedt toestelfabrikanten en mobiele operators, en daarmee ook applicatiemakers, een enkel technologisch aanspreekpunt (API) om NFC te gebruiken. MIFARE4Mobile ondersteunt drie MIFARE-dialecten te weten Classic, DESFire en DESFire EV1.

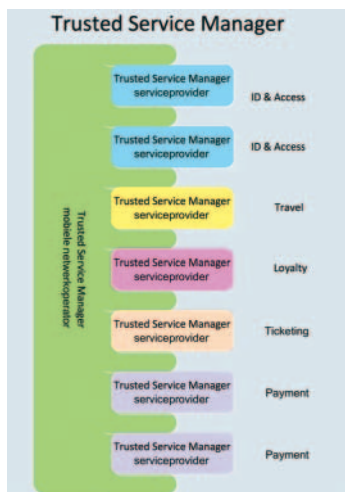
De Trusted Service Manager

Zoals eerder aangegeven zijn er voor NFC aanpassing in de GSM-netwerken nodig. Om het NFC-ecosysteem goed te laten werken is mondiaal draagvlak nodig. Zo dienen de GSM-netwerken te worden uitgerust met een zogenaamde Trusted Service Manager (TSM) en dient er roaming te zijn tussen de netwerken. Binnen het eerder genoemde NFC Forum zijn een aantal fabrikanten van TSM's actief. Deze spelen een belangrijke rol want een TSM is een cruciaal onderdeel van het NFC ecosysteem. Een TSM faciliteert als neutrale bemiddelaar tussen diensten leverancier en de netwerk operators (MNO's). De TSM stelt diensten leveranciers in staat om op afstand hun dienst, welke als software op de NFC-chip aanwezig is, te distribueren en te beheren. De TSM vergemakkelijkt distributie en beheer van toepassingen die zich bevinden op een onderdeel in de GSM. De belangrijkste rollen van een TSM zijn:

- Interconnectie tussen netwerkoperators en de dienstenleveranciers
- Faciliteren van end-to-end-security
- Lifecycle-management
- Uitrol van nieuwe gebruikers
- Faciliteren van download Over-The-Air-applicaties
- Personaliseren Over-the-air-applicaties
- Activeren / Deactiveren diensten
- Update User Interface
- Management van de NFC-klantendatabase
- Bijhouden van de counters voor betalingen en logging
- Faciliteren van toegevoegdewaardediensten zoals; ticketing, toegangscontrole, betalen etc..etc.

Inwendig is een TSM op te delen in een domein voor de

diensten leverancier en domein voor de netwerk operator. Op één TSM kunnen meerdere dienstenleveranciers worden aangesloten. Onderlinge verbinding tussen de TSM 's van verschillende netwerkoperators is van dus groot belang. Sterker nog, hoe meer TSM's met elkaar verbonden zijn hoe beter het NFC-ecosysteem functioneert.



Toegangscontrole systemen

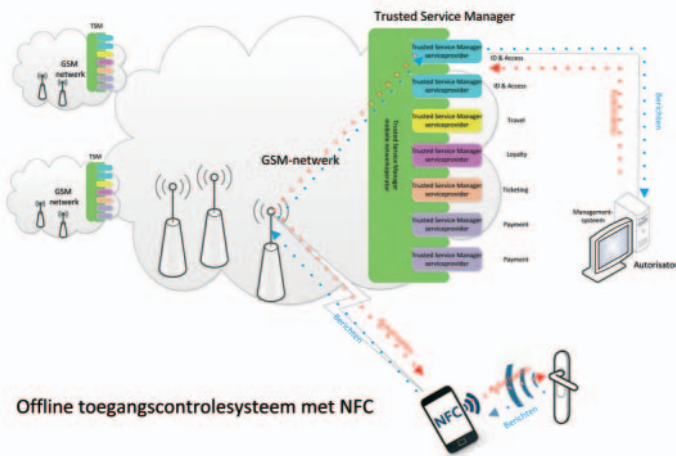
Toegangsbeheer is vereist in vele situaties, kantoorgebouwen, datacenters en parkeergelegenheden zijn slechts enkele voorbeelden. De voornaamste doelstelling van goed toegangsbeheer is het adequaat en klantvriendelijk organiseren van de toegankelijkheid van een terrein, gebouw of ruimte. Het uitgeven en beheren van toegangspassen is een vaak een rompslomp. NFC kan hier een uitkomst zijn. Een NFC-chip kan via een Over-The-Air (OTA)-verbinding, in de kaartemulatie-mode worden geschakeld waardoor de NFC-chip zich gedraagt als een contactloze smart-card en MIFARE4Mobile zorgt er voor dat MIFARE Classic, DESFire en DESFire EV1 kunnen worden ondersteund.

NFC kan zowel bij online als offline toegangscontrole worden toegepast. Offline systemen zijn zelfstandig functionerende toegangscontrolesystemen waarbij autorisatie wordt bepaald door de offline lezer. Offline lezers hebben een eigen intelligentie en verlenen aan de hand van autorisaties autonoom toegang. In de offline lezer is dan de leeseenheid zelf, een batterij voor de voedingsspanningen en een eenvoudige verwerkingseenheid ingebouwd. Offline lezers en zijn er in verschillende verschijningsvormen. Daarbij moet men denken aan varianten die zijn ingebouwd in het deurbeslag, losse kaartlezers maar modellen die dienst doen als inbouwslot. Bij de offline lezers is er geen noodzaak om aanvullende bekabeling te leggen en vervallen de kosten van bekabeling (230 Volt en datakabel).

Bij veel offline toegangscontrolesysteem worden autorisaties van alle kaarthouders, met behulp van een softwareprogramma, op de toegangspas geschreven. Vaak gebeurt dit via een

zogenaaemde update-lezer. Wanneer een toegangspas wordt aangeboden aan een offline lezers wordt de kaart in zijn geheel uitgelezen en worden de autorisaties opgeslagen in het geheugen van de offline lezer. Op deze manier verspreiden de autorisaties zich over alle offline lezers binnen het systeem. Via dit zelfde communicatiepad kunnen offline lezers berichten sturen naar het managementsysteem. (Hierbij moet worden gedacht aan log- en statusmeldingen, maar ook 'battery low'-meldingen.)

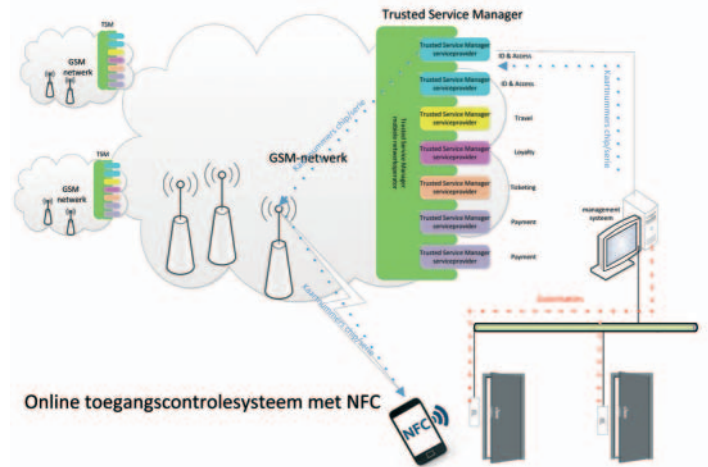
Dit neemt niet weg dat bij een offline situatie nog altijd toegangspassen uitgegeven en beheerd moeten worden. Zoals eerder aangegeven kan met behulp van een NCF-geschikte-telefoon en het NFC-ecosysteem de NFC-chip opdracht krijgen zich te gedragen als een toegangspas voor een offline systeem. Op deze wijze kunnen NFC-gebruikers met hun mobiel toegang krijgen.



Online systemen

Naast offline toegangscontrolesysteem zijn er ook online systemen. Deze systemen hebben als kenmerk dat er een centrale verwerkingseenheid (managementsysteem) aanwezig is die het mogelijk maakt om alle deuren centraal te beheren met behulp van programmatuur. De sturing voor de ontgrendeling wordt geïnitieerd vanuit het managementsysteem waarna het een en ander lokaal bij een deur wordt verwerkt. Bij dit type systemen worden de kaarten voorzien van codering, vaak het chip-serienummer en/of een fabrikant-gebonden nummers en een soms nog vercijferde sleutels. De nummers en sleutels kunnen met behulp van het managementsysteem op een toegangspas worden geschreven. De autorisaties worden vanaf het managementsysteem doorgegeven aan de intelligentie bij de deur. De intelligentie bij de deur checkt of de aanbieder van de pas gerechtigd is om toegang te verkrijgen en indien gerechtigd wordt toegang verleend. Voor NFC-toepassingen worden de benodigde gegevens via het managementsysteem en een Over-The-Air (OTA) verbinding weggeschreven op een NFC-chip welke voldoet aan MIFARE4Mobile. In dit scenario zal

de NFC-chip zich gedragen als een MIFARE kaart met de vereiste codering en sleutels zodat toegang wordt gekregen.



Voordelen NFC

We gaan meer en meer flexwerken. Arbeidscontracten vervagen en werk wordt uitbesteed aan ZZP-er. De vraag naar het op een flexibele en veilig manier verkrijgen van toegang wordt hierdoor steeds actueler. Het gebruik van NFC technologie kan hierin een cruciale rol spelen. Immers via de Over-The-Air (OTA) verbinding kan eenvoudig een virtuele sleutel worden uitgegeven en/of ingetrokken. Met deze virtuele sleutel kan de bezitter van de NFC telefoon zich dan toegang verschaffen tot de gewenste locatie. Het NFC ecosysteem zorgt er voor dat oplossingen provideronafhankelijk werken.

(fk)De marktontwikkelingen

Volgens marktonderzoeksbureau securityinfowatch ontwikkelt de markt voor toegangscontrole op basis van NFC-technologie zich zeer snel. Zo geeft Blake Kozak, senior analyst bij marktonderzoeksbureau IHS Technology, aan dat de adoptie van offline systemen de markt zal domineren. Grote traditionele toegangscontrolespelers zoals HID, KABA, ASSA-ABLOY en SALTO zijn klaar voor NFC. Met name de laatste drie hebben grote stappen gemaakt met NFC-technologie. Zo maakt KABA met haar Legic divisie TSM's, heeft ASSA-ABLOY met haar SEOS standaard de NFC sleutelbeheer verder gestandaardiseerd en heeft SALTO veel NFC-systemen, zonder TSM-koppeling in het veld staan. In 2014 zullen de netwerkoperators TSM's in de netwerken plaatsen en zal de markt in nog hogere versnelling komen.

Links

- <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>