Stratix

Gedeeld gebruik MNC's voor M2M toepassingen

RAPPORT

Rapport uitgebracht aan
het Ministerie van Economische Zaken

Hilversum, april 2013

Stratix

Inhoud

Stratix

1 Introductie

Door het gebruik van SIM-kaarten kunnen netwerken en netwerkaanbieders los gekozen worden van client-apparatuur (zoals telefoons), zodat vendor lock-in bij aanbieders kan worden voorkomen en de keuzevrijheid wordt gewaarborgd.

De "identiteits"-informatie die een netwerk nodig heeft om te bepalen of een gebruiker van een netwerk gebruik mag maken, zit op deze SIM-kaart besloten. Daardoor kunnen gebruikers in beginsel eenvoudig van netwerkaanbieder wisselen door de SIM in het toestel te vervangen door een nieuwe SIM van een andere aanbieder. Deze systematiek zorgt voor een grote mate van flexibiliteit voor gebruikers van mobiele telefoons.

Randvoorwaarde voor deze dynamiek is echter dat de SIM-kaart eenvoudig, en daarmee relatief goedkoop, uitgewisseld kan worden (waarbij "relatief goedkoop" bezien moet worden in relatie tot de totale communicatiekosten). Voor consumenten is dit veelal geen probleem: de nummerportabiliteit is goed geregeld, en bij het afsluiten van een nieuw abonnement verstrekt de nieuwe aanbieder een SIM-kaart die de gebruiker zelf in het toestel kan zetten. Gebruikers die dat niet zelf kunnen, kunnen bij een winkel langs gaan of een handige kennis vragen.

Bij andere toepassingen, en dan met name toepassingen op het gebied van "Machine-to-Machine" communicatie (M2M), wordt niet altijd aan de genoemde randvoorwaarde voldaan. Vaak is het wisselen fysiek lastig en daardoor duur, omdat er een monteur langs de "machines" moet, terwijl de communicatiekosten bij veel toepassingen relatief laag zijn[1].

Keuzevrijheid tussen mobiele aanbieders is daardoor voor met name grote gebruikers van M2M[2] feitelijk niet geborgd, terwijl daar wel behoefte aan is.

1.1 SIM wissel M2M

De problematiek rond het wisselen van aanbieder speelt zoals aangegeven met name bij Machine-to-Machine toepassingen, omdat een fysieke SIM-wissel daar lastig en daardoor relatief duur is.

Veel M2M toepassingen bevinden zich in het veld, en van een aantal toepassingen ligt het niet in de lijn der verwachting dat er regelmatig een monteur in de buurt van de apparatuur komt. Denk hierbij aan toepassingen zoals slimme meters, maar ook toepassingen in auto's zoals e-Call of locatiebepaling voor verzekeraars. In voertuigen brengt een SIM-wissel uitdagingen en kosten met zich mee, omdat de SIM dusdanig weggewerkt moet worden dat deze slecht toegankelijk is; vaak is de SIM zelfs als "vaste chip" op een printplaat gesoldeerd.

[1] Dit alles geldt zeker niet voor alle M2M toepassingen; paragraaf 1.5 gaat hier verder op in.
[2] OECD work on Internet of Things "The liberalisation of the SIM-card or what to learn from IP interconnection", http://www.internet-science.eu/sites/internet-science.eu/files/OECD%20work%20on%20Internet%20of%20Things%20for%20Turin.pdf

Daarnaast betreft het dataverbruik van veel M2M-toepassingen slechts enkele kilobytes tot een megabyte per maand[3], waardoor de abonnementskosten per aansluiting veel lager liggen dan bij "reguliere" smartphone of laptopgebruikers.

Omdat wisselen *relatief duur* (ten opzichte van de maandelijkse communicatiekosten) en *lastig* (devices staan vaak in het veld en SIM's zitten vast gesoldeerd of weggestopt) is, zitten M2M gebruikers dus feitelijk vast aan hun initiële aanbieder, en dat terwijl de levensduur soms erg lang is en het daardoor niet goed mogelijk is om van te voren alles contractueel vast te leggen.

1.2 Mobiele Netwerkcodes en IMSI-nummers

Mobiele aansluitingen worden geïdentificeerd aan de hand van een IMSI (International Mobile Subscriber Identity) nummer, dat op de SIM staat. De eerste vijf cijfers van de IMSI vormen een per aanbieder unieke code, bestaande uit een landcode (Mobile Country Code, MCC) en een netwerkcode (Mobile Network Code, MNC). Door middel van de MCC/MNC combinatie worden aanbieders van elkaar onderscheiden.

De MNC identificeert van oorsprong een netwerk[4], en is op de SIM-kaart opgeslagen, zodat er een 'vaste' relatie ontstaat tussen SIM-kaart (en dus gebruik) en een netwerk.

MNC's worden tegenwoordig niet alleen meer gebruikt door de Mobile Network Operators (MNO's) met een eigen radionetwerk, maar ook door de Mobile Virtual Network Operator (MVNO's), aanbieders zonder eigen radionetwerk maar met eigen netwerkelementen zoals een HLR (Home Location Register). Een MVNO sluit een contract met een MNO, waarin is afgesproken dat een MVNO gebruik kan maken van het radionetwerk van de desbetreffende MNO. In dat geval accepteert de betreffende MNO alle gebruikers met IMSI nummers die met de MCC/MNC[5] combinatie van de MVNO beginnen.

Een 'eigen' MNC geeft dus (aan bijvoorbeeld een MVNO) de technische vrijheid om na afloop van het contract over te stappen naar een andere MNO, zonder daarbij nieuwe SIM-kaarten uit te hoeven delen. De MVNO kan immers een contract afsluiten met een nieuwe aanbieder, die vervolgens de betreffende MCC/MNC combinatie op zijn netwerk accepteert.

Voor grootschalige gebruikers, en met name voor M2M toepassingen, is zoals gezegd het wisselen van SIM-kaarten vaak een relatief dure zaak. Een oplossing waarbij miljoenen M2M aansluitingen onder een aparte MNC worden ondergebracht zou voor dergelijke gebruikers een oplossing kunnen vormen voor deze lastige overstap.

[3] Bij gebruik van Smartphones zijn datahoeveelheden van honderden Megabytes of zelfs Gigabytes per maand steeds gebruikelijker, en hier staan abonnementskosten van tien of tientallen euro's per aansluiting tegenover.

[4] In dit rapport wordt steeds de terminologie van GSM/GPRS gehanteerd. Hoewel de benamingen vaak anders zijn, gelden de conclusies echter ook voor UMTS en LTE.

[5] Waar in dit rapport verder over MNC's gesproken wordt, gaat het steeds om een MNC binnen de MCC van Nederland (204).

1.3 Probleemstelling: MNC's voor grootschalig gebruik

Gebruikers van grootschalige mobiele toepassingen, en met name van grootschalige M2M toepassingen, hebben behoefte aan een flexibele manier om na afloop van een contract te kunnen wisselen van aanbieder zonder een SIM-wissel.

Hiervoor zijn grofweg twee oplossingsrichtingen te onderscheiden, namelijk:

- Het kunnen beschikken over een eigen MNC en IMSI-reeks waardoor de SIM hetzelfde blijft maar aan de netwerkkant de overschakeling plaatsvindt. Hiervoor is flexibilisering van de manier waarop MNC's worden toegekend nodig.

- Het op de SIM op afstand kunnen aanpassen van het IMSI-nummer. Hiervoor is een "Over the Air" herprogrammeringsmogelijkheid nodig;

Optie twee, "Over the Air" aanpassing, zal in paragraaf 2.2 kort worden toegelicht; de focus van dit onderzoek ligt op de eerste optie, het flexibel gebruik van MNC's voor grootschalige M2M gebruikers.

Als M2M gebruikers zouden kunnen beschikken over eigen MNC's, dan zou het wisselen van aanbieder veel eenvoudiger zijn. Probleem is echter dat MNC's vooralsnog (met enkele specifieke uitzonderingen) alleen aan *aanbieders van openbare telecom diensten* kunnen worden toegekend. Dit volgt uit de ITU aanbeveling E.212, en uit de Nederlandse implementatie daarvan in het Nummerplan IMSI nummers[6]. De reden voor deze beperking is dat de MNC uit twee cijfers bestaat, en er dus per land maar 100 van dergelijke codes te vergeven zijn[7]. Als MNC's zonder meer aan gebruikers toegekend zouden worden, zouden die codes snel op zijn.

Weliswaar is het voor sommige toepassingen mogelijk om driecijferige MNC's toe te kennen, maar zelfs dan is het uit te geven aantal te beperkt om dergelijke codes zonder meer aan gebruikers toe te kennen. Doordat er tot op heden al 31 tweecijferige codes zijn toegekend, en nog negen zijn gereserveerd voor tweecijferig gebruik, zouden er hooguit 600 driecijferige codes toegekend kunnen worden.

1.4 Onderzoeksvragen

Het Ministerie van Economische Zaken heeft aan Stratix Consulting gevraagd om onderzoek te doen naar de mogelijkheden en obstakels voor een gedeelde MNC voor grootschalige gebruikers, en met name voor M2M.

In aanloop naar dit onderzoek heeft het ministerie een aantal onderzoeksvragen opgesteld. Deze vragen en de bijbehorende antwoorden staan in Annex A; de antwoorden moeten wel in samenhang met de hoofdtekst van dit rapport gelezen worden.

---

[6] Formeel: "Nummerplan voor identiteitsnummers ten behoeve van internationale mobiliteit (IMSI-nummers)".

[7] Een land kan ook meerdere MCC's krijgen, maar de ITU is terughoudend met het uitgeven van additionele MCC's.

1.5 Relevante toepassingen

De omschreven problematiek speelt vooral bij grootschalige M2M-toepassingen[8] zoals bij de "slimme meters" of bij "e-call" in auto's, maar wellicht ook bij kleinere M2M toepassingen of bij andere grootschalige toepassingen.

Specifiek kijkt het Ministerie van Economische Zaken op dit moment naar de uitrol van geautomatiseerde energiemeters. Door de wettelijke invoering van deze "slimme meters" vanaf 2014, en de bijbehorende plicht om zes keer per jaar[9], en op verzoek van de energie eindverbruiker vaker, meterstanden uit te lezen zijn de netbeheerders genoodzaakt een communicatieoplossing voor deze slimme meters te gaan gebruiken. Hierbij zijn allerlei communicatiemiddelen mogelijk, waaronder GPRS (daarnaast worden ook een aantal andere technologieën overwogen, zoals PLC, CDMA, of het gebruik van reeds aanwezig draadloos internet via WiFi).

Vanuit de beheerders van de energienetten bezien is het voordelig om te kunnen kiezen uit meerdere alternatieven, en om binnen een technologie zoals GPRS ook op een gegeven moment te kunnen wisselen van aanbieder[10]. Een SIM wisselen in een slimme meter kost tussen 50 en 80 Euro, terwijl de totale communicatiekosten niet meer dan 10 Euro per jaar mogen bedragen. Als een netbeheerder om de vijf jaar van contract wil wisselen, kost het wisselen hem dus meer dan de totale communicatiekosten over die periode.

Naast de slimme energiemeter worden er de komende jaren nog enkele andere grootschalige M2M toepassingen verwacht. Zo wordt het vanuit de EU in de toekomst verplicht om iedere auto uit te rusten met een zogenaamde "emergency-Call", of e-call, applicatie, waarbij een boordcomputer bij een ongeval automatisch de hulpinstantie waarschuwt, en meteen alle relevante informatie zoals locatie en aantal inzittenden doorgeeft.

Naast deze vanuit de overheid gedreven grootschalige toepassingen zijn er de komende jaren vanuit de markt zeer veel kleinschalige M2M toepassingen op allerlei gebied te verwachten, waarvan een deel ook GPRS of LTE als communicatiekanaal zal gebruiken.

Voor veel van deze toepassingen speelt de hier beschreven problematiek veel minder dan voor de genoemde grootschalige toepassingen: bij bijvoorbeeld een frisdrankautomaat of een kopieerapparaat met een M2M module komt er zo vaak een monteur langs, dat een SIM wissel geen groot probleem is.

Er zullen echter ook kleinschalige toepassingen zijn waar het probleem van de SIM wissel wel speelt, met name omdat het betreffende apparaat ergens ingebouwd is waar zelden een monteur langsgaat.

---

[8] Het Stratix rapport "Nummers voor Machines" (2009) geeft een uitgebreider overzicht; zie http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2009/04/16/stratix-rapport-m2m-nummers-nummers-voor-machines.html

[9] Zie Artikel 26ae lid 1 van de Electriciteitswet en Artikel 1 van het Besluit Kostenoverzicht Energie.

[10] Het is hierbij niet direct van belang dat ze ook daadwerkelijk wisselen, het enkele feit dat ze dit in principe eenvoudig zouden kunnen doen zorgt reeds voor meer inkoopkracht.

2 Flexibilisering door controle SIM's en IMSI

Verschillende netwerken binnen een land worden van elkaar onderscheiden door de Mobile Network Codes (MNC's). Een operator (MNO of MVNO) heeft de beschikking over één of meer MNC's en de bijbehorende IMSI-reeksen, en kan daarmee nummers uit deze reeksen toekennen aan eindgebruikers.

Een partij die controle heeft over een 'eigen' MNC kan hiermee een netwerk inrichten, of met een aanbieder van een netwerk afspraken maken over het verzorgen van diensten voor zijn gebruikers.

2.1 Creëren IMSI sub-reeksen voor M2M

Een mogelijkheid om gebruikers van met name grootschalige M2M toepassingen meer flexibiliteit te geven, zonder dat de voorraad MNC's in korte tijd uitgeput raakt, is om een aantal van deze gebruikers *gezamenlijk* een MNC toe te kennen. Vanuit deze MNC kunnen dan IMSI sub-reeksen toegekend worden aan deze grootschalige M2M gebruikers. Op die manier ontstaat een groter aantal kleinere IMSI sub-reeksen[11], waardoor aan meer partijen (vergeleken met het aantal dat met de huidige 100 beschikbare combinaties mogelijk zou zijn) een IMSI sub-reeks toegekend kan worden.

De gebruikers van deze IMSI sub-reeksen richten hierbij zelf een oplossing in om de koppelingen van de MNC richting de MNO's te realiseren en om de MNC/IMSI reeks verder uit te splitsen. Op deze manier is de impact voor de operators beperkt, en vergelijkbaar met de technische koppeling van een nieuwe MVNO.

Dit brengt een aantal technische, organisatorische en juridische uitdagingen met zich mee, omdat deze centrale oplossing als "tussenschakel" fungeert tussen de netwerkaanbieders en de diverse (M2M)-gebruikers, die sterk kunnen verschillen in bijvoorbeeld omvang en type gebruik.

2.2 Alternatief: Over the Air aanpassen IMSI-nummer

Het probleem van overstappen bij M2M toepassingen zou in principe ook kunnen worden verminderd indien het IMSI-nummer en bijbehorende authenticatiesleutels op afstand zouden kunnen worden aangepast. Er wordt in de industrie al langere tijd gekeken naar manieren om door middel van een "herprogrammeerbare SIM" of "Soft-SIM" deze informatie aan te kunnen passen zonder een fysieke wissel van de SIM-kaarten, maar via een "Over The Air" (OTA) mechanisme. Hiervan zijn meerdere varianten denkbaar:

- De SIM bevat vanaf het begin meerdere identiteiten, en OTA wordt gebruikt om te wisselen tussen deze identiteiten.

[11] Indien binnen het huidige 5-cijferige MCC/MNC gebruik drie cijfers worden gebruikt ontstaan er 1000 sub-'reeksen, waarmee binnen elk van deze reeksen nog 7 cijfers over zijn, ieder goed voor 10 miljoen aansluitingen.

- De SIM is dusdanig flexibel dat de hele identiteit, inclusief keys, later kan worden aangebracht.

De eerste variant sluit het meest aan op de manier waarop het nu werkt: de benodigde informatie van (weliswaar meerdere) operators, inclusief de encryptiesleutels, zijn "hard" op de SIM-kaart aangebracht. In feite zijn er dus twee of meer identiteiten ondergebracht op één "SIM-kaart"[12], en alleen het mechanisme om te kunnen kiezen tussen die identiteiten dient *"over the air"* mogelijk te zijn. Hiervoor zal men dus voorafgaand aan productie van de SIM-kaart afspraken met meerdere operators moeten maken, omdat operators hun keys beschikbaar zullen moeten stellen om op de SIM-kaarten te laten programmeren. Er zal dus een overeenkomst met al deze operators gesloten moeten worden, ook met diegene die in eerste instantie geen mobiele telecomdienst levert. Daarbij is de vraag wie de sleutels op de kaart zou moeten zetten; de operators hebben hiertoe normaal alleen afspraken met hun eigen SIM–leverancier[13], en het is dan ook de vraag of men hieraan mee zou werken. Naast security-vraagstukken brengt deze oplossing ook (licentie- en capaciteits-) kosten met zich mee, omdat alle betrokken aanbieders een entry in hun HLR moeten maken voor deze IMSI (circa 1 Euro per SIM, per operator). Ook kunnen er alleen operators op de SIM worden geïmplementeerd die nu al operationeel zijn (of althans kunnen beschikken over een MNC en over sleutels), en worden toekomstige operators feitelijk bij voorbaat uitgesloten.

De tweede mogelijkheid is het op afstand programmeren van een nieuwe identiteit op een (soft)SIM. Ook hier zitten nadelen aan: de sleutels zullen "Over The Air" aangepast moeten worden, en als er intussen iets mis gaat dan wordt het apparaat wellicht onbereikbaar. Ook hier zullen afspraken nodig zijn tussen de gebruiker, de "oude" netwerkaanbieder en de "nieuwe" netwerkaanbieder, onder andere over de mogelijkheid de sleutels te verzenden waardoor wellicht een veiligheidsrisico ontstaat. De huidige praktijk is dat deze sleutels fysiek op de SIM's worden gezet, juist om deze risico's te vermijden. Met dit model zijn er wel trials uitgevoerd, maar is er nog geen standaardwerkwijze voor geïmplementeerd. De verwachting in de industrie is dat het nog zeker een aantal jaren zal duren voordat deze oplossing universeel inzetbaar is.

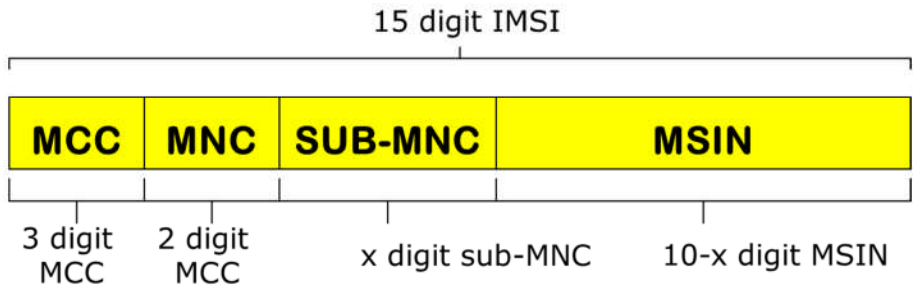
Alles bij elkaar is duidelijk dat de verschillende mechanismen voor "Over The Air" provisioning van IMSI-nummers voor de nabije toekomst geen realistische oplossingen zullen leveren voor de huidige in de markt ondervonden overstapdrempels.

[12] In de praktijk worden soms al wel twee IMSI's van een enkele aanbieder ondergebracht op een SIM-kaart, bijvoorbeeld ten behoeve van roaming.
[13] Er zullen dus wellicht IMSI's van directe concurrenten ondergebracht moeten worden op 1 SIM.

3 Voorzien gebruiksmodel "Gedeelde MNC"

3.1 Beschrijving voorgestelde oplossing

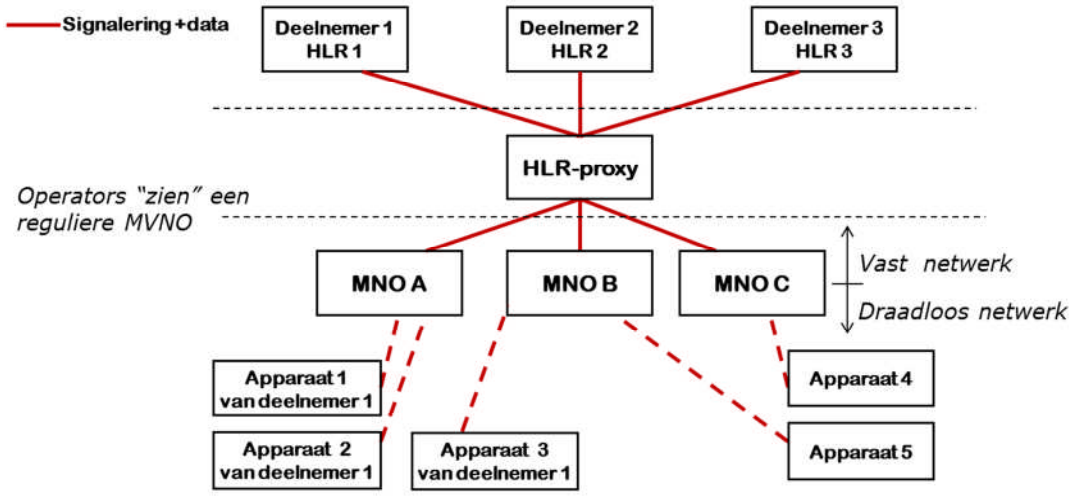
Bij de voorgestelde flexibilisering van netwerkcodes zal een MNC (of meerdere) worden opgesplitst, waardoor meer IMSI "sub-reeksen" ontstaan binnen de Nederlandse MCC-ruimte dan de huidige 100.



Figuur 1: Opgesplitst IMSI-nummer

Dit type flexibilisering kan echter niet zondermeer worden geïmplementeerd. De huidige netwerken (in Nederland en elders) zijn zo ingericht dat ze bij het verifiëren van de oorsprong van een IMSI-nummer dat zich aanmeldt op het netwerk alleen kijken naar de eerste 5 cijfers (MCC en MNC gedeelte) van het IMSI-nummer, en aan de hand van deze cijfers bepalen bij welke partij het netwerk moet "navragen" of dit device toegang verleend mag worden. Het 'zomaar' toekennen van een opgesplitste MNC zou dan ook weinig zin hebben, omdat de netwerken hier niet mee om kunnen gaan. Alhoewel in theorie de netwerkapparatuur geschikt zou kunnen worden gemaakt voor het onderscheiden op meercijferige MNC's, is dit niet iets wat op korte termijn zal worden aangeboden door de leveranciers van netwerkequipment, omdat deze feature vooralsnog in de praktijk nergens gebruikt zal worden.

In het voorstel zoals dat door het ministerie wordt aangedragen wordt dit probleem opgelost door het invoeren van een tussenliggende, neutrale partij die de MNC beheert. Deze op te delen MNC betreft een reguliere 5-cijferige MNC en wordt dus als zodanig ondersteund vanuit de netwerken. De centrale entiteit zorgt vervolgens voor onderverdeling in IMSI-reeksen voor gebruik door de (M2M-)gebruikers. Vanuit de MNO's bezien ziet de centrale entiteit er technisch uit alsof het een "reguliere" MVNO is. De normale koppelingsmechanismen en authenticatie-mechanismen kunnen dus worden gebruikt als ware het een MVNO.



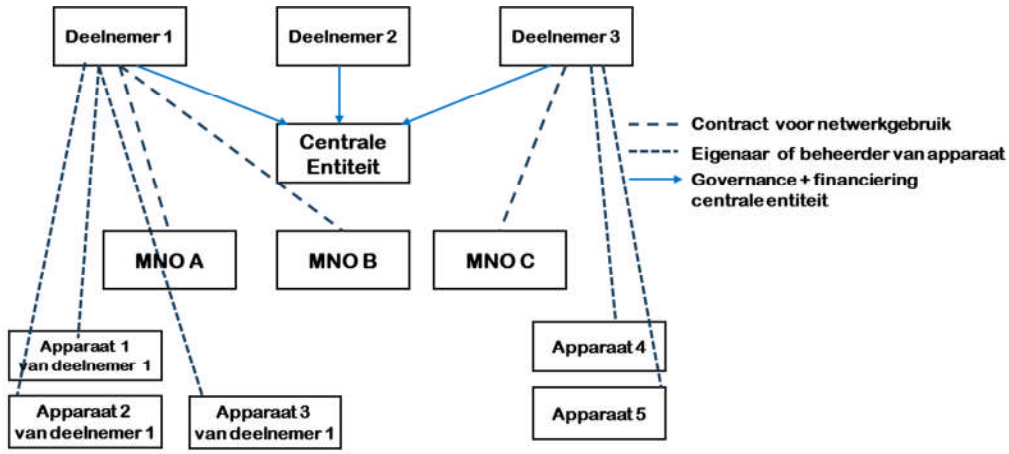
Figuur 2 Gebruiksmodel waarin een centrale entiteit de HLR-Proxy waar de MNC is ondergebracht beheert en deze verdeelt in IMSI "sub-reeksen" waar de beheerders van grootschalige M2M toepassingen (deelnemers aan de gezamenlijke MNC) gebruik van kunnen maken.

De M2M gebruikers kunnen ieder een eigen contract voor Megabytes, minuten, of radiocapaciteit op de fysieke netwerken afsluiten (inkopen draadloze netwerkdienst), vergelijkbaar met de manier waarop reguliere MVNO's afspraken maken met de MNO's. Na afloop van het contract kunnen nieuwe contracten worden afgesloten met dezelfde MNO of met één van de anderen. Overigens kunnen de gebruikers ook besluiten gezamenlijk in te kopen, bijvoorbeeld doordat de centrale entiteit de contracten met de MNO's afsluit.

3.2 Relaties diverse partijen binnen het gebruiksmodel

Binnen het voorgestelde model zullen technische koppelingen[14] verlopen via de centrale entiteit, maar kunnen andere zaken zoals afspraken rond netwerkgebruik direct tussen M2M-gebruikers en MNO's worden gemaakt. De gebruikspartijen samen zullen de centrale entiteit bekostigen en besturen.

[14] In het plaatje verlopen ook de datastromen via de centrale entiteit. Dit is strikt genomen niet noodzakelijk, maar wellicht wel het meest praktisch. Zo sluit het model optimaal aan bij de in de markt gebruikelijke constructies, waarbij de MVNO al het dataverkeer voor zijn klanten verwerkt.



Figuur 3: Zeggenschap en organisatorische verbanden: De gebruikers ("users") van de gedeelde MNC (bijvoorbeeld grootschalige M2M gebruikers) beheren en betalen gezamenlijk de centrale entiteit, die de HLR-proxy beheert. Zij kunnen wel ieder zelf afspraken maken met MNO's over het onderbrengen van devices op hun mobiele netwerk.

Hierbij is het van belang dat afhankelijk van de wensen van de deelnemers de juiste, wellicht meer specifieke, functionaliteit wordt ondersteund vanuit de centrale entiteit.

Over de functionaliteit, investeringen en onderhoud zal door de gebruikers gezamenlijk besloten moeten worden. Zo is het wellicht voor de slimme meters nodig om naast de mogelijkheid van een dataverbinding, ook een wake-up mechanisme te implementeren, bijvoorbeeld in de vorm van SMS; voor andere toepassingen kan juist de mogelijkheid om ook een spraakoproep tot stand te brengen van belang zijn. Al deze opties brengen kosten met zich mee voor de centrale entiteit, en het zal voor de gebruikers op voorhand duidelijk moeten zijn hoe dergelijke kosten verdeeld worden en hoe in de toekomst besloten wordt de functionaliteit al dan niet aan te passen. Voor de deelnemers zal vanaf het begin duidelijk moeten zijn welke zeggenschap ze hebben, en hoe dit is georganiseerd. Afspraken rondom deze zeggenschap en de besluitvorming (de governance-structuur) zijn dus van groot belang om voor deelnemers voldoende zekerheid te bieden.

4 Technische aspecten

Voor het delen van een MNC vormt de centrale entiteit het technische koppelvlak tussen aan de ene kant de MNO's, en aan de andere kant enkele of meerdere deelnemers[15]. Deze centrale entiteit zal fungeren als "beheerder" van de MCC/MNC, en de onderliggende IMSI's technisch en organisatorisch verder verdelen voor de deelnemende gebruikers.

Hierbij is er geen harde beperking voor de manier waarop de reeks wordt opgedeeld. Er kunnen "grote" reeksen worden gecreëerd, door de sub-reeksen te identificeren aan de hand van de op de MNC volgende 2 cijfers, maar het is ook mogelijk het nummer veel fijnmaziger op te delen. Combinaties zijn ook mogelijk, waarbij grote gebruikers reeksen krijgen van bijvoorbeeld een miljoen IMSI-nummers, en kleinere gebruikers reeksen van 10.000 nummers krijgen. Hierdoor kan ook voor kleine gebruikers een passende reeks worden gecreëerd.

De deelnemende organisaties en bedrijven kunnen gebruik maken van koppelingen die de centrale entiteit heeft met de MNO's voor signalering en afhandeling van het verkeer, terwijl ze zelf contracten sluiten met de MNO's voor het inkopen van dienstverlening op hun radionetwerk.

4.1 Verschillende rollen MNC's in mobiele communicatie

Voor het begrip van de volgende secties is het relevant om de verschillende rollen te onderscheiden die de MNC speelt in de mobiele communicatie.

Zo speelt de MNC een rol binnen het IMSI nummer (bestaande uit een MCC, MNC, en een MSIN) dat gebruikt wordt om eindgebruikers te identificeren. Het IMSI-nummer identificeert hierbij het gebruikersprofiel in de HLR, en de IMSI wordt met de bijbehorende Ki encryptiesleutel gebruikt om de mobiele aansluiting te authentiseren.

In het radionetwerk identificeert een MCC/MNC combinatie het netwerk. Deze combinatie wordt uitgezonden door het netwerk. Doordat deze MCC/MNC combinatie opgeslagen is op een SIM-kaart, als deel van de IMSI, kan er een link tussen het "thuis" netwerk en de SIM-kaart worden gemaakt. Dit geldt echter alleen voor klanten van de MNO; klanten van een MVNO hebben technisch gezien geen mobiel "thuis" netwerk en zijn dus altijd "te gast" bij de MNO. In dat geval staat de MCC/MNC combinatie van de betreffende MNO in een aparte lijst op de SIM: de "Preferred Network" lijst. Omgekeerd staan de MCC/MNC combinaties van MNO's waar de gebruiker geen toegang toe krijgt in de "Forbidden Network" lijst.

Ook voor de afhandeling van verkeer tussen netwerken onderling wordt de MCC/MNC gebruikt om de "home operator" te identificeren; voor de routering van het verkeer wordt de MCC/MNC combinatie eerst vertaald in een ander type nummer[16] door middel van Mobile

[15] Deelnemers zijn bijvoorbeeld aanbieders van M2M diensten, en/of de Netbeheerders in de energie sector.

[16] Hiervoor wordt een nummer gebruikt dat lijkt op een gewoon telefoonnummer, zodat de vaste netwerken het ook kunnen routeren.

Global Titel Translation. Daarnaast wordt deze MCC/MNC gebruikt als kenmerk voor de billing van roaming verkeer tussen operators.

SIM kaarten met een MNC en bijbehorende IMSI nummers worden niet alleen gebruikt in de mobiele netwerken volgens de 3GPP standaarden (GSM, UMTS en LTE), maar ook in mobiele netwerken volgens diverse andere standaarden, waaronder de vooral in de VS gebruikte oneCDMA standaard.

4.2 Koppeling richting MNO's

Vanuit de centrale systemen zal een koppeling richting de MNO's geregeld dienen te worden voor signalering. Deze koppeling kan gerealiseerd worden op dezelfde wijze als een standaard MVNO-koppeling (op basis van C7 over IP op basis van SIGTRAN, en GTP voor het dataverkeer). De centrale entiteit zal richting de MNO's alle requests voor de toegekende MCC/MNC accepteren en verder afhandelen, hetzij via een eigen HLR, hetzij via een doorverwijzing naar een andere HLR of database. Om te voorkomen dat de MNO een uitgebreidere analyse op de IMSI moet doen dan de gebruikelijke MCC/MNC, dient de centrale entiteit zich te gedragen als één netwerk met één unieke Mobile Global Mobile Titel (MGT).

De centrale entiteit zal er dus richting de MNO's uitzien als een reguliere MVNO, waarbij de mechanismen welke gebruikt worden om gebruik te kunnen maken van het radionetwerk dezelfde zijn als die nu al gebruikt worden bij een MVNO.

Naast een koppeling voor signalering is er een koppeling voor data nodig. Hoewel deze in principe ook tussen de MNO's en elke gebruiker afzonderlijk opgebouwd zou kunnen worden, op basis van de bijbehorende APN (Access Point Name), is het effectiever om dit via de centrale entiteit te doen.

4.3 HLR-proxy

Indien de centrale entiteit alleen als "doorgeefluik" fungeert dan dient dit doorgeefluik in de vorm van een "HLR-proxy" in te worden gericht, waarbij deze alle verzoeken voor de MNC aanneemt en vervolgens op basis van de IMSI-nummers bepaalt aan welke deelnemer het verzoek wordt doorgestuurd. Iedere deelnemer heeft in dat geval een eigen HLR.

Deze variant biedt de meeste vrijheid aan de deelnemers om hun eigen core zo in te richten als ze willen, met die functies die ze nodig hebben, en niet meer.

De centrale entiteit kan echter ook meer functionaliteit implementeren, waaronder een volledige HLR. In dat geval hoeven de deelnemers deze niet afzonder in te richten, maar gebruiken zij ieder een deel van de ruimte op de gezamenlijke HLR.

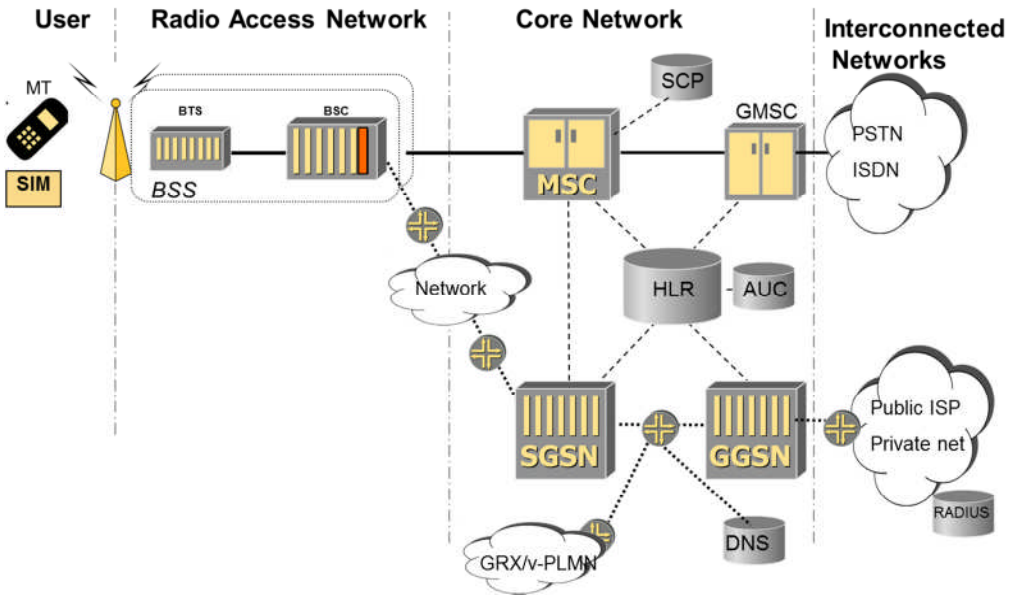
4.4 Inrichting mobiele core

De deelnemers in de centrale entiteit zullen een eigen mobiele (mvno-achtige) core in moeten richten waarin de aansluitingen (IMSI-nummers) worden ondergebracht en waar

afhandeling van het verkeer plaatsvindt. De precieze functionaliteit van deze core hangt af van de toepassing waarvoor het netwerk gebruikt gaat worden.

In ieder geval dienen voor M2M-dataverbindingen over GPRS een HLR met Authentication-center (AuC), een Gateway GPRS Serving Node (GGSN), een Signalling Transfer Point (STP), en de genoemde koppelingen met een MNO ingericht worden. Afhankelijk van aanvullende wensen zullen er nog aanvullende functies nodig zijn, zoals een SMS Service Centre (SMSC) voor SMS of een Gateway Mobile Switching Center (GMSC) voor spraak.

Voor LTE of UMTS dienen vergelijkbare functies te worden ingericht, in de vorm van een "Evolved Packet Core" (EPC). Deze bevat functioneel grotendeels dezelfde bouwblokken, maar met andere benamingen en een net iets andere inrichting. In dit rapport wordt alleen de GSM terminologie gebruikt, maar indien de deelnemers ook UMTS of LTE willen ondersteunen dan zullen de betreffende functies in de vorm van een Evolved Packet Core opgezet moeten worden.



Figuur 4 Globaal overzicht van een GSM/GPRS netwerk.

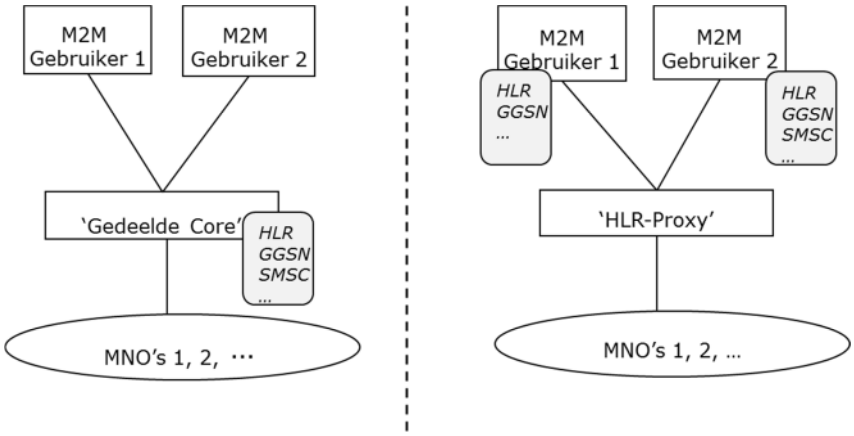
4.4.1 Core in centrale entiteit of per M2M eindgebruiker?

De nodige core functies kunnen op verschillende niveaus worden vorm gegeven. Er kan worden gekozen voor inrichting van de volledige core door de centrale entiteit[17], of er kan gekozen worden voor inrichting van deze core door de M2M gebruikers. Beide mogelijkheden

[17] Als hier wordt gesproken over "het inrichten van een core:" wordt bedoeld onder wiens verantwoordelijkheid dit gebeurt. Het is aannemelijk dat een dergelijke partij het werk weer uitbesteed of de functionaliteit "as a service" af zou kunnen nemen bij derden (zoals een integrator).

hebben voor- en nadelen: De core kan goedkoper en efficiënter neer worden gezet als dit gebeurt voor meerdere deelnemers en meer aansluitingen tegelijk. Daar staat tegenover dat als de M2M-gebruikers zelf hun core inrichten, ze meer controle hebben over wat er precies wordt ingericht.

Binnen deze modellen kunnen tegenstrijdige belangen spelen die door de verschillende deelnemers anders worden afgewogen: er kan bijvoorbeeld een financieel (schaalgrootte) voordeel zijn als de HLR centraal wordt ingericht, maar deelnemers kunnen om andere redenen (autonomie, zelf investeringsbeslissingen af kunnen wegen) besluiten om deze functies zelf in te richten.



Figuur 5: De core functionaliteit kan worden ondergebracht bij de centrale entiteit of bij de individuele private MVNO's, waarbij de centrale entiteit alleen een simpele HLR-proxy functie heeft.

4.5 SIM-kaarten

In iedere telefoon of apparaat is een Subscriber Identity Module, of SIM, nodig die de identiteit en benodigde informatie (zoals t.b.v. encryptie) bevat waarmee een device zich op een netwerk kan aanmelden. Dit kan in de vorm van de bekende *SIM-kaart* of als vast ingebouwde "embedded" chip. Ten behoeve van de gedeelde IMSI-reeksen zullen ook SIM[18]'s verkregen moeten worden, die naast het IMSI-nummer ook de benodigde Ki-keys bevatten om authenticatie mogelijk te maken. De keys worden zowel in de HLR/AuC als op de SIM-kaart opgeslagen. Afhankelijk van het gekozen gebruiksmodel zal de verantwoordelijkheid hiervoor bij of de centrale entiteit (bij een gezamenlijke HLR) of bij de deelnemers zelf liggen indien ze zelf een HLR inrichten

[18] Vanuit M2M perspectief is er –zeker in de situatie dat fysieke SIM-wissels niet nodig zijn- idealiter geen sprake van een "kaart" zoals we die kennen uit de mobiele telefoons, maar zal een dergelijke SIM in de vorm van een chip op de toepassing worden vast gesoldeerd.

De SIM-leverancier speelt in het voorgestelde model een speciale rol, en waar SIM's voorheen via operators werden verkregen zullen deze nu dus ook direct aan M2M-leveranciers kunnen gaan leveren.

4.6 Netwerktechnische aspecten host-netwerk

4.6.1 "International" en "national" Roaming

De term 'roaming' wordt veelal gebruikt voor de situatie waarin een gebruiker met een Nederlands abonnement, in het buitenland gebruik maakt van een "gast" netwerk (international roaming) om te bellen, sms-en, of te internetten. Technisch gesproken is er echter sprake van roaming als een device gebruik maakt van een ander netwerk dan het "home" netwerk; dat kan dus zowel nationaal als internationaal zijn.

MNO's (dus de operators met een eigen fysieke radionetwerk) staan vaak geen National Roaming toe, omdat men in eigen land het eigen netwerk wil gebruiken voor het afhandelen van verkeer[19], maar technisch is het mechanisme hetzelfde.

Wel wordt het zelfde "national roaming"-mechanisme toegepast om MVNO's (virtual operators zonder netwerk) te accommoderen. De MCC/MNC van een MVNO wordt door geen enkel radionetwerk uitgezonden, aangezien de MVNO immers geen radionetwerk heeft. Klanten met IMSI's binnen deze MNC krijgen toegang tot het netwerk van de betreffende MNO op basis van roaming-principes, vergelijkbaar met de wijze waarop roaming afspraken met het buitenland zijn ingericht.

Vanuit het netwerk wordt, zodra een IMSI met een dergelijke MNC zich aanmeldt, een verzoek gestuurd aan de HLR van de betreffende MVNO. Deze meldt vervolgens terug of de betreffende gebruiker (IMSI) bij hem bekend is en welke rechten deze heeft.

4.6.2 Gevolgen National Roaming

Roaming overhead

Voor roaming is communicatie nodig tussen het gastnetwerk en het home-netwerk, en is ruimte in de VLR (Visitors Location Register) database van het gastnetwerk nodig. Bij een oplossing waarbij devices gebruik maken van roaming zullen de MNO's dus voldoende capaciteit in de signalering en in de VLR moeten hebben.

Deze overhead is bij een gedeelde MNC vergelijkbaar met de overhead die ontstaat indien een MVNO wordt ontsloten.

Aanmelden op alle netwerken als gevolg national roaming

Bij roaming zal een device zelf een netwerk zoeken, en een poging doen zich aan te melden op dit netwerk. Bij een 'reguliere' aansluiting wordt, indien een MNC niet in de tabel van

[19] Discussies over inrichting van national roaming speelden onder andere na een aantal grote netwerkstoringen in 2012, waarbij grote gebruikersgroepen niet meer op het netwerk konden.

roaming-partners staat, het verzoek in een vroeg stadium geweigerd; alleen als de MNC wel in deze tabel staat wordt de reguliere authenticatieprocedure uitgevoerd door contact te leggen met de HLR van het "home netwerk". Ook in dat geval kan nog blijken dat de betreffende gebruiker geen recht heeft om het netwerk te gebruiken; dat blijkt dan uit de reactie uit de HLR.

In het nu voorgestelde model zal de gezamenlijke MNC echter bij alle MNO's in de tabel van roaming partners staan, mits iedere MNO contracten heeft met een deel van de deelnemers. Zonder verdere maatregelen zou elk nieuw device zich op een willekeurig netwerk aanmelden, waarna de HLR aangeeft of het device toegang tot dat netwerk dient te krijgen. Dit levert extra signalering op[20]; dit is echter grotendeels te vermijden door van te voren het juiste netwerk op de "Preferred Network" lijst te zetten. In dat geval probeert het device in eerste instantie het juiste netwerk te gebruiken, en probeert het de andere netwerken alleen als dat eerste netwerk niet lukt. Aangezien de netwerken in Nederland in het algemeen een goede dekking bieden, zal dit slechts voor een klein percentage van de devices het geval zijn.

Na een afwijzing zal het device het netwerk op de "Forbidden Network" lijst op de SIM-kaart zetten. Er moet dan ook een mogelijkheid zijn om de "Forbidden Network" lijst periodiek te wissen, omdat een overstap naar een ander netwerk anders niet meer zal lukken (het device probeert het nieuwe netwerk immers niet meer). Dit kan op verschillende manieren: door maatwerk in de client hardware, door toepassing van een hiervoor ingerichte SIM-toolkit applicatie, of door gebruik te maken van timers voor het periodiek wissen van deze lijst die in de 3GPP standaarden (sinds Release 10) zijn opgenomen voor M2M-achtige toepassingen[21].

4.6.3 Beperking ten aanzien van gebruik in radionetwerk

MNC's worden, naast het gebruik voor het routeren van signalen ten behoeve van roaming, ook ingezet ter identificatie van een fysiek radionetwerk. In het geval van een gedeelde MNC kan een dergelijk gebruik echter tot technische problemen leiden.

Zo zal een M2M-device met een IMSI-nummer uit de gedeelde MNC, zodra het zich in het bereik van een netwerk bevindt dat deze zelfde MNC gebruikt ter identificatie van dat netwerk, zich aan proberen te melden op dit netwerk omdat op basis van de MNC wordt geconcludeerd dat het het "home" netwerk betreft. Dit zal in het algemeen niet het geval zijn, zodat het netwerk dan het device zal weigeren. Het device concludeert vervolgens dat het geweigerd wordt op zijn "home" netwerk en probeert vervolgens ook niet om zich op een ander netwerk aan te melden. Het device zal daardoor geen verbinding krijgen zolang het zich binnen bereik van het "vreemde" netwerk bevindt – hetgeen bij veel M2M toepassingen een permanente situatie zal zijn.

---

[20] Bij international roaming speelt dit niet omdat operators afspraken hebben met meerdere operators in het buitenland, en daar de eerste aanmeldpoging dus meestal wel direct succesvol zal zijn.

[21] Voorstel is om voor M2M deze timer te gebruiken, om zonder gebruikersinterventie of speciale client-side applicatie de forbidden-lijst op een SIM te wissen. Zie http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/GSMA-Whitepaper-Embedded-Mobile-Guidelines-Release_3-Network-Aspects1.pdf

Dit betekent dat gebruik van de gedeelde MNC in zoverre beperkt moet worden dat het niet toegestaan is deze MNC in een radio netwerk uit te zenden als identificatie van dat netwerk[22].

[22] Dit zou ook op kunnen treden bij private GSM netwerken die een IMSI gebruiken zoals voorgesteld in het ontwerpbesluit "netwerkintern gebruik van IMSI-nummers in niet-openbare netwerken". Deze netwerken hebben echter in het algemeen een klein bereik, zodat het geweigerde device na enige tijd weer in het bereik komt van het "eigen" netwerk en uit het bereik van het "vreemde" netwerk. Afhankelijk van de "reject clause" zal het toestel dan wel weer proberen zich aan te melden.

5 Organisatorische en operationele aspecten

De MNC zal voor de opsplitsing in IMSI sub-reeksen moeten worden toegekend aan een partij die de opsplitsing verzorgt door middel van de eerder genoemde technische oplossing. Deze partij geeft vervolgens de sub-reeksen uit aan de eigenlijke gebruikers.

In de voorgestelde constructie wordt dus in feite de "lock-in" bij een MNO/MVNO vervangen door een "lock-in" bij de nieuwe entiteit. Het grote verschil is dat de gemeenschappelijke entiteit eigendom kan zijn van de deelnemers, en dat de deelnemers zeggenschap hebben over deze partij. De manier waarop deze centrale entiteit wordt ingericht is dan ook van groot belang om de nadelen van een "lock-in" te vermijden.

5.1 Onafhankelijke centrale entiteit

Het ligt niet direct voor de hand om de verantwoordelijkheid voor de centrale entiteit bij een commerciële partij zoals een bestaande MVNO te leggen, omdat dan de afhankelijkheid van een 'telco met netwerk' wordt ingeruild voor afhankelijkheid van een 'telco zonder netwerk', zonder dat overstappen eenvoudiger is geworden. Meer voor de hand ligt een neutrale tussenliggende partij, die namens de deelnemers hun belang in het hebben van een eigen netwerkcode kan behartigen, zonder belangenverstrengeling. Hierbij kan gedacht worden aan een stichting of coöperatie waarin alle gebruikers deelnemen.

5.1.1 Governance gezamenlijk beheer

De besluitvorming/governance structuur van de centrale entiteit zal zo moeten worden ingericht dat de belangen van de deelnemers zo goed mogelijk worden behartigd.

Er zullen afspraken gemaakt moeten worden over hoe kosten worden verdeeld, en hoe in de toekomst zal worden besloten ook andere koppelingen aan te gaan of nieuwe functies te ondersteunen.

Voor de eenvoud van de governance structuur heeft een "kale" proxy-HLR zonder additionele of optionele functies duidelijk voordelen.

Denk bij dit laatste onder andere aan discussies die zouden kunnen ontstaan indien de entiteit naast de proxy-HLR ook andere core systemen (zoals een HLR of SMSC) gaat inrichten. Dergelijke zaken zullen sowieso ergens ingericht moeten worden, maar indien de centrale entiteit dit doet (in plaats van de private MVNO zelf) dan zal duidelijk moeten zijn wie voor welke functionaliteit zal gaan betalen. Sommige deelnemers willen wellicht alleen een dataverbinding zonder SMS, terwijl andere additioneel ook SMS willen ondersteunen, waardoor een SMSC nodig wordt. Voor het afhandelen van spraak gelden vergelijkbare zaken. Dit geldt ook voor bijvoorbeeld de HLR zelf: De mate waarin de records in de HLR complexer worden, bepaalt mede de prijs, en afhankelijk van het type toepassing kan hier dus door verschillende deelnemers verschillend over gedacht worden. Duidelijk moet zijn hoe wordt besloten wie bepaalde kosten draagt voor extra functionaliteit die initieel, maar ook gedurende de looptijd wordt ingericht. Hoe meer functionaliteit in het centrale deel wordt

ondergebracht, hoe meer kans er is op verschillen van mening over het dragen van de kosten.

5.1.2 Aanbestedingsplicht

Een ander organisatorisch aandachtpunt is de manier waarop vanuit de centrale entiteit contracten worden gesloten voor onder meer de inrichting van de HLR-proxy, de eventuele inrichting van een MVNO-core, en het beheer van deze onderdelen. Een aantal potentiele deelnemers, waaronder in elk geval de genoemde Netbeheerders, is aanbestedingsplichtig. Dit betekent dat ook de centrale entiteit de contracten zal moeten aanbesteden. Voor commerciële partijen geldt dit niet, en deze kunnen de aanbestedingsprocedure al snel als "overbodige rompslomp en vertraging" gaan zien. Om die reden kan het een goed idee zijn deze twee groepen te scheiden, met ieder een eigen MNC.

5.1.3 Centrale entiteit Non-profit organisatie

De Netbeheerders mogen vanuit hun gereguleerde operatie geen commerciële activiteiten ondernemen, of deelnemen in organisaties die dit doen. Dit betekent dat ook een eventuele gemeenschappelijke entiteit waaraan zij deelnemen een 'non-profit' partij zal moeten zijn. Dit is overigens ook vanuit governance oogpunt het meest eenvoudig, omdat dit het risico op tegenstrijdige financiële belangen reduceert.

5.1.4 Toetreden nieuwe deelnemers

Inrichting van de entiteit en opsplitsing van de MNC in IMSI sub-reeksen zal zo moeten worden gedaan dat later ook nieuwe deelnemers kunnen toetreden. Hier zal op voorhand rekening mee moeten worden gehouden. Zo zal er een verdeelsleutel voor kosten (en zeggenschap) dienen te zijn, waarmee duidelijk is welk deel van de nieuwkomer draagt (zowel initieel als later), en dient de structuur zo te worden vormgegeven dat nieuwkomers niet een "extra drempel" kan worden opgelegd. Als dit niet goed gebeurt ontstaat het risico dat nieuwkomers het te bezwaarlijk vinden om in de bestaande entiteit deel te nemen, en dat zij daarom om een eigen MNC zullen vragen.

5.2 Beheersaspecten

5.2.1 Additionele complexiteit beheer

In het voorgestelde model wordt de traditionele telecomketen (toegangsnetwerk, core netwerk, netwerkbeheer, billing, etc.) over verschillende partijen opgesplitst. Dit heeft voordelen, maar brengt ook een aantal extra (beheers) interfaces met zich mee: als er een storing wordt geconstateerd dan kan deze op meerdere plekken binnen de keten liggen. Veelal is niet direct duidelijk waar de problemen (en dus de verantwoordelijkheden) liggen bij een storing.

Er zullen dus goede beheers-afspraken gemaakt moeten worden tussen de M2M-deelnemer en de centrale entiteit, tussen de centrale entiteit en de MNO, en tussen MNO en de M2M-deelnemer. Daar komt nog een beheer-interface met een eventuele beheers-partij voor de

centrale systemen bij, die weer in opdracht van de centrale entiteit deze systemen inricht en beheert.

5.3 Kosten

De kosten voor een 'eigen' MNC bestaan uit het inrichten van een 'MVNO-core' , een koppeling naar een provider van de draadloze netwerkconnectiviteit (de MNO), en het beheer van de nodige systemen.

Indien gebruik wordt gemaakt van een gedeelde MNC dan zal bovendien de mogelijkheid gecreëerd moeten worden om onderscheid te maken tussen de verschillende IMSI sub-reeksen. Dit kan door een aparte 'verdeler' in de vorm van een 'HLR-proxy' of door aanpassingen van de MVNO-core.

De kosten die gemaakt moeten worden voor het inrichten van de basis MVNO-core functionaliteit bestaan voornamelijk uit kosten voor de Home Location Register (HLR), Authentication Center (AuC), GGSN en GMSC.

Indien de MVNO-core per deelnemer wordt ingericht, dan dienen de niet schalende kosten zoals beheer en housing (in ieder geval deels) per deelnemer te worden gerekend. Het gemeenschappelijke deel bestaat dan alleen uit de "HLR-proxy".

De grootste hardware-kostenpost hangt samen met de HLR-capaciteit. Dit zijn echter kosten die sowieso ergens meegenomen moeten worden, of dit nou door de centrale MNC-beheerder, de deelnemende partijen, een MVNO, of een MNO geregeld wordt (dus ook als geen "gedeelde MNC" wordt toegepast).

Onderstaand wordt een indicatie van de investeringskosten voor de inrichting van de centrale core systemen en een indicatie van de kosten voor beheer gegeven, uitgaande van grootschalige toepassingen (miljoenen aansluitingen). Deze indicatie is gebaseerd op schattingen van diverse partijen. Uiteindelijk worden de kosten bepaald door de precieze inrichting, door aspecten zoals redundantie en de exact gewenste functionaliteit.

De basiskosten voor de HLR/AuC zelf (Home Location Register en bijbehorende Authentication Center) bedragen bij grote aantallen zo'n 1 a 2 Euro per subscriber. Daar komen dan nog bij: maatwerk inrichting van de (nieuwe) HLR-proxy functionaliteit (ordegrootte 50k€ - 200 k€), kosten voor de GGSN (100k€ - 500 k€), koppeling naar MNO's (100k€) en wellicht nog zaken als GMSC en SMSC (100k€ - 500k€). De implementatiekosten zijn naar schatting enkele manjaren (100 k€ - 500k€). Alles bij elkaar betekent dit dat de investeringen voor 5 miljoen subscribers (devices) in de orde van 5,5 M€ - 12 M€ zullen liggen.

De jaarlijkse operationele kosten voor housing, connectiviteit en power bedragen ongeveer 50k€- 200k€, en het beheer kost ongeveer 100 k€ - 400k€ (er van uitgaande dat het beheer wordt ondergebracht bij een partij die dit soort zaken al in portfolio heeft). Daarnaast zijn er administratieve kosten voor het in stand houden van de centrale entiteit (50k€). De operationele kosten komen daarmee uit op zo'n 200 k€ a 650 k€ per jaar.

6 Overwegingen bij toekennen gedeelde MNC's

Binnen het door de overheid voorgestelde model zal een aantal keuzes gemaakt moeten worden. Veel van deze keuzes zullen gemaakt moeten worden voordat een MNC voor opdeling wordt toegekend, omdat deze keuzes randvoorwaarden voor het gebruik met zich mee kunnen meebrengen.

6.1 Eén MNC voor alle toepassingen, of voor een specifieke gebruikersgroep?

Alhoewel het technisch niet zo veel uitmaakt hoeveel partijen de "gedeelde MNC" samen delen, komen hier -zoals genoemd in hoofdstuk 5- wel een aantal organisatorische uitdagingen bij kijken. Er zullen immers afspraken gemaakt moeten worden tussen de deelnemende partijen; hoe meer partijen meedoen, en hoe meer divers ze zijn, hoe lastiger het kan zijn om tot overeenstemming te komen. Een manier om de diversiteit binnen een "centrale" entiteit te beperken, en dus de governance eenvoudiger te maken, is het toekennen van een MNC voor een bepaalde doelgroep met grotendeels gemeenschappelijke belangen.

Door een "op te delen MNC" toe te kennen voor een meer specifieke doelgroep[23] zal governance makkelijker kunnen worden. Binnen een dergelijke specifieke groep kunnen dan nog steeds tegenstrijdige belangen spelen, maar zaken als aanbestedingsplicht of wettelijke beperkingen kunnen binnen een dergelijke specifieke groep wel identiek of tenminste makkelijker verenigbaar zijn.

Hierbij zal bekeken moeten worden hoe ver men wil gaan in het definiëren van een specifieke doelgroep, zonder andere partijen buiten te sluiten, en zonder het zo specifiek te maken dat er straks veel andere groepen ook een eigen MNC voor hun specifieke toepassing nodig achten.

Toekenning MNC tbv slimme meters

Zo zal een MNC die toegekend wordt ten behoeve van de slimme meters tot minder discussies in het kader van gezamenlijk gebruik hiervan leiden: de betrokken netbeheerders hebben veelal dezelfde belangen, en moeten voldoen aan dezelfde wettelijke randvoorwaarden zoals aanbestedingsplicht of zaken die voortvloeien uit de energiewet[24]. Bovendien zijn zij er al aan gewend om samen te werken. Nadeel van een dergelijke specifieke toepassing is dat er wellicht straks andere soortgelijke groepen zijn die daarmee uit deze samenwerking uitgesloten worden. Alhoewel de slimme meters een bijzondere positie innemen (zie volgende paragraaf) en het dus wellicht te overwegen is hiervoor een aparte MNC te reserveren, blijven er dan vergelijkbare overstapdrempels voor andere M2M toepassingen.

[23] Bijvoorbeeld door een MNC voor overheidsdiensten en een MNC voor commerciële toepassingen toe te kennen

[24] Voordeel voor de commerciële partijen om een 'eigen' op te delen MNC te hebben is dat zij wellicht juist sneller kunnen schakelen omdat een aanbesteding daar niet nodig is.

Toekenning MNC aan diverse toepassingen met maatschappelijk nut

Een bredere variant hierop is een MNC toe te kennen aan "vitale" maatschappelijke diensten vanuit de overheid, zodat ook andere partijen die aanbestedingsplichtig zijn, en/of een wettelijk vastgestelde of opgelegde taak uitvoeren (zoals de waterschappen) mee zouden kunnen doen. Samenwerking met andere (eveneens aanbestedingsplichtige en/of met een wettelijke taak belaste) instanties is complexer dan samenwerking met organisaties met dezelfde taken en doelstellingen, maar is weer eenvoudiger dan samenwerking met commerciële partijen.

Toekenning aan private applicaties

Er zullen echter ook commerciële partijen uit de private sector zijn die met vergelijkbare vraagstukken zitten en een oplossing zoeken voor hun specifieke M2M toepassing. Indien er een aparte MNC komt voor 'publieke taken', is het daarom zinvol om ook de mogelijkheid te scheppen een soortgelijke MNC toe te kennen aan andere, meer commerciële partijen Hiermee worden de voordelen niet beperkt tot overheidssector maar worden deze ook mogelijk voor commerciële partijen.

Ook deze MNC wordt dan bij een neutrale centrale entiteit (maar wel een andere) ondergebracht. Voor commerciële partijen onderling geldt ook dat tegenstrijdige belangen zouden kunnen ontstaan indien belangen van partijen uiteenlopen, bijvoorbeeld omdat ze hele andere functionaliteit verwachten van een centrale entiteit, of juist omdat ze directe concurrenten zijn van elkaar en juist concurreren op functionaliteit (en deze dus niet gezamenlijk zouden willen onderbrengen in één entiteit). Ook hier zullen de deelnemers dus aandacht aan de governance structuur moeten besteden. Net als bij de 'publieke taken' ligt het voor de hand dat de centrale entiteit een "non-profit" organisatie moet zijn, zodat deze alleen in het belang van de deelnemers blijft werken.

6.2 Randvoorwaarde gebruik MNC

Aan het gebruik van de MNC dienen vanuit praktisch oogpunt een aantal randvoorwaarden te worden gesteld. Deze precieze randvoorwaarden zullen vormgegeven moeten worden voordat de MNC ter opdeling wordt toegekend aan een of meerdere partijen. Dit zijn onder meer de technische voorwaarden, zoals het niet gebruiken van de MNC voor het identificeren van een radionetwerk als "home netwerk". Daarnaast zullen voorwaarden voor "verstandig uitdelen van IMSI sub-reeksen" moeten worden gesteld, om te voorkomen dat door onhandig opdelen de MNC snel is uitgeput. Hierbij kan gedacht worden aan opdeling in kleine reeksen (van bijvoorbeeld 10.000 IMSI nummers) voor nieuwe toetreders, waarbij pas wordt overgegaan op toekenning van grote reeksen (van 100.000 of meer IMSI nummers) steeds als de voorgaande reeks voor 80% daadwerkelijk in gebruik is. Dit voorkomt dat overoptimistische deelnemers meteen een miljoen nummers reserveren, waarvan uiteindelijk er maar een paar duizend gebruikt worden, ook omdat het lastig is eenmaal uitgegeven IMSI reeksen terug te vorderen.

6.3 Netbeheerders en Slimme Meters

De grootschalige uitrol van "Slimme Energie Meters" start begin 2014 met het doel om uiteindelijk alle Nederlandse huishoudens van een dergelijke meter te voorzien. De slimme meter gebruikt een communicatiekanaal om de meterstanden periodiek te versturen. Voor de communicatie wordt onder meer gebruik gemaakt van GPRS (of op termijn LTE). Hiermee spelen de uitdagingen zoals geschetst voor M2M dus op korte termijn, en zoeken de netbeheerders naar manieren om na afloop van een contract eenvoudig (dus zonder SIM-wissel) van telecomprovider te kunnen wisselen.

De energiesector streeft naar een combinatie van telecomoplossingen, die ieder kunnen worden ingezet waar dat het handigst is. Een groot deel van de slimme meters werkt op dit moment met GPRS, omdat dit een proven technologie is waar landelijk dekkende netwerken voor beschikbaar zijn; een deel van de netbeheerders verwacht hier mee door te gaan. Daarnaast wordt er ook gekeken naar CDMA[25] en PLC.

Alhoewel er binnen de sector wel verschillende denkbeelden zijn over de precieze invulling van telecom, komen de belangen sterk overeen en wordt er vanuit onder meer Netbeheer Nederland samen gezocht naar mogelijke oplossingen voor de telecom ten behoeve van slimme meters.

De "slimme meter" neemt in de bredere M2M-discussie een bijzondere positie in ten opzichte van andere M2M toepassingen.

Om te beginnen is de uitrol van de "slimme meter" naar alle huishoudens een wettelijke verplichting, waarbij de elektriciteitsmeters zich binnen in het privédomein van burgers bevinden[26]. Dit maakt toegang tot de meter zeer lastig.

De meter zelf zal maximaal in de orde van een paar honderd euro mogen gaan kosten, en dient idealiter 15 a 20 jaar operationeel te kunnen zijn zonder iemand langs te sturen[27].

Daar komt bij dat, terwijl de slimme meter voor tenminste 15 à 20 jaar geplaatst zal moeten worden, het ondoenlijk is met aanbieders van telecom afspraken over dergelijke termijnen te maken. Toch zal de "slimme meter" nu uitgerold moeten worden, en zal dus nu moeten worden gezorgd voor een zo groot mogelijke flexibiliteit, niet eens zo zeer voor de eerste paar jaar, maar vooral voor over 8, 15 of 20 jaar.

Daarnaast is de "slimme meter" met zo'n 7 miljoen aansluitingen op dit moment de grootste toepassing van M2M die binnen Nederland concreet uitgerold gaat worden. Andere denkbare toepassingen met een vergelijkbare schaal zijn toepassingen op automotive-gebied (E-call, kilometerheffing), maar deze zijn op dit moment minder concreet.

---

[25] Ook voor CDMA zijn identifiers in de vorm van IMSI's nodig. Afhankelijk van de aard van het netwerk kunnen hier IMSI's gebruikt worden zoals voorgesteld in het ontwerpbesluit "netwerkintern gebruik van IMSI-nummers in niet-openbare netwerken". Als een netbeheerder echter "dual-mode" CDMA/GPRS modules wil inzetten dan is dit geen geschikte optie, en ligt gebruik van de hier voorgestelde gedeelde MNC meer voor de hand.

[26] Dit is niet in alle landen zo; Sommige andere landen gebruiken elektriciteitsmeters die zich aan de buitenkant van woningen bevinden zodat toegang daar eenvoudiger is.

[27] Langs sturen van een monteur (voor onderhoud of SIM-wissel) is relatief duur ten opzichte van deze totale kosten.

Vanuit de Netbeheerders bezien vormt een 'eigen' MNC die binnen de energiesector gedeeld kan worden voor slimme meters een oplossing voor een aantal van deze problemen. Zo kan men na afloop van het telecomcontract wisselen van operator zonder SIM-wissel, en ontstaat flexibiliteit over de af te sluiten contracten; met een eigen MNC kunnen zij dit alles sneller opzetten dan in een constructie met nog andere partijen. Verder is er de wens vanuit de netbeheerders zelf in grote mate hun "slimme meter" keten in te richten, en om dit te kunnen willen ze graag ook grote delen van de telecomketen in eigen beheer kunnen uitvoeren.

Samenwerking binnen de energiesector ligt voor de hand: deze partijen delen veel uitgangspunten, waardoor governance van een entiteit voor een 'slimme-meter-MNC' veel minder een uitdaging vormt dan het geval is als hierbinnen ook andere belangen spelen. Omdat ze gewend zijn met elkaar samen te werken zal een dergelijke entiteit ook relatief eenvoudig en snel ingericht kunnen worden.

Samenwerking met andere partijen die op vergelijkbare wijze een publiek belang dienen is hierbij ook nog mogelijk, mits de entiteit zo is ingericht dat de wensen op het gebied van autonomie en eigen controle over de telecomketen zijn meegenomen en de langere termijn zekerheden voor de netbeheerders geborgd zijn. Deze andere partijen zouden dan ook idealiter in vergelijkbare termijnen denken, omdat de zekerheden vanuit de netbeheerders bezien voor tenminste 15 à 20 jaar (levensduur slimme meter) geborgd moeten zijn. Deelnemende partijen met een veel kortere horizon zijn bijvoorbeeld minder genegen om veel te investeren in de kwaliteit van de gezamenlijke voorziening, zeker als al van plan zijn om op korte termijn uit de samenwerking te stappen. Daar komt bij dat vanuit telecom perspectief de termijn van 15 à 20 jaar bijzonder lang is.

7 Samenvatting

7.1 Voorgestelde oplossing

De voorgestelde oplossing, waarbij een gedeelde MNC wordt gebruikt om aan grootschalige M2M gebruikers een IMSI sub-reeks toe te kennen, is technisch haalbaar en kan er voor zorgen dat overstapdrempels worden weggenomen. Wel dient er een "HLR-proxy" te worden ingericht en beheerd om dit mogelijk te maken, en dient er voor gewaakt te worden dat de afhankelijkheid van een commerciële aanbieder van telecomdiensten wordt ingeruild voor afhankelijkheid van deze beheerpartij. Deze partij dient daarom neutraal richting de deelnemers, en non-profit te zijn. Dit kan worden gerealiseerd door de centrale beheerpartij waar deze proxy is ondergebracht zo in te richten dat de deelnemers eigenaar zijn en/of zeggenschap hebben.

Het verdient aanbeveling de centrale entiteit zo in te richten dat er zo min mogelijk tegenstrijdige belangen een rol kunnen spelen bij besluitvorming binnen deze entiteit. Dit kan onder meer door zo min mogelijk functionaliteit centraal te beleggen (zodat over implementatie en kosten van deze functionaliteit geen discussies ontstaan) en door aparte MNC's toe te wijzen aan sectoren met fundamenteel andere belangen, zoals aanbestedingsplichtige versus niet aanbestedingsplichtige gebruikers.

7.2 Eén of twee MNC's ?

Er spelen bij de vraag omtrent het toekennen steeds twee vraagstukken door elkaar, waarbij de eerste vraag de dynamiek in de M2M markt in algemene zin betreft, en de tweede specifiek van toepassing is op de aanstaande wettelijke uitrol van slimme meters.

> *Is het wenselijk om de omschreven mogelijkheid om overstapdrempels op de M2M markt weg te nemen in bredere zin in te zetten voor allerlei toepassingen?*

Om de markt voor die M2M toepassingen die zitten met overstapdrempels verder te flexibiliseren zal het antwoord op de eerste vraag zijn dat het inderdaad wenselijk is om deze mogelijkheid in brede zin beschikbaar te maken voor M2M, zowel voor commerciële toepassingen als voor toepassingen van overheidswege, en zowel voor grootschalige, als wellicht voor meer kleinschalige toepassingen. Over de benodigde schaal hoeft overigens niet direct een oordeel te worden geveld: marktpartijen zullen zelf de afweging maken of het de moeite en kosten van deze oplossing waard is om extra flexibiliteit te verkrijgen. Wel speelt binnen dit vraagstuk de discussie rondom de aanbestedingswet en de behoefte om voor langere tijd een bepaalde maatschappelijke taak gegarandeerd te ondersteunen vanuit de telecomoplossing. Er kan er voor gekozen worden twee MNC's beschikbaar te maken, waarbij er een MNC is voor maatschappelijke toepassingen met een aanbestedingsplicht, en een MNC voor tevens meer commerciële toepassingen.

> *Is het mogelijk/wenselijk om voor een specifieke toepassing onder bepaalde omstandigheden zoals het dienen van een wettelijk vastgelegd maatschappelijk belang een "eigen" MNC toe te kennen?*

Dit betreft op korte termijn vooral de "slimme meter" en staat deels los van de eerste vraag. De energiemeters vormen een speciaal geval, en het ligt niet in de lijn der verwachting dat er in de komende jaren veel vergelijkbare toepassingen op die schaal en met een vergelijkbare wettelijke verplichting tot uitrol in het privédomein zullen komen.

Gegeven het specifieke karakter van de slimme meter kan goed beargumenteerd worden dat er een aparte MNC voor deze sector wordt toegekend, waarbij de governance en afspraken binnen de beheers-entiteit kunnen worden toegespitst op de uitrol van de slimme meter zodat ook in de toekomst, bij verdere uitrol van "smart grids", deze entiteit specifiek voor dat doel is toegerust. Echter kan deze toepassing ook worden ondergebracht bij een meer brede maatschappelijke MNC indien deze zo wordt vormgegeven dat er voldoende lange termijn zekerheid ontstaat voor de deelnemende partijen. Deze zekerheid kan bijvoorbeeld ontstaan doordat deze MNC wordt toegekend ten behoeve van toepassingen die vergelijkbare karakteristieken bezitten, zoals toepassingen waarbij het onevenredig lastig is de SIM te wisselen en waarbij apparaten voor (zeer) lange perioden dienst moeten kunnen doen. Dergelijke zaken zouden in de statuten van de entiteit geborgd moeten worden, waarbij Autoriteit Consument en Markt[28] een rol kan spelen bij handhaving van deze voorwaarden en toezicht op de mate waarin de statuten deze zaken en de mogelijkheid voor nieuwe toetreders borgen. Indien deze zekerheden zijn geborgd, dan is deelname aan de "brede" overheids-MNC voor slimme meters zeker mogelijk. Daar staat tegenover dat de netbeheerders ook bij samenwerking met andere (weliswaar overheids-) partijen uitdagingen zien op het gebied van de samenwerking, omdat ook daar de belangen uiteen kunnen lopen. Zo gaat het bij de slimme meter om uitzonderlijk hoge aantallen, en hebben ze de wens zelf 'hun' keten in eigen beheer in te richten en te beheren.

7.3 Aandachtspunten Telecomdienstverlening

Deelnemers aan een "gedeelde MNC" nemen geen totale telecomdienst af van de mobiele operator, maar hebben dankzij de eigen IMSI sub-reeks de mogelijkheid diverse onderdelen in de keten 'los' te verkrijgen of in te richten. Dit brengt een nieuwe dynamiek met zich mee.

Door de voorgestelde constructie kunnen verschillende onderdelen van de keten bij verschillende partijen worden ondergebracht, waardoor ook op dat vlak meer dynamiek ontstaat. Consequentie is wel dat de telecomketen niet meer "end-to-end" bewaakt wordt door één aanbieder, maar dat er een aantal extra interfaces -met bijbehorende beheer en SLA afspraken- gemaakt zullen moeten worden, waarvoor ook technische telecomkennis bij de centrale entiteit en bij de M2M deelnemers nodig is. Voor grote partijen is dit wellicht niet direct een probleem (maar een afweging die ze zullen moeten maken), maar hier dient bij deelname in een gezamenlijke MNC wel duidelijk rekening mee te worden gehouden.

[28] Voorheen de OPTA (zie www.acm.nl)

Annex A Beantwoording onderzoeksvragen

Algemeen

1) Ontwikkelingen op het vlak van Over The Air programming (OTA) kunnen een deel van de problematiek waaruit de behoefte aan eigen IMSI-nummers voortkomt wegnemen. OTA is veelbelovend maar heeft beperkingen, zo is nog altijd een MNO of MVNO nodig om deze techniek te ondersteunen. In dit kader speelt de vraag in hoeverre het gebruik van OTA en eigen IMSI-nummers elkaar zouden kunnen aanvullen om in deze behoefte te voorzien.

Alhoewel er veel plannen zijn op het gebied van OTA herprovisioning van IMSI nummers is hier nog geen goed bruikbare standaard voor.
Zolang het OTA-herprovisionen alleen het "switchen" tussen twee IMSI-nummers betreft, zullen deze op voorhand in geprogrammeerd moeten zijn. Dit betekent dat de tweede IMSI al toegewezen moet zijn, en dat de M2M-operator dus al een contract moet hebben met de aanbieder van deze 2e IMSI. Naar alle waarschijnlijkheid zal hij daar ook voor zal moeten betalen, omdat ook deze 2e aanbieder de IMSI's zal moeten provisionen (o.a. capaciteit HLR).
Het Over The Air programmeren van een nieuwe, nog niet eerder toegewezen IMSI (plus bijbehorende sleutel) is een veel complexere zaak, en op dit moment feitelijk niet mogelijk. Alhoewel hier in de toekomst wellicht nog ontwikkelingen zullen plaatsvinden is dit op korte of middellange termijn niet haalbaar.
Een belangrijk obstakel voor Over The Air programmeren van een nieuwe IMSI is dat hiervoor medewerking van de bestaande operator nodig is (mobiele operator of MVNO). Dit obstakel kan weliswaar weggenomen worden door eigen IMSI's te gebruiken, maar in dat geval heeft de Over The Air programmering feitelijk geen meerwaarde aangezien de vereiste flexibiliteit dan al bereikt is.
Er zijn initiatieven om dit probleem op te lossen door een "trusted third party" in te richten die over IMSI's beschikt en die toegang krijgt tot alle netwerken; dit lost het probleem echter niet geheel op aangezien de gebruiker dan alsnog een "lock-in" heeft bij deze trusted third party (feitelijk is dit een MVNO).
Een additioneel probleem bij Over The Air programmering is dat dit type actie niet altijd slaagt. Als een device door een mislukte programmering niet via de nieuwe IMSI kan communiceren, maar ook niet meer via de oude, is het device onbereikbaar geworden en moet er een monteur naar toe. Gezien de grote aantallen M2M devices die de komende jaren verwacht worden is dit, zelfs bij een zeer gering percentage foutgevallen, nog altijd een aanzienlijke kostenpost.

2) Wat zijn algemeen gezien de voor- en nadelen voor partijen die gebruik maken van de gedeelde MNC, afgezet tegen de roaming mogelijkheden die deze partijen hebben onder eventueel te maken afspraken tussen MNO's in verband met storingen in mobiele netwerken? Hoe werkt dit uit voor de communicatie met slimme meters?

Zowel bij gebruik van de MNC van een MNO of MVNO, als bij gebruik van een eigen, gedeelde MNC, is het mogelijk roaming afspraken te maken. Een voordeel van een eigen MNC is daarbij dat de gebruiker die afspraken zelf kan maken en inregelen, terwijl bij

gebruik van de MNC van een MNO hiervoor medewerking van de MNO noodzakelijk is. Indien de gedeelde eigen MNC bij een neutrale partij belegd is die al verbindingen heeft met alle MNO's, dan is nationale roaming zelfs gemakkelijk in te richten.
Deze oplossing staat los van de mogelijke implementatie van national roaming tussen operators onderling om de gevoeligheid voor storingen te verminderen. Daarbij worden weliswaar dezelfde roaming mechanismen gebruikt, maar de benodigde technische en commerciële afspraken zijn geheel anders.
Ongeacht de gekozen oplossing zou een roaming mogelijkheid voor grootschalige M2M gebruikers bij storingen in mobiele netwerken grote risico's met zich meebrengen. Het gaat immers potentieel om miljoenen devices die, als een netwerk faalt, zich op een ander netwerk aan zullen melden, met een enorme hoeveelheid extra signaleringsverkeer als gevolg. Grootschalige M2M gebruikers zullen daarom in beide scenario's hun devices, in overleg met de mobiele operators, zo in moeten stellen dat het roaming verkeer in alle gevallen beperkt wordt.

3) Toekenning van een MNC aan specifiek de netbeheerders in de energiesector zou kunnen worden gestoeld op de omstandigheid dat het gaat om apparaten gaat die zijn opgesteld in het privédomein van consumenten, wat specifieke gevolgen heeft voor het beheer van deze apparaten. De vraag is hier of dit op de wat langere termijn wellicht minder precedentrisico oplevert dan de in het voorgaande genoemde andere criteria hiervoor, en zonder dat hierdoor asymmetrische behandeling van bedrijven ontstaat.

De "slimme meter" vormt een speciaal geval. Zo betreft het een apparaat in privé-domein (waardoor een SIM wissel zeer hoge kosten met zich meebrengt) en zijn de netbeheerders van overheidswege verplicht om deze dienst te gaan leveren. Daar komt bij dat het bij de 'slimme meter' gaat om op dit moment de meest concrete zeer grootschalige toepassing die ook nog eens voor 15 tot 20 jaar operationeel dient te blijven zonder dat er onderhoud aan de meter gepleegd zal worden. Deze zaken maken dat er vanuit toekenning aan deze partijen minder precedentwerking uit zal gaan dan bij toekenning aan anderen. Er zijn immers niet veel applicaties denkbaar waarvoor deze afwegingen ook gelden. Een MNC toekennen voor gebruik in de slimme meters zal daardoor op deze wijze onderbouwd kunnen worden zonder dat veel andere toepassingen om dezelfde redenen een eigen MNC zouden willen verkrijgen. Wat wel blijft is dat het toekennen ten behoeve van een specifiek doel met zich mee brengt dat er wellicht later toch weer andere, eveneens specifieke toepassingen, ook een MNC zouden kunnen aanvragen.

Een iets ruimere optie zou zijn om een gedeelde MNC te reserveren voor instellingen binnen de overheid met een bijzondere maatschappelijke taak en de bijzondere sectoren[29] (waarvan de netbeheerders de eerste zouden zijn).

Het voordeel van deze ruimere optie is dat ook deze organisaties in de toekomst kunnen deelnemen in de MNC (en er dus niet nog meer MNC's toegekend hoeven te worden) en

[29] De bijzondere sectoren zijn limitatief opgesomd in het Besluit Aanbestedingen Bijzondere Sectoren, en dus eenduidig vast te stellen. Enkele voorbeelden zijn de netbeheerders voor elektriciteit, gas, warmte, en drinkwater, en ProRail als beheerder van het spoorwegnet.

op die manier dus wordt voorkomen dat er juist precedentwerking uitgaat van "het toekennen voor een specifiek doel".

Er zullen echter meer partijen (bijvoorbeeld uit de private sector) kunnen zijn die ook met dergelijke praktische overstap barrières zitten. Indien er een aparte MNC komt voor 'publieke taken' zoals hierboven genoemd kan het daarnaast zinvol zijn om ook voor andere dergelijke partijen te kijken naar mogelijkheden voor toekenning van eenzelfde type op te delen MNC voor overige, meer commerciële partijen, waarbij hier wel zal moeten gezorgd dat ook deze bij een (maar wel een andere) neutrale centrale entiteit wordt ondergebracht.

4) Een andere weg zou kunnen zijn als criterium voor toekenning van een MNC te hanteren dat een bepaald minimum aantal aansluitingen met een MNC moet worden bediend. Omdat het vooral bij M2M van belang is waarbij grote aantallen aansluitingen zijn betrokken, kun je denken aan een hoog aantal (miljoenen). Het werpt een drempel op voor aanvragen door individuele bedrijven. Dit is echter mogelijk niet toekomstbestendig als de bv. de M2M sector snel door blijft groeien waardoor de kans bestaat dat een dergelijke grens later opgehoogd moet worden. Dit geeft juridische onzekerheid. Zou een dergelijk criterium toch op een of andere manier kunnen worden gebruikt?

Het opwerpen van een drempel door een minimum aantal gebruikers te vragen kan er voor zorgen dat het aantal MNC's beperkt blijft. Als er een grens van (bijvoorbeeld) 3 miljoen aansluitingen wordt gehanteerd, kunnen feitelijk alleen de gezamenlijke energiebedrijven en de gezamenlijke automotive dienstaanbieders een MNC aanvragen.

Nadeel van deze constructie is echter dat voor andere, wellicht ook relevante maar kleinschaligere M2M toepassingen geen flexibele gebruiksmogelijkheden ontstaan, want zodra deze twee toepassingen een eigen MNC hebben zijn er van alle overige toepassingen voorlopig niet genoeg aansluitingen meer te verwachten om vanuit een centraal platform aan deze eis te voldoen. Het ligt dan ook voor de hand dat de grens na enkele jaren, eerder verlaagd dan verhoogd zal worden. Daarmee komt een MNC binnen bereik voor platformen die een groot aantal niche toepassingen ondersteunen, terwijl het aantal benodigde MNC's beperkt blijft.

Gesteld kan dus worden dat alhoewel het stellen van een drempel aan het aantal aansluitingen dit weliswaar het aantal aanvragen zal beperken, het erg moeilijk is deze drempel objectief en zonder "onterechte" uitsluiting van andere toepassingen voor lange termijn vast te stellen.

Aspecten t.a.v. de implementatie van het gedeelde gebruik van een MNC

5) In hoeverre is het zinvol om het gebruik van de gedeelde MNC te beperken tot het routeren van elektronische signalen, waarbij de MNC dan dus niet mag worden gebruikt ten behoeve van een eigenstandig netwerk, gelet op bijvoorbeeld beheers-aspecten? Is bij deze beperking te verwachten dat in een bepaalde behoefte in de markt op het vlak van IMSI-nummers niet wordt voorzien?

De MNC speelt in mobiele netwerken diverse rollen. Het routeren van elektronische signalen is er daar 1 van, maar daarnaast wordt de MNC gebruik in andere onderdelen van mobiele netwerken, zoals als deel van de "id" van gebruikers in een HLR-roaming situaties, en ter identificatie van een fysiek radionetwerk.

Het heeft grote voordelen om de gedeelde MCC/MNC niet te laten uitzenden ter identificatie van een netwerk omdat er daardoor problemen kunnen ontstaan als een "slimme meter" probeert zich bij een dergelijk netwerk aan te melden. Een beperking tot het routeren van signalen is daarvoor niet nodig; om de genoemde problemen volstaat een verbod om de betreffende MNC in een radio netwerk uit te zenden als identificatie van dat netwerk. Een gebruiker van een privaat GSM netwerk kan de MNC dan nog steeds gebruiken voor zijn SIM's en voor zijn roaming afspraken, en intussen een andere MNC uitzenden (bijvoorbeeld een MNC zoals benoemd in het voorgenomen "Besluit netwerkintern gebruik van IMSI-nummers in niet-openbare netwerken"). Zie in het rapport hoofdstuk 2 en 4.

Indien de stringentere beperking wordt gehanteerd waarbij "gebruik ten behoeve van een eigenstandig netwerk" wordt voorkomen wordt ook voorkomen dat partijen met private GSM/LTE netwerken een sub-MNC zouden gaan gebruiken voor eigen roaming contracten. Dit is een beperking, aangezien er op termijn wel een behoefte te voorzien valt voor gebruik van IMSI-nummers ten behoeve van dergelijke private netwerken.

6) In hoeverre beperkt het voorziene gebruiksmodel partijen die behoefte hebben aan een zo groot mogelijk eigen beheer van IMSI-nummers en SIM-kaarten? Om welke beheers-aspecten gaat het daarbij? In hoeverre heeft dit een relatie met het: 1) beveiligen van mobiele communicatie, 2) de continuïteit hiervan, 3) kosten, en 4) de mogelijkheden om beheer over eigen SIM-kaarten te kunnen voeren, waaronder de productie hiervan?

Partijen die participeren in een gezamenlijke entiteit die een MNC beheert, kunnen kiezen of zij de centrale entiteit ook de HLR/AuC laten beheren, of dit zelf doen.

Indien de HLR centraal wordt ingericht dan ligt het voor de hand ook centraal de SIM-kaarten te laten maken, waardoor keuze over SIM-kaarten een gezamenlijke aangelegenheid wordt en dus minder "eigen beheer" is. Dit betekent ook dat een partij dan zelf minder controle heeft over de veiligheid (dit is immers een gemeenschappelijke verantwoordelijkheid geworden). Bij centrale inkoop SIM-kaarten kan er een schaalvoordeel ontstaan, maar heeft de gebruikende partij er minder controle over. Bovendien bezit de centrale entiteit dan de sleutels van alle SIM's, en moeten er dus hoge eisen aan de beveiliging van deze entiteit gesteld worden;

Als de centrale entiteit echter alleen een doorgeefluik realiseert dan kunnen de SIM-kaarten decentraal in eigen beheer van de p-MVNO's worden gemaakt/ingekocht. Bij decentrale inkoop zullen door de deelnemers zelf (wellicht deze zelfde) eisen op het gebied van veiligheid gesteld worden. Hierbij hebben de deelnemers dus wel meer zeggenschap over de IMSI-reeks, de SIM-kaarten, en de veiligheidseisen. Wel zal ook in dit 'uitgeklede' gebruiksmodel centraal overeenstemming dienen te zijn over zaken als redundantie en beveiliging van de proxy-functionaliteit.

Naar verwachting zal het kostenverschil tussen centrale of decentrale inkoop van SIM's veel kleiner zijn dan het kostenverschil tussen een centrale core en een aantal decentrale p-MVNO cores.

Bij centrale inrichting zal ook de optionele functionaliteit wellicht centraal worden ondergebracht. Naarmate er meer gezamenlijk gebeurt wordt het wellicht lastiger om overeenstemming te krijgen over inrichting van de centrale systemen (wat gaan we precies doen?) en de kosten hiervoor (wie betaalt wat?). Besluitvorming/governance kan dan dus lastiger zijn. Bij een meer decentrale core (en dus een 'kale' centrale entiteit) zal dit naar verwachting veel minder spelen: De partijen beslissen zelf over wat ze wel en niet willen inrichten, en hoeven het alleen eens te zijn over het (kleine) centrale deel waar dus ook minder moeite en geld mee gemoeid is.

7) Hoe spelen de in punt 5 genoemde aspecten in het geval van de uitrol van slimme energiemeters? Deze vraag dient te worden beschouwd in de context dat de netbeheerders ook op andere vlakken relaties hebben met commerciële partijen. Ook speelt hierbij bijvoorbeeld de vraag wat de relatie precies is tussen het beheer van de gedeelde MNC, het risico van discontinuïteit van de beoogde communicatie, en de eventuele gevolgen van deze discontinuïteit voor de energielevering.

Geen gebruik t.b.v. eigenstandig netwerk

Voor de slimme meters geldt dat het in eerste instantie niet de bedoeling van de netbeheerders is om de MNC te gebruiken voor een eigenstandig netwerk. In theorie is het echter mogelijk dat zij op plaatsen met slechte dekking een privaat netwerk in zouden richten (GSM/LTE in de 1800 MHz band).

Risico van discontinuïteit van de beoogde communicatie

Indien de gedeelde MNC's en bijbehorende IMSI-reeksen wel ook voor eigenstandige netwerken zoals private GSM netwerken gebruikt mogen worden, dan bestaat er een groot risico op problemen voor die slimme meters die zich in de nabijheid van dit netwerk bevinden. In dat geval kan het immers voorkomen dat de slimme meter zich op dit netwerk probeert aan te melden; aangezien dat niet zal lukken zal de meter het steeds opnieuw proberen. Dat levert een extra belasting van zowel de slimme meter als het private netwerk.

Dit kan voorkomen worden door een verbod om de betreffende MNC in een radio netwerk uit te zenden als identificatie van dat netwerk.

***Is te verwachten dat in een bepaalde behoefte op het vlak van IMSI-nummers niet wordt voorzien** [bij het beperken van gebruik van de gedeelde MNC tot het routeren van elektronische signalen] ?*

In het geval de netbeheerders zouden besluiten om op plaatsen met slechte dekking een privaat netwerk in te richten, zou een dergelijke beperking ze daarin belemmeren. Dit scenario is echter vrij onwaarschijnlijk, aangezien er voor het beperkte aantal locaties waar geen GSM dekking is veel betere opties bestaan.

8) Wat zijn, gelet op het genoemde in punt 6, de voor- en nadelen voor de netbeheerders van participeren in een gedeeld gebruik van een MNC ten opzichte van de situatie dat de netbeheerders een eigen MNC wordt toegekend?

Beveiliging

In het algemeen kan gesteld worden dat hoe meer partijen er in de keten betrokken zijn hoe lastiger het is om de beveiliging geheel naar eigen wensen in te richten. Zo zal binnen de centrale entiteit (in beide scenario's) in overleg de beveiliging moeten worden geregeld. Als de centrale entiteit onder controle van de netbeheerders staat dan is dit vanuit de netbeheerder bezien dus beter te controleren (ze hebben naar verwachting vergelijkbare wensen en eisen met betrekking tot de beveiliging) dan als hier allerlei andere partijen aan mee doen.

Voor wat betreft authenticatie geldt dat het in eigen hand hebben van de sleutels op SIM-kaarten en in de HLR voor de netbeheerders een grotere zekerheid geeft dan als deze bij een centrale partij zijn ondergebracht.

Beheer eigen SIM-kaarten

Voor een gedeelde MNC, waarbij we uitgaan van de "uitgeklede variant" waarbij de centrale entiteit alleen een "HLR-proxy" inricht, zijn de netbeheerders technisch vrijwel net zo flexibel als met een eigen MNC.

Kosten

De uitdagingen liggen bij een gedeelde MNC voornamelijk in het governance en continuïteits-vraagstuk, waarbij kosten snel een belangrijke rol zullen spelen in discussies: als er meerdere partijen zeggenschap hebben in de centrale entiteit (of in de toekomst zeggenschap kunnen krijgen), met wellicht andere belangen, dan is er een risico dat op termijn de HLR-proxy steeds meer 'toeters en bellen' zal krijgen om ook andere partijen te faciliteren in hun specifieke wensen. Dit is iets wat voor de netbeheerders een nadeel zou zijn ten op zichtte van een "eigen" MNC.

Ook aanbestedingsplicht en de energiewet kunnen een rol spelen: vanuit de netbeheerders bezien zal de door hen opgerichte centrale entiteit ook aanbestedingsplichtig zijn, en zal deze entiteit geen commerciële activiteiten mogen ontplooien. Commerciële deelnemers kunnen hier anders over denken. Dit vormt een nadeel voor de netbeheerders: de centrale entiteit moet in eerste instantie, maar ook over 15 jaar, nog aan de wettelijke randvoorwaarden kunnen voldoen. Mocht in die tijd de Aanbestedingswet of de Energiewet aangepast worden, dan kunnen de netbeheerders wellicht niet meer onder dezelfde voorwaarden deel blijven nemen in de centrale entiteit, terwijl ze er technisch wel aan vast zitten. In het ergste geval zullen ze alsnog alle SIM's moeten wisselen om aan nieuwe wetgeving te kunnen voldoen. Deze problemen spelen niet bij een centrale entiteit die alleen de netbeheerders bedient, aangezien zij allemaal onder dezelfde wetgeving vallen. Het verbod voor de netbeheerders om commerciële activiteiten te ontplooien is op te lossen door deze voorwaarde door te trekken naar de

centrale entiteit, en te stellen dat deze entiteit geen commerciële activiteiten mogen worden ontplooid.

9) Zijn er algemeen gezien organisatorische moeilijkheden te voorzien indien zowel instanties met maatschappelijke functies als commerciële marktpartijen in het beoogde gebruiksmodel moeten samenwerken?

Hier zit een aantal uitdagingen aan.

Veel instanties met maatschappelijke functies, waaronder de netbeheerders, hebben een aanbestedingsplicht, commerciële partijen niet. Dit betekent dat de gezamenlijke entiteit in principe zal moeten aanbesteden.

Daar komt bij dat verschillende partijen kunnen zeer uiteenlopende verschillende doelstellingen hebben (en zullen daarmee ook andere functionaliteit, beschikbaarheid, etc. verlangen van de centrale entiteit) voor de systemen voor de "gedeelde MNC".

Dit kan ook al spelen bij maatschappelijke partijen onderling (bijvoorbeeld omdat de aantallen verschillen, of omdat sommige wel en andere geen sms-service nodig hebben), maar naar verwachting zullen de verschillen met commerciële partijen groter zijn.

Dit kan deels opgelost worden door te kiezen voor de variant waarbij de centrale entiteit zo weinig mogelijk functionaliteit realiseert, maar het is lastiger te borgen dat dit ook zo blijft, maar ook dan blijft dit een punt van zorg, mede omdat aanbestedingsplicht en de technische inrichting van de HLR-proxy gezamenlijk zullen moeten worden vormgegeven.

De inrichting van de governance-structuur is dus in beide varianten van groot belang, en deze zal zo moeten zijn dat bepaalde zekerheden die in het begin (bijvoorbeeld omdat er alleen instanties met maatschappelijke functies deelnemen) gewaarborgd zijn, ook in de toekomst zeker zullen blijven, ook als op termijn een meerderheid van de deelnemers commercieel is en/of veel andere functionaliteit wenst.

10) Indien verschillende entiteiten als BTG en de netbeheerders bereidwillig zouden zijn om samen te werken, hoeveel tijd zou er dan zijn om het gedeelde gebruik van een MNC te implementeren, en om de beoogde roaming situatie te realiseren? Welke eventuele technische, organisatorische en commerciële aspecten spelen daarbij een rol en/of kunnen knelpunten vormen?

Voor het inrichten van het technische gedeelte (zowel in de variant waarbij een volledige core wordt ingericht als in de variant waarbij centraal alleen een HLR-proxy wordt gerealiseerd en de partijen zelf een "core" inrichten) zou 6 tot 10 maanden volstaan. Dit is onder de aanname dat precies duidelijk is wat er gerealiseerd dient te worden.

De doorlooptijd voor een eventuele aanbesteding voor inrichting en beheer van de centrale HLR-proxy en MVNO-core komt hier nog bij (ongeveer 12 maanden).

Aangezien een aanbesteding in de praktijk pas kan starten als er enkele basisafspraken gemaakt zijn over de toekomstige structuur en governance, zal de totale doorlooptijd ongeveer twee jaar bedragen, en wellicht langer als het samenwerking tussen diverse partijen zoals maatschappelijke partijen en commerciële partijen betreft die dit samen zouden inrichten.

Een centrale entiteit van alleen netbeheerders met hun slimme meters zou in principe sneller kunnen schakelen, omdat de governance eenvoudiger kan zijn alle participanten hebben immers vrijwel identieke belangen, en er wordt binnen de sector al veel samen nagedacht op het gebied van slimme meters. Naar verwachting zou voor de netbeheerders een dergelijke oplossing in zo'n 14-18 maanden gerealiseerd kunnen worden. Alhoewel deze oplossing er dus niet is op het moment dat de grootschalige uitrol van start gaat (en de netbeheerders naar verwachting in eerste instantie dus nog operator-SIM's of andere oplossingen zullen gebruiken) kan dan vanaf eind 2014 wel gebruik worden gemaakt van de gedeelde MNC.

Voor een overheidsvariant hangt de doorlooptijd sterk af van hoeveel partijen direct deelnemen. Als het alleen de netbeheerders zijn dan is de doorlooptijd vergelijkbaar. Als er ook anderen meedoen dan is snel meer tijd nodig (naar schatting wellicht enkele maanden) om tot overeenstemming te komen: Wie doet er mee, wat wil men precies, waar ligt de gemeenschappelijke deler? Dit hangt ook af van de manier waarop de MNC's toegekend gaan worden en samen worden gebracht. (Kunnen partijen zich aanmelden bij de ACM (voorheen OPTA), en brengt de ACM ze samen?)

NB: Ook het onderbrengen van de MNC bij bijvoorbeeld (enkel) de BTG zou sneller kunnen gaan omdat deze organisatie er al is.

Om te borgen dat partijen ook later kunnen toetreden en er geen oneigenlijke drempels ontstaan, kan ACM toezicht houden op de statuten en toetsen of deze voldoen aan de randvoorwaarden zoals gesteld bij toekennen van de MNC.

11) Wat zijn de verwachte kosten van de implementatie van een gedeelde MNC voor de partijen die deze MNC gezamenlijk beheren? Hiervoor dient een schatting te worden gemaakt.

De kosten die gemaakt moeten worden bestaan uit het inrichten van de basis MVNO-core functionaliteit. Indien elke deelnemer een eigen MVNO-core inricht dan zijn de kosten van de gezamenlijke entiteit beperkt. Het gemeenschappelijke deel bestaat dan alleen uit de "HLR-proxy": een signalling gateway, een koppeling met alle MNO's en een koppeling met alle deelnemers. De deelnemers moeten dan wel aanzienlijke kosten maken voor de eigen MVNO-core. Zie hoofdstuk 5.3.

Elke MVNO-core bestaat tenminste uit een HLR/AuC, GGSN, GMSC, STP, en diverse koppelingen. De HLR/AuC is daarin het duurste deel. Daar komen dan nog de GGSN, GMSC, en STP bij en eventueel nog netwerkelementen voor extra functies zoals een SMSC. Daarbij komt het maatwerk voor het kunnen differentiëren op IMSI sub-reeks (HLR-proxy of maatwerk HLR).

Indicatie kosten: De kosten voor een Home Location Register en bijbehorende Authentication Center bedragen zo'n 1 a 2 Euro per subscriber, bij grote aantallen. Maatwerk inrichting van de (nieuwe) HLR-proxy functionaliteit kost (ordegrootte) 50k€ - 200 k€, en daarbij komen nog de kosten voor GGSN (100k€ - 500 k€), koppeling naar MNO's (100k€) en wellicht nog zaken als GMSC en SMSC (100k€ - 500k€). De implementatiekosten zijn naar schatting enkele manjaren (100 k€ - 500k€). Dit betekent dat de investeringen voor 5 miljoen subscribers (devices) in de orde van 5,5 M€ - 12 M€ zullen liggen. De jaarlijkse operationele kosten voor housing, connectiviteit en powerbedragen ongeveer 50k€- 200k€, en het beheer kost ongeveer 100 k€ - 400k€ (er van uitgaande dat het beheer wordt ondergebracht bij een partij die dit soort zaken al in portfolio heeft). Daarnaast zijn er administratieve kosten voor het in stand houden van de centrale entiteit (50k€). De operationele kosten komen daarmee uit op zo'n 200 k€ a 650 k€ per jaar.

12a) In hoeverre is te verwachten dat, gegeven de situatie dat dit model technisch en organisatorisch kan worden geïmplementeerd, MNO's/MVNO's bereid zijn roaming contracten af te sluiten met de entiteit die de MNC beheert of specifieke groepen eindgebruikers die gebruik maken van deze MNC?

MNO's zullen waarschijnlijk in eerste instantie terughoudend zijn een dergelijke oplossing te implementeren. Commercieel zullen ze immers een deel van hun meerwaarde-diensten verliezen, en ze zullen voor delen van hun dienstverlening meer concurrentie krijgen van onder meer MVNE's en systemintegrators.

Naar verwachting zullen met name de netbeheerders voor hun slimme meters voldoende volume hebben om te zorgen dat (tenminste enkele) huidige MNO's of MVNO's geïnteresseerd zijn in het aanbieden van netwerkcapaciteit en/of aanvullende diensten ten behoeve van het voorgestelde model. Daar komt bij dat voor de uitrol van de slimme meters de keuze voor GPRS nog niet vaststaat, en dat ook zaken als PLC of CDMA worden overwogen.

Indien de MNO's besluiten mee te doen binnen het gestelde model zal er rekening mee moeten worden gehouden dat zaken zoals bijvoorbeeld SLA's en het verhelpen van storingen anders zullen verlopen dan het geval zou zijn bij de huidige M2M-proposities vanuit de operators. MNO's zullen dus geen 'keten' verantwoordelijkheid meer dragen omdat een deel van de keten elders is ondergebracht. Deze verantwoordelijkheid komt dan nadrukkelijk bij anderen te liggen, en SLA's met MNO's zullen alleen nog maar gaan over het 'netwerk gedeelte' omdat dat de dienst is die wordt afgenomen.

12b) In welk opzicht en tegen welke kosten dient een openbare mobiel netwerk te worden aangepast om deze vorm van roaming mogelijk te maken? Voor deze kosten dient een schatting te worden gemaakt.

De aanpassingen in het openbare netwerk zijn voor de verschillende oplossingen vergelijkbaar. De werkwijze zoals deze met National Roaming wordt geïmplementeerd is

ook de manier waarop de huidige MVNO's werken, en de aansluitingen zijn technisch, en dus ook qua kosten, vergelijkbaar. De technische voorzieningen zijn al aanwezig ten behoeve van de MVNO's, en alleen de capaciteit moet uitgebreid worden. Daarnaast heeft een MNO projectkosten om een nieuwe roaming partner te implementeren. Alles bij elkaar zijn de kosten dus vergelijkbaar met het contracteren van een nieuwe ("gewone") MVNO. Ten opzichte van de situatie waarin de M2M gebruiker zich rechtstreeks bij de MNO abonneert is er wel een verschil: eigen aansluitingen staan in een HLR, terwijl bij roaming alleen gebruik wordt gemaakt van de VLR. Dit betekent, zeker omdat het miljoenen aansluitingen betreft (veel meer dan de grootste MVNO op dit moment in Nederland heeft) dat de MNO in dit model een substantieel bedrag bespaart doordat er geen HLR uitbreidingen nodig zijn. Deze besparingen liggen rond de eerder genoemde 1 miljoen Euro per miljoen aansluitingen (waarschijnlijk iets lager, vanwege het schaalvoordeel van de MNO).

Als laatste speelt bij de "gedeelde MNC" dat er bij vele M2M toepassingen (bijvoorbeeld indien deze zich na een storing allemaal tegelijk proberen aan te melden) het risico is op aanmelden op het verkeerde netwerk[30] waar ze geweigerd zullen worden ("reject") en daarmee extra load op deze netwerken. Deze zaken kunnen opgelost worden door slim om te gaan met onder meer instellen van het "preferred netwerk" en zijn dus technisch oplosbaar, en hoeven daarmee geen grote knelpunten te vormen indien hier rekening mee wordt gehouden bij uitrol van de toepassingen.

13) Hoe kunnen IMSI-reeksen onder de gedeelde MNC het beste worden beheerd? Kan dit overgelaten worden aan de eindgebruikers zelf, of dient OPTA[31] hier een rol te spelen, bv. door in het kader van efficiënt nummerbeheer bepaalde IMSI-reeksen toe te kennen aan bepaalde gebruikers(groepen).

Het uitdelen van de 'IMSI-reeksen kan technisch en praktisch het beste gebeuren door de entiteit aan wie de MNC is toegekend door de ACM. Eventueel kunnen bij de toewijzing van de MNC aanwijzingen worden gegeven over de mogelijke te sub-alloceren IMSI-reeksen en voorwaarden waaronder de entiteit deze IMSI-reeksen toekent aan de gebruikers.

Met het oog op de toekomstvastheid zal vanaf het begin duidelijk moeten zijn hoe groot de opdeling moet zijn (i.e. wordt de IMSI opgedeeld in blokken van duizend, van een miljoen MSIN's, of van 10 miljoen MSIN's), welke voorwaarden gelden, en welke blokgrootte onder welke voorwaarden aan welke partij wordt toegekend.

Het ligt voor de hand dat de ACM in elk geval een rol hebben bij de handhaving van de voorwaarden en regels.

[30] Eventueel extra verkeer omdat roaming wordt gebruikt op het netwerk waar wel een contract mee is zal onderdeel vormen van de commerciële afspraken tussen MNO en gebruiker.
[31] Per april 2013 de "Autoriteit Consument en Markt", of ACM.

CONTACT

Stratix Consulting B.V.
Villa Hestia - Utrechtseweg 29
1213 TK Hilversum

Telefoon: +31.35.622 2020
E-mail: office@stratix.nl
URL: http://www.stratix.nl