Risicoanalyse Slimme Meter Keten

Privacy en Security in het nieuwe marktmodel

Technical Sciences
Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO-rapport

TNO 2012 R10633 | Eindrapport

Risicoanalyse Slimme Meter Keten

Datum	12 november 2012
Auteur(s)	Ir. B.J. te Paske, Dr. C.M.K.C. Cuijpers, Prof. Dr. M.C.J.D. van Eekelen, Dr. Ir. E. Poll, Drs. B.H.A. van Schoonhoven
Exemplaarnummer	
Oplage	
Aantal pagina's	47 (incl. bijlagen)
Aantal bijlagen	3
Opdrachtgever	NMa
Projectnaam	Risicoanalyse Slimme Meter Keten
Projectnummer	

Samenvatting

De Energiekamer van de Nederlandse Mededingingsautoriteit (hierna: de NMa) is door het Ministerie van EL&I belast met het monitoren van de uitrol van de slimme meter (tijdens de kleinschalige uitrol). De NMa dient zich daarvoor een goed beeld te vormen van alle aspecten van de uitrol, waaronder ook privacy en security.

Om haar monitoringstaak doelgericht te kunnen uitvoeren heeft de NMa aan TNO, LaQuSo en TILT gevraagd om de risico's en potentiële problemen in de meter keten en het marktmodel rondom de slimme meter te onderzoeken. De scope van het onderzoek beperkt zich tot partijen in het Nederlandse vrije marktdomein binnen de metermarkt. Dit zijn in ieder geval de Overige Diensten Aanbieders (ODA's), meetbedrijven, leveranciers en kleinverbruikers. Het domein van de netbeheerders is buiten scope, evenals de grootverbruikaansluitingen. De focus van de risicoanalyse ligt op risico's met mogelijke impact voor de consument/kleinverbruiker.

In het onderzoek is een aantal bevindingen gedaan ten aanzien van het marktmodel en de meter keten. De belangrijkste bevindingen, die de context van de risico's bepalen:

- De uitwerking en de nadere invulling van het nieuwe marktmodel zijn nog in volle gang terwijl dit onderzoek loopt. Op basis van de voor dit onderzoek verkregen informatie lijken diverse aspecten van privacy- en security nog onvolledig uitgewerkt, vastgelegd en geïmplementeerd.
- Omdat de rol van overige diensten aanbieder (ODA) als een vrije marktrol wordt beschouwd, wordt deze in de geraadpleegde brondocumenten niet gedefinieerd of ingeperkt. Als gevolg hiervan ontbreekt wel een helder kader voor toetredingscriteria en toezicht op de ODA's.
- In de slimme meter keten zijn feitelijk verschillende categorieën van ODA's ontstaan met een eigen risicoprofiel:
  - Enerzijds is er een belangrijk onderscheid tussen een ODA die de P1 poort (hoogfrequente gegevens via de klant zelf) gebruikt en een ODA die de P4 poort (laagfrequente gegevens via Netbeheerder/EDSN) gebruikt;
  - Bij leveranciers die ook als ODA opereren bestaat het risico dat informatie die verkregen wordt vanuit de leveranciersrol wordt gebruikt voor de ODA-rol (rollenvermenging). Dit staat een level playing field voor ODA's in de weg.

De volgende risico's voor privacy en security worden als tenminste 'hoog' beoordeeld:

- Het risico op verlies van vertrouwen van consumenten in de slimme meter of het marktmodel als gevolg van misbruik van hoogfrequente meetgegevens uit de P1 wordt als **zeer hoog** beoordeeld. Mogelijke scenario's zijn:
  - Derden verkrijgen toegang tot meetgegevens via slecht beveiligde systemen van de ODA;
  - Schending van het doelbindingsprincipe: meetgegevens worden verwerkt voor andere doelen dan waar de consument toestemming voor heeft gegeven;
  - Er is geen sprake van 'informed consent': de kleinverbruiker beseft niet hoe zijn P1-gegevens gebruikt zullen worden.
- Het risico van misbruik van de schakelfunctie wordt als **zeer hoog** ervaren vanwege de grote potentiële impact en het feit dat met geavanceerde externe aanvallers rekening moet worden gehouden.
- Een **hoog** risico bestaat dat leveranciers hun (informatie-)positie misbruiken ten behoeve van hun dubbelrol als ODA. Dit kan het level playing field bedreigen dat in het marktmodel wordt beoogd.

In deze rapportage worden aanbevelingen gedaan voor hoe de NMa de benoemde risico's vanuit haar toezichtrol kan adresseren.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

De kleinschalige nationale uitrol (KSU) van slimme energiemeters door de netbeheerders is begin 2012 gestart. Een aspect dat in de voorbereiding hierop veel aandacht heeft gekregen zijn de privacy en security van de slimme meter keten. In antwoord op een vraag van de Eerste Kamer heeft TNO in 2010 de toekomstvastheid, security en privacybescherming onderzocht. Eén van de voorwaarden voor veilige uitrol die uit dit onderzoek naar voren kwam is effectief toezicht door de overheid. Vanuit deze achtergrond is de Energiekamer van de Nederlandse Mededingingsautoriteit (hierna: de NMa) door het Ministerie van EL&I belast met het monitoren van de uitrol van de slimme meter (tijdens de KSU). De NMa dient zich een goed beeld te vormen van alle aspecten van de uitrol, waaronder ook privacy en security.

Naast de monitoringopdracht van de Minister heeft de NMa uiteraard ook haar reguliere toezichttaak op de energiewetgeving privacy en security van de slimme meter keten. In de energiewetgeving zijn diverse uitwerkingen van het privacy- en securitykader opgenomen. Op deze wijze kan de NMa toezicht houden op de uitvoer van een belangrijk deel van het privacy- en securitykader door de energiebedrijven.

De NMa stelt het belang van een consumentvriendelijke uitrol centraal en is van mening dat het daartoe noodzakelijk is om zicht te krijgen op mogelijke privacy en security risico's bij elk van de marktrollen in het marktmodel. De NMa is de toezichthouder voor de regionale netbeheerder, die de slimme meter uitrolt en verantwoordelijk is voor het beheer van de gehele meetinrichting. De NMa is ook de toezichthouder voor de leveranciers, welke allemaal een leveringsvergunning van de NMa hebben. De NMa vraagt zich af welke risico's er voor de consument zijn bij de marktrollen die niet direct onder het toezicht van de NMa vallen. Met andere woorden: de NMa wil haar monitoringstaak ketenbreed uitvoeren, waarbij de scope alle marktrollen omvat die een rol spelen in de slimme meter keten. Deze marktrollen verschillen sterk van elkaar, zowel in hun doelstellingen als in hoe zij processen en techniek inrichten (bijvoorbeeld de wijze waarop meetgegevens worden opgeslagen en gecommuniceerd). Het is van belang om voor elk van de marktrollen de privacy- en securityrisico's in kaart te brengen, en daarnaast eventuele ketenbrede risico's.

Tot op heden lag de focus van de privacy- en securitydiscussie op het netbeheerderdomein. Zowel de wetgever als de netbeheerders (en ook het College Bescherming Persoonsgegevens) zelf hebben hieraan veel aandacht besteed. Om deze reden is het op dit moment niet noodzakelijk om binnen het netbeheerderdomein een risicoanalyse uit te voeren, De NMa heeft op dit moment echter onvoldoende inzicht in privacy- en securityrisico's bij andere marktrollen zoals de consument, het meetbedrijf, de energieleverancier en de onafhankelijke dienstenaanbieder (ODA).

1.2 Probleemstelling

Om haar monitoringstaak doelgericht te kunnen uitvoeren wil de NMa kwalitatief inzicht verkrijgen in de risico's en potentiële problemen in de gehele meter keten en het marktmodel rondom de slimme meter.

De NMa laat hiertoe een risicoanalyse uitvoeren door een onafhankelijk onderzoeksinstituut met de benodigde privacy- en security expertise en daarnaast domeinkennis van de slimme meter keten[1,2].

1.3 Afbakening

De reikwijdte van het onderzoek is als volgt afgebakend:

- Het onderzoek richt zich op zowel privacy- als securityrisico's. Daarnaast worden onderlinge relaties benoemd, bijvoorbeeld informatiebeveiligingsrisico's met mogelijke privacy-impact.
- Het onderzoek richt zich met name op de gegevens die direct met de slimme meter te maken hebben, zoals meet- en schakelgegevens. Meer gebruikelijke gegevens, zoals een medewerker- of klantenadministratie worden buiten beschouwing gelaten voor zover deze niet wezenlijk verschillen ten opzichte van vrijwel elke andere marktketen.
- De focus ligt op risico's bij geautoriseerde toegang tot de slimme meter keten in het huidige marktmodel. Risico's gebaseerd op ongeautoriseerde toegang zijn wel in scope maar minder prominent.
- De scope beperkt zich tot partijen in het Nederlandse vrije marktdomein binnen de metermarkt. Dit zijn in ieder geval de Overige Diensten Aanbieders (ODA's), meetbedrijven, leveranciers en kleinverbruikers. Het domein van de netbeheerders is buiten scope, evenals de grootverbruikaansluitingen.
- De huidige wet- en regelgeving gelden als uitgangspunt. Toetsing hiervan is niet in scope van de opdracht. Bij de inventarisatie van privacy-risico's is wel de voorgestelde nieuwe Europese verordening rond dataprotectie in ogenschouw genomen (met aanscherpingen op een aantal terreinen waaronder dataportabiliteit, transparantie en accountability).Als uitgangspunt voor het vaststellen van relevante stakeholders en hun requirements in de context van de slimme meter keten worden de volgende documenten gebruikt:
  - Elektriciteitswet 1998 [3]
  - Begrippenlijst Elektriciteit [8]
  - Wet Marktmodel [4]
  - Concept Informatiecode – verstrekt door NMa [5]
  - Concept Meetcode – verstrekt door NMa [6]
- De focus ligt op risico's met mogelijke impact voor de consument/kleinverbruiker. Aanvullend hierop zijn risico's waarvan vooral andere marktrollen schade kunnen ondervinden van belang.

1.4 Documentwijzer

Als voorbereiding op de daadwerkelijke risicobeoordeling worden in hoofdstuk 2 relevante privacy- en security requirements voor de slimme meter keten uitgewerkt. In hoofdstuk 3 wordt een overzicht gegeven van de slimme meter keten, op basis van het nieuwe marktmodel en de functionaliteit van de slimme meter. De daadwerkelijke risicoanalyse is in twee onderdelen opgesplitst: een "long-list" van risico's in hoofdstuk 4, waarbij de meest opvallende risico's uitgelicht en besproken worden in hoofdstuk 5. Tot slot worden conclusies en aanbevelingen geformuleerd in hoofdstuk 6.

2 Privacy en security requirements

In deze risicoanalyse worden privacy- en securityrisico's geïnventariseerd, onderzocht en beoordeeld. Bij het beoordelen van risico's zijn we uitgegaan van een set requirements waaraan de beveiliging van de slimme meter keten dient te voldoen. Deze requirements volgen uit twee overwegingen:

- Wat is de maximale impact die partijen in de meter keten (en met name de consument) kunnen ondervinden van privacy- en security incidenten? Zonder de dreigingen al in detail uit te werken kunnen requirements worden afgeleid die de belangrijkste impacttypen beperken.

- Welke requirements volgen uit wet- en regelgeving? Hierbij gelden zowel de algemene kaders rond privacy en gegevensbescherming als specifieke regelgeving voor de slimme meter keten.

Deze aspecten worden in 2.1 respectievelijk 2.2 uitgewerkt. In 2.2 wordt ook aandacht besteed aan het toezicht door het College Bescherming Persoonsgegevens voor een helder beeld omtrent de taakverdeling in het toezicht op de slimme meter keten. De wijze waarop politiek en praktijk gereageerd hebben op eerdere kritiek betreffende privacyaspecten van de slimme meter wordt kort besproken om inzicht te geven in de waarborgen en garanties die zijn ingebouwd om aan privacy en gegevensbescherming tegemoet te komen.

Sectie 2.3 vat de requirements samen. Hierbij beperken we ons tot requirements die vallen binnen het toezichtsdomein van de NMa, en die we als uitgangspunt bij deze studie hanteren.

2.1 Maximale impact van incidenten

Als kader voor de risicoanalyse is een inschatting gemaakt van de maximale impact die bij verschillende typen incidenten kan optreden. Binnen de scope van dit onderzoek kunnen incidenten worden onderscheiden waarbij:
- de privacy van aangeslotenen wordt aangetast;
- de beschikbaarheid van meetgegevens onderbroken wordt;
- de integriteit van meetgegevens aangetast wordt;
- de beschikbaarheid van schakelberichten onderbroken wordt;
- de integriteit van schakelberichten aangetast wordt.

Uiteraard zijn ook incidenten denkbaar die gevolgen hebben in meer dan één van de genoemde categorieën. We bespreken deze soorten incidenten, en hun maximale impact, hieronder uitgebreider.

2.1.1 Aantasting van privacy

De slimme meter registreert – onder andere – verbruiksgegevens in digitale vorm, en maakt het mogelijk om deze verbruiksgegevens op afstand uit te lezen. Deze verbruiksgegevens vertellen in veel gevallen iets over het gedrag van personen, en zijn daarom in potentie persoonsgegevens. Als het om het inschatten van de maximale impact van een privacyschending bij verbruiksgegevens gaat is het van belang om onderscheid te maken in de *granulariteit*, *actualiteit* en *kwantiteit* van deze gegevens:
- Verbruiksgegevens met een hoge *granulariteit* bevatten meer metingen per tijdseenheid en zijn meer gedetailleerd dan verbruiksgegevens met een lage granulariteit. Een lek van verbruiksgegevens met hoge granulariteit vertelt meer over het gedrag van personen.
- *Actuele* verbruiksgegevens zijn korter geleden gemeten, en geven dus een inzicht in recente gedragingen. Dit maakt dat een lek van actuele verbruiksgegevens een hogere impact heeft.

- Tot slot is de *kwantiteit* van de gegevens een bepalende factor voor de maximale impact van een privacyschending: verbruiksgegevens over een langere periode maken het beter mogelijk om gedragspatronen te herkennen.

Als we de *maximale* impact van een aantasting van privacy door een lek van verbruiksgegevens willen bepalen, gaan we dus uit van een lek van een grote kwantiteit aan actuele gegevens met een hoge granulariteit. Door de veelheid en gedetailleerdheid van consumptiegegevens kan een zeer indringend beeld geschetst worden van gedrag, dagelijkse routine en levensstijl van de kleingebruiker. Onderzoek heeft bijvoorbeeld aangetoond dat op basis van het verbruikspatroon van elektriciteit en gas het gebruik van specifieke apparaten in huis geïdentificeerd kan worden [12, 18, 19, 20].

Verbruiksgegevens met een zekere actualiteit en granulariteit zijn noodzakelijk voor het mogelijk maken van de gereguleerde basisdiensten en het goed functioneren en beheren van het energienet. Deze gegevens maken het echter ook mogelijk om aangeslotenen te profileren, waarbij op basis van persoonsgegevens een profiel wordt aangemaakt. Het risico van profielen is met name gelegen in het feit dat op basis van deze profielen beslissingen worden genomen, met name om data subjecten in- of juist uit te sluiten van bijvoorbeeld aanbiedingen, kortingen, of heffingen.

Indien gebruiksgegevens ongewenst gedrag laten zien - mogelijk vanuit het perspectief van betrokken marktpartijen met bijvoorbeeld het oog op het goed functioneren van het netwerk, of vanuit een oogpunt van politie, justitie of andere opsporingsdiensten - kan er sprake zijn van een inmenging van deze partijen in het energieverbruik. Dit kan in de vorm van een waarschuwing om bepaald gedrag te beëindigen, of wellicht dat de marktpartij zelf energietoevoer kan verminderen of kan beëindigen. Tevens kan melding worden gedaan bij politie, justitie of een andere opsporingsdienst, die mogelijk op grond van eigen bevoegdheden – zelfs zonder melding maar op basis van eigen vermoedens - gegevens op kunnen vragen bij een van de in het proces van energielevering betrokken partijen.

Uit bovenstaande kunnen verschillende (denkbeeldige) scenario's afgeleid worden waarin inmenging in het privéleven van een kleinverbruiker plaats kan vinden:

a) Inbrekers kunnen op basis van informatie die de slimme meter genereert beter hun doelwit bepalen. Informatie over leefpatronen maakt duidelijk wanneer personen niet in huis aanwezig zijn en meetgegevens kunnen de aanwezigheid van gewenste apparatuur inzichtelijk maken, alsmede de afwezigheid of het niet ingeschakeld zijn van beveiligingsapparatuur.
b) Marketeers kunnen op basis van meetgegevens een meer gerichte marketing strategie voeren, en consumenten meer of minder indringend lastig vallen met specifiek op hen toepasselijke marketing ("wij zien dat uw wasmachine aan vervanging toe is, nu in de aanbieding …").
c) Verzekeraars kunnen op basis van de meetgegevens meer of andere voorwaarden aan een verzekering stellen, of niet uitkeren omdat uit meetgegevens blijkt dat een specifiek apparaat veroorzaker is geweest van kortsluiting (en de consument hier al meerdere keren voor gewaarschuwd was door een commerciële partij die aanbiedingen heeft gedaan ter vervanging van dit apparaat).
d) Kleinverbruikers kunnen geconfronteerd worden met bevraging door politie en justitie in verband met een buitenproportioneel energieverbruik of opmerkelijke patronen in energieverbruik, bijvoorbeeld omdat dit mogelijk duidt op de aanwezigheid van een wietplantage in de woning van de kleinverbruiker of op gedrag wat in een "crimineel" profiel past.
e) Kleinverbruikers kunnen gekort worden op hun uitkering omdat meetgegevens gebruikt zijn onderzoek naar sociale zekerheidsfraude (energieverbruik kan bijvoorbeeld samenwonen

aantonen). Als praktijkvoorbeeld kan gewezen worden op een zaak waarbij (in strijd met de Wbp) gebruik is gemaakt van informatie over het verbruik van water.[1]

De wetenschap bij kleinverbruikers dat dit soort scenario´s tot de mogelijkheden behoren, kan ertoe leiden dat kleinverbruikers de slimme meter als “big brother” gaan zien en de meter als zodanig niet vertrouwen en dus niet accepteren. Dit kan een grote impact hebben op de slimme meter keten als geheel.[2]

Door de – in potentie – hoge impact van dit soort incident verdienen risico’s die hiertoe kunnen leiden bijzondere aandacht.

Observatie 1:
Verbruiksgegevens met een hoge granulariteit kunnen vanuit privacy oogpunt zeer gevoelig zijn, om meerdere redenen. Ten eerste kan in potentie uit deze gegevens veel over het gedrag en het leven van individuen afgeleid worden. Denk bijvoorbeeld aan het afleiden uit deze gegevens van de aanwezigheid van bepaalde medische apparatuur, of gedragingen waaruit religieuze overtuigingen afgeleid kunnen worden. Ten tweede hebben deze gegevens veelal betrekking op de (grondwettelijk beschermde) persoonlijke levenssfeer. Partijen die verantwoordelijk zijn voor het verwerken van deze gegevens moeten zich hier terdege van bewust zijn.

2.1.2 Onderbreking levering elektriciteit

Onterechte onderbreking van de elektriciteitsvoorziening kan zeer grote impact hebben, zeker als het grote aantallen kleinverbruikers raakt en/of pas na langere tijd wordt hersteld. Het is voorstelbaar dat zo’n scenario optreedt als gevolg van het versturen van ongeautoriseerde schakelberichten door een leverancier of door een derde partij die zich via systemen van een leverancier of anderszins als leverancier voordoet. Een complicerende factor is dat het gelijktijdig afschakelen van een groot aantal huishoudens de vraag naar elektriciteit in een zeer korte tijdspanne zeer sterk kan doen dalen, wat schadelijke gevolgen kan hebben voor de stabiliteit van het elektriciteitsnetwerk als geheel.

Door de – in potentie – zeer hoge impact van dit soort incident verdienen risico’s die hiertoe kunnen leiden bijzondere aandacht.

[1] Zie in dit verband: http://www.cbpweb.nl/Pages/pb_20070531_bestkopel_fraude_onrechtm.aspx en meer recent over vergelijkbaar thema: http://www.cbpweb.nl/Pages/pb_20110317_SIOD.aspx
[2] Sommige personen kunnen een slimme meter, bijvoorbeeld het knipperende licht erop, emotioneel confronterend vinden en de suggestie vinden wekken dat “Big Brother” mee kijkt[30].

Observatie 2:
Bij de introductie van de slimme meter is er veel aandacht geweest voor het feit dat deze meter het op afstand uitlezen van verbruiksgegevens mogelijk maakt. Echter, een (grootschalig) incident met de schakelfunctie op afstand die er in resulteert dat een groot aantal kleinverbruikers gelijktijdig worden afgesloten kan nog veel grotere en direct voelbare gevolgen hebben. Beide aspecten van de slimme meer – op afstand uitlezen en op afstand schakelen – verdienen daarom evenzeer de aandacht.

2.1.3 Aantasting integriteit meetgegevens

Correcte facturatie van verbruik is één van de primaire processen die de slimme meter keten dient te ondersteunen. Zeker voor de kleinverbruiker geldt dat de integriteit van de meetgegevens van veel groter belang is dan de tijdigheid/beschikbaarheid. Het is voorstelbaar dat de meetgegevens van grote aantallen kleinverbruikers corrupt raken, bijvoorbeeld als gevolg van een systeemstoring of bewuste handeling in het domein van de leverancier. Dit kan leiden tot incorrecte facturen. Indien afwijkingen door de kleinverbruiker opgemerkt worden zal de schade voor de consument echter beperkt blijven omdat hij de fouten kan aantonen op basis van de meterstanden in de meter zelf (in deze risicoanalyse wordt aangenomen dat de netbeheerder zorgdraagt voor de integriteit van de bronstanden). Naast impact voor de consument kan ook de leverancier impact ondervinden; deze kan zelfs ontstaan door moedwillige verstoring van de meterfuncties door kleinverbruikers.

2.1.4 Onderbreking beschikbaarheid meetgegevens

Een onderbreking van de beschikbaarheid van meetgegevens heeft wel gevolgen, maar deze zijn relatief gering vergeleken bij de eerder genoemde impacts. Voor een leverancier kan dit betekenen dat delen van de dienstverlening zoals de facturatie vertraging oplopen. Aangenomen dat meetgegevens niet verloren gaan (wat we onder de integriteit van meetgegevens scharen) maar na herstel van de beschikbaarheid als historie opgevraagd kunnen worden blijft de impact van dit soort incidenten maximaal beperkt tot een vertraging in de facturatie. Voor een ODA kan een hogere impact op de dienstverlening denkbaar zijn, als deze een dienst aanbiedt die afhankelijk is van de beschikbaarheid van actuele (real-time) gegevens.

2.1.5 Onderbreking beschikbaarheid schakelfunctie / schakelgegevens

Een onderbreking in de beschikbaarheid van de schakelfunctie van de slimme meter kan tot gevolg hebben dat een kleinverbruiker onterecht aangeschakeld blijft (bijvoorbeeld na verhuizing of na wanbetaling). Ook kan het resulteren in een kleinverbruiker die onterecht niet aangeschakeld wordt (bijvoorbeeld ook na een verhuizing). In beide gevallen zal het om relatief kleine aantallen gebruikers gaan, waarbij alternatieve mogelijkheden (een monteur langs sturen) beschikbaar zijn. De impact van dit soort incidenten schatten we dus laag in.

2.2 Regelgeving, toezicht en zelfregulering

Bij slimme energiemeting kunnen privacyrisico´s samenhangen met een aantasting van de privacy en met de verwerking van persoonsgegevens, als onderdeel van het recht op privacy. Het juridisch kader wordt dan ook niet alleen gevormd door het meer gedetailleerde recht op gegevensbescherming, in Nederland verankerd in de Wet bescherming persoonsgegevens (Wbp), maar ook door het meer overkoepelende recht op privacy.

Voor Nederland is dit recht verankerd in artikel 10 van de Grondwet, welk artikel wordt uitgelegd in overeenstemming met artikel 8 EVRM. Hierbij is van belang dat ook bij rechtmatige verwerking van persoonsgegevens (verwerking in overeenstemming met de Wbp), sprake kan zijn van inbreuk op

privacy, doordat bijvoorbeeld de meetgegevens inzicht geven in relaties (2 personen verbruiken nu eenmaal meer energie dan 1) waardoor niet zozeer het recht op gegevensbescherming geschonden wordt, maar de meetgegevens mogelijk interfereren met de relationele dimensie van privacy, of mogelijk met het huisrecht omdat de meetgegevens van de slimme meter een ‘ kijkje achter de voordeur’ van de kleinverbruiker kunnen bieden. De NMa houdt in beginsel geen toezicht op de naleving van de Wbp. Echter de requirements die uit de Wbp voortvloeien geven wel inzicht in de vereisten die vanuit privacy- en gegevensbeschermingsperspectief gelden voor de slimme meter keten, en zijn daarom opgenomen in bijlage B en C.

2.2.1 Toezicht

De verdeling van toezicht tussen NMa en CBP valt samen met de wetgeving waarop toezicht plaatsvindt: in de Wbp is geregeld waar het CBP toezicht op houdt, terwijl in de Elektriciteitwet 1998 en de Gaswet is geregeld waar de NMa toezicht op houdt. Vereisten met betrekking tot beveiliging volgen zowel uit de Wbp als uit de Elektriciteits- en Gaswet.

In dit verband heeft het toezicht van de NMa vooral als doel het voorkomen van fraude met, misbruik van of inbreuk op de meetinrichting. Het gaat voornamelijk om het voorkomen van acties die de hoogte van de energierekening beïnvloeden. De beveiligingsvereisten in het kader van de Wbp betreffen passende technische en organisatorische maatregelen met betrekking tot de bescherming van persoonsgegevens. Vanuit dit perspectief kan gesteld worden dat de rol van de NMa met betrekking tot het toezicht op de naleving van privacy en gegevensverwerking minimaal is.[3] Er is enkel sprake van toezicht op de naleving van de verantwoordingsvoorwaarden van de NMa krachtens hoofdstuk 4 van de Elektriciteitswet en hoofdstuk 3 van de Gaswet betreffende *“voorwaarden wijze van gegevensverwerking”*.[4] Hierbij betreft het geen inhoudelijke toets of de Wbp is nageleefd, maar of in de toelichting op de jaarrekening deugdelijk gerapporteerd is over de wijze waarop uitvoering is gegeven aan de voorwaarden voor gegevensverwerking (art. 53 Elektriciteitswet, art. 22 Gaswet).

Observatie 3:
Hoewel de NMa niet toetst op naleving van de Wbp, kan het niet voldoen aan privacy en gegevensbescherming ook consequenties hebben voor consumentenbescherming en marktwerking, gebieden waarop de NMa wel toezicht houdt. Dit wordt geïllustreerd door een recente zaak waarin de NMa een boete heeft opgelegd aan Liander en Nuon omdat Liander klantgegevens onvoldoende had afgeschermd voor energieleverancier Nuon Sales, die deze gegevens kon gebruiken voor eigen marketingdoeleinden. Hoewel van daadwerkelijk misbruik niet is gebleken, wijst de NMa erop dat zo’n voordeel kan leiden tot oneigenlijke concurrentie en dus tot verstoring van de markt. Afhankelijk van de precieze vorm en de gevolgen die een onvoldoende beveiliging in een bepaald geval heeft, kan een boete worden opgelegd door een van de toezichthouders.

2.2.2 Informatiecode

De afspraken die bedrijven in de energiesector maken met het oog op gegevensbeheer worden vastgelegd in voorwaarden die bedrijven jegens elkaar en jegens afnemers hanteren betreffende het

[4] Hierbij is het wel relevant om te wijzen op de Regeling gegevensbeheer en afdracht elektriciteit en gas. Deze regeling vormt een specifieke aanvulling op de Wbp wat betreft de energiesector. De regeling vormt een kader waarbinnen voorwaarden kunnen worden vastgesteld waaronder persoonsgegevens van kleinverbruikers verzameld en verwerkt mogen worden. Het gaat hier vooral om Artikel 8 van de Regeling van de Minister van Economische Zaken, Landbouw en Innovatie van 14 juni 2011, nr. WJZ/11060599, houdende regels inzake de voorwaarden voor gegevensbeheer en afdracht elektriciteit.

gegevensbeheer in het kader van administratieve ketenprocessen. Deze voorwaarden worden aangeduid als de 'Informatiecode Elektriciteit en Gas'. Deze Informatiecode voorziet niet in een generieke wettelijke grondslag voor het mogen uitwisselen en verwerken van persoonsgegevens, maar vormt een uitwerking van de Wbp. De plicht om een dergelijke Informatiecode op te stellen vloeit voort uit hoofdstuk 4 van de Elektriciteitswet en hoofdstuk 3 van de Gaswet.

2.2.3 Vierkeuzenmodel

De reden waarom de slimme meter keten zoals voorgesteld in de initiële Nederlandse wetsvoorstellen de privacytoets niet kon doorstaan, was voornamelijk gelegen in de volgende drie kenmerken van de voorgestelde slimme meter keten: het gebrek aan keuzemogelijkheid voor de consument; zeer frequente uitlezing van meterstanden; de centrale opslag van persoonsgegevens; en de afsluitfunctie.[5] Of, en zo ja in welke mate, deze aspecten daadwerkelijk problematisch zijn vanuit een oogpunt van privacy en security hangt grotendeels af van de inrichting van de slimme energieketen en de waarborgen en garanties die deze keten omgeven.

Om tegemoet te komen aan de in de initiële voorstellen gesignaleerde problemen, is met zogenaamde novellen (Kamerstukken 32 373 en 32 374) een keuzemodel ingevoerd op basis waarvan kleinverbruikers vier keuzes hebben:

1) Geen op afstand uitleesbare meter;
2) Een op afstand uitleesbare meter die administratief uitstaat;
3) Een op afstand uitleesbare meter met standaard meetgegevenscollectie-regime;
4) Een op afstand uitleesbare meter waarbij toestemming is verleend om meer gegevens te mogen uitlezen.[6]

Indien een meter administratief uitstaat mogen meetgegevens niet op afstand uitgelezen worden. In de standaardmeetstand mogen slechts de volgende gegevens worden verzameld: een keer per jaar voor de jaarnota; per evenement als er sprake is van verandering van leverancier of verhuizen; tweemaandelijks voor het inzicht in het energieverbruik; dat wat noodzakelijk is voor het technisch beheer van het net op grond van de wettelijke taak die netbeheerders uitvoeren. (art. 16 Elektriciteitswet / art. 10 Gaswet). Bovendien zijn de voorwaarden waaronder persoonsgegevens van afnemers kunnen worden verzameld en verwerkt geëxpliciteerd. Tevens is een verplichting voor de energiesector ingevoerd om in de toelichting op de jaarrekening te rapporteren over verantwoordingsvoorwaarden die door de NMa in een Informatiecode zijn vastgesteld. Met dit keuzemodel en de gecreëerde verantwoordingsmechanismen wordt tegemoet gekomen aan het gebrek aan keuzevrijheid en de frequente uitlezing.

Observatie 4:
De waarde van dit vierkeuzenmodel is sterk afhankelijk van de informatie die een kleinverbruiker heeft omtrent de te maken keuzes, wat deze inhouden en wat de gevolgen zijn. Vanuit het recht op privacy is deze informatie van belang voor kleinverbruikers om daadwerkelijk toestemming ofwel 'informed consent' te kunnen geven voor verwerking van persoonsgegevens die niet noodzakelijkerwijs samenhangt met de levering van energie.

2.3 Requirements

Op basis van de impactbeoordeling en de voorgaande analyses kunnen requirements voor de slimme

[5] In dit verband was vooral problematisch dat er geen onderzoek voorhanden is waaruit ondubbelzinnig blijkt dat deze kenmerken noodzakelijk zijn in een democratische samenleving en dat er geen minder ingrijpende alternatieven voorhanden zijn.
[6] Kamerstukken II, vergaderjaar 2009-2012, 32 374, nr. 3, p. 8.

meter keten worden afgeleid in drie verschillende domeinen: privacy; beschikbaarheid en integriteit van meetgegevens; beschikbaarheid van elektriciteit / continuïteit van levering. Voor wat betreft privacy is een volledig overzicht van requirements die voortvloeien uit de Wbp en artikel 8 EVRM weergegeven in Bijlage B en C. Een deelverzameling van requirements met bijzondere relevantie voor de rol van de NMa is hieronder weergegeven.

2.3.1 Privacy requirements

R1 Er dient sprake te zijn van uitdrukkelijke doelspecificatie.
R2 Er dient invulling gegeven te worden[7] aan garanties/waarborgen betreffende doelbinding, dat wil zeggen dat gegevens slechts worden verwerkt voor het gespecificeerde doel.
R3 Er dient invulling gegeven te worden aan informatieplichten.[8]
R4 Gegevens die niet noodzakelijk zijn voor de basisdiensten energielevering en facturatie dienen slechts te worden verwerkt op basis van expliciete toestemming door de consument.
R5 In de toelichting op de jaarrekening moet verantwoording worden afgelegd over naleving van de Informatiecode.
R6 Leveranciers, meetbedrijven en ODA's moeten een Gedragscode opstellen en conform deze code handelen.

2.3.2 Requirements rond beschikbaarheid en integriteit van meetgegevens

R7 De meetfunctie van de slimme meter dient integer te zijn, dus de door de meter geproduceerde meetgegevens dienen het daadwerkelijke netto verbruik weer te geven.
R8 Van meetgegevens die in de slimme meter keten worden verwerkt moet de herkomst (de meter die ze heeft vastgesteld) eenduidig bepaald kunnen worden.
R9 Aanpassingen van meetgegevens in de keten (nadat deze initieel door de meter zijn geproduceerd) moeten gedetecteerd / aangetoond kunnen worden.
R10 Meetgegevens (zowel actuele als historische) dienen alleen toegankelijk te zijn voor partijen die deze vanuit hun rol nodig hebben. NB: dit is een vertrouwelijkheidseis die ook beschermt tegen aanvallen op integriteit .
R11 De meetfunctie dient aan zeer hoge beschikbaarheidseisen te voldoen.
R12 De beschikbaarheid van meetgegevens mag hooguit voor beperkte tijd worden onderbroken.

2.3.3 Requirements rond beschikbaarheid van elektriciteit / continuïteit van levering

R13 De schakelfunctie van de slimme meter dient zodanig te zijn geïmplementeerd dat alleen op basis van een authentiek schakelbericht van een geautoriseerde partij wordt geschakeld.
R14 Schakelgegevens (zowel actuele als historische) dienen alleen toegankelijk te zijn voor partijen die deze vanuit hun rol nodig hebben.
R15 De beschikbaarheid van schakelfunctionaliteit en schakelgegevens mag hooguit voor beperkte tijd worden onderbroken.

---

[7] Waar gesproken wordt van ´invulling geven aan´ wordt gedoeld op een uitdrukkelijke opschriftstelling van alle technische, organisatorische, procedurele en praktische aspecten van de daadwerkelijke implementatie van het desbetreffende requirement.
[8] Hierbij is met name van belang: indien de verwerking van persoonsgegevens plaatsvindt op basis van toestemming van de consument, moet de consument vooraf voldoende en in begrijpelijke taal geïnformeerd zijn over wat er met zijn persoonsgegevens gebeurt en hoe toestemming ingetrokken kan worden.

3 De slimme meter keten

We bespreken twee belangrijke ontwikkelingen die onder de nieuwe slimme meter keten liggen: het nieuwe marktmodel en de slimme meter zelf. Daarna volgt een beschrijving van de technische architectuur en de interfaces daarbinnen.

3.1 Het nieuwe marktmodel

Het nieuwe marktmodel dat de basis vormt voor de inrichting van de slimme meter keten is gebaseerd op drie uitgangspunten die in de context van deze risicoanalyse van belang zijn:

1. Leveranciersmodel;
2. Metermarktmodel;
3. Capaciteitstarief.

Leveranciersmodel:
In het leveranciersmodel ontvangt de kleinverbruiker uitsluitend een factuur van zijn leverancier. De leverancier factureert namens de (regionale) netbeheerder de netwerkkosten, int en draagt vervolgens af aan de netbeheerder. In het nieuwe marktmodel doet de kleinverbruiker dus uitsluitend zaken met zijn leverancier; dit brengt voor de leverancier zowel verantwoordelijkheden en plichten als bevoegdheden met zich mee.

Metermarktmodel:
In het nieuwe metermarktmodel wordt de verantwoordelijkheid voor de collectie en verwerking van meetgegevens verlegd van de netbeheerder naar de leverancier. De leverancier dient deze verantwoordelijkheid uit te laten voeren door een meetbedrijf. De kleinverbruiker kan zijn leverancier aanspreken wanneer het in rekening gebrachte verbruik niet correct is. De leverancier heeft dan ook de middelen om correcties door te voeren. Een ander aspect van het metermarktmodel is dat de regionale netbeheerder volledig verantwoordelijk is voor het beheer van de meetinrichtingen.

Capaciteitstarief:
In het nieuwe marktmodel wordt een einde gemaakt aan verbruiksafhankelijke facturatie door de netbeheerder. In plaats daarvan zullen de kosten van de netbeheerder op basis van de capaciteit van de aansluiting worden gefactureerd. De netbeheerder heeft dus niet langer verbruiksgegevens nodig voor de eigen facturatie. De leverancier heeft wel gegevens van de netbeheerder nodig over het aantal dagen dat de transportdienst is geleverd. Deze aanpassing van het nieuwe marktmodel is reeds geïmplementeerd in 2009.

Bevinding 1:
Omdat de rol van overige diensten aanbieder (ODA) als een vrije marktrol wordt beschouwd, wordt deze in de geraadpleegde brondocumenten niet gedefinieerd of ingeperkt. Als gevolg hiervan ontbreekt wel een helder kader voor toetredingscriteria en toezicht op de ODA's.

Bevinding 2:
Onder de noemer van ODA vallen eigenlijk verschillende rollen (P1 ODA en P4 ODA) met een wezenlijk verschillend risicoprofiel. Naar verwachting zal de P1 ODA een belangrijke rol gaan spelen. Naar onze mening maakt de P1 ODA echter geen deel uit van de slimme meter keten, maar dient deze te worden gezien als een van de vele (web-)dienstaanbieders waaraan een consument op basis van een bilaterale overeenkomst persoonsgegevens beschikbaar stelt. Daarmee valt de P1 ODA onder het reguliere toezicht van het CBP.

3.2 De slimme meter

Naast het nieuwe marktmodel brengt de introductie van de “slimme meter” ook veranderingen met zich mee. De “slimme meter” is echter niet zozeer “slim”; er zit niet noodzakelijkerwijs veel digitale intelligentie in. In het “Besluit op afstand uitleesbare meetinrichtingen” van met Ministerie van EL&I uit 2011 staat omschreven wat we hier onder de slimme meter verstaan. Deze is in staat om onder andere:

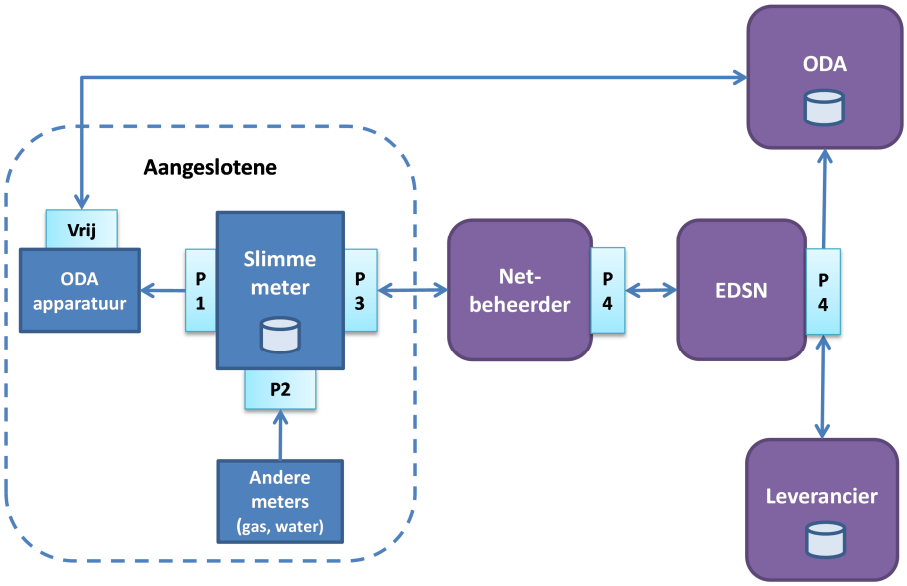
1. actuele vermogen (Watt) en de meterstand (kWh) te registreren, weer te geven en uit te wisselen met een applicatie die op de meter is aangesloten bij de afnemer;
2. de meterstand elk kwartier te registeren en op afstand met de netbeheerder uit te wisselen;
3. op afstand besturings- en toepassingsprogrammatuur van de meter aan te passen;
4. op afstand de levering van elektriciteit te onderbreken of te beperken en te hervatten;
5. fraude met, misbruik van of inbreuk op de meetinrichting of pogingen daartoe te registreren en informatie daarover op afstand uit te wisselen met de netbeheerder.[9]

Daarnaast heeft de slimme meter een display waarop de huidige meterstand zichtbaar is. Het is belangrijk om onderscheid te maken tussen twee aansluitingen die de slimme meter heeft die gebruikt kunnen worden om gegevens uit te lezen: de P1 poort en de P3 poort. De P1 poort levert gedetailleerde vebruiksgegevens aan een applicatie die bij de verbruiker in de meterkast op de meter aangesloten wordt (zoals hierboven bij punt 1 bedoeld), terwijl de P3 poort verbruiksgegevens overbrengt naar de netbeheerder, en instructies kan ontvangen zoals het aan- en afschakelen van de meter. De gegevens uit de P3 poort komen via de netbeheerder via een andere virtuele poort – de P4 poort – bij dienstenaanbieders en leveranciers terecht. De P3 poort is buiten scope voor deze studie, maar de P1 en P4 poort (omdat deze aansluiten op de andere marktpartijen) zijn binnen scope.

3.3 Rollen en interfaces in de slimme meter keten

Figuur 1 geeft een vereenvoudigde schematische weergave van de rollen, domeinen en interfaces in de slimme meter keten.

[9] Besluit op afstand uitleesbare meetinrichtingen, ministerie EL&I, 27-10-2011, online beschikbaar op: http://www.rijksoverheid.nl/documenten-en-publicaties/besluiten/2011/10/27/besluit-op-afstand-uitleesbare-meetinrichtingen.html



Figuur 1 - Domeinen, systemen en interfaces

In deze weergave zijn vier rollen aanwezig zoals omschreven in [3], [4], [5] en [6]:

- **Consument:** een kleinverbruiker met een slimme meter. De slimme meter bij een aangeslotene heeft 2 mogelijke interfaces met de buitenwereld: de P3 poort naar de netbeheerder, en een door aangeslotene of ODA vrij in te vullen interface met een ODA ("Vrij"), bijvoorbeeld een internetverbinding.
- **Netbeheerder:** de regionale netbeheerder heeft toegang tot de P3 poort van de meter en gebruikt deze voor het uitvoeren van verzoeken die binnenkomen op de P4-poort (zowel verzoeken om meetgegevens als schakelopdrachten).
- **Leverancier:** verkrijgt via de netbeheerder (P4) verbruiksgegevens van de slimme meter van aangeslotene, voor zover nodig voor facturering van de energielevering. Kan tevens via netbeheerder meters op afstand aan- en afschakelen.
- **Overige Diensten Aanbieder (ODA):** verkrijgt via de P1 poort (bijvoorbeeld met behulp van een apparaat dat de kleinverbruiker in de meterkast plaatst) of via de netbeheerder (P4) verbruiksgegevens van de slimme meter van aangeslotene, voor zover nodig voor het verlenen van een dienst. Een ODA kan meters niet aan- of afschakelen.

Een vijfde rol, die van **Meetbedrijf** is niet opgenomen in figuur 1; aan deze kan de uitvoering van een deel van de verantwoordelijkheid van de leverancier worden uitbesteed, namelijk het ophalen van meetgegevens.

Tot slot wijzen we op **EDSN:** deze uitvoeringsorganisatie speelt een belangrijke ondersteunende rol in de slimme meter keten . Deze rol kan worden omschreven als 'facilitator administratieve processen'. EDSN heeft als databeheerder en –broker een rol in de interfaces tussen meetbedrijf/netbeheerder en derde partijen en is hierdoor aangewezen door de Vereniging Nederlandse Energie Data Uitwisseling (NEDU).

Zoals in figuur 1 zichtbaar is, kunnen verbruiksgegevens via twee wegen van de kleinverbruiker bij de andere marktpartijen terecht komen: de P1 poort en de P3 / P4 poort. Gegevens uit de P3 poort komen altijd via de P4 poort bij leveranciers en ODA's terecht, daarom spreken we in deze studie over de P4 poort, als we het over gegevens afkomstig uit de P3 poort hebben. De P1 en P4 poort verschillen van elkaar op een aantal punten, zoals de granulariteit (het detailniveau) van de gegevens, of de mate waarin de aansluiting op de poort gereguleerd is. Deze verschillen zetten we hieronder in tabelvorm op een rij:

	P1 poort	P4 poort
Actualiteit verbruiksgegevens	Real-time	Batchverzoeken: vertraging 1 dag Actuele stand: vertraging < 1 uur
Granulariteit verbruiksgegevens	10 seconden	>= 15 minuten
Historie verbruiksgegevens	Nee	Laatste 10 dagen, met een granulariteit van 15 minuten. Laatste 40 dagen met granulariteit van 1 dag. Laatste 13 maanden met granulariteit van 1 maand.
Overige gegevens opvraagbaar	Nee	Statusinformatie zoals actuele maximale doorlaatwaarde, schakelstand, etc.
Besturingsopdrachten	Nee	Ja, aan/afschakelen en aanpassen van de doorlaatwaarde. Ook tonen van een boodschap op de display van de meter.
Relevante regelgeving	Wbp	Wbp, Elektriciteitswet, Gaswet
Verantwoordelijke toezichthouder	CBP	NMa en CBP

Tabel: verschillen tussen de P1 en P4 poort. Bronnen voor gegevens over P4: [11] en [12].

In het onderstaande bespreken we de verschillende rollen, en de interfaces tussen deze rollen, uitgebreider.

3.3.1 Aangeslotene

Een aangeslotene is in dit verband een kleinverbruiker (persoon of (klein)bedrijf) die beschikt over een aansluiting op het elektriciteitsnetwerk (en dus over een analoge, digitale of slimme meter). In principe kunnen aangeslotenen ook grootverbruikers zijn, maar deze zijn buiten scope voor deze studie. Vaak zal een aangesloten kleinverbruiker een bewoner van een woonhuis zijn, maar het kan hier bijvoorbeeld ook om kleinere bedrijfspanden gaan.

3.3.1.1 Interface aangeslotene – ODA (P1)

De meterstanden die worden aangeboden via de P1 poort zijn, zoals beschreven in NTA 8130 [9]:

- De actuele meterstanden voor elektriciteit. Deze worden elke 10 seconden aangeboden.
- De laatste 24 uurmeterstanden voor gas. Deze worden tenminste eenmaal per 24 uur aangeboden.

Bij meterstanden voor elektriciteit gaat het om 4 waarden, namelijk voor hoog- en laagtarief, en voor geleverde elektriciteit aan de aangeslotene respectievelijk de teruggeleverde elektriciteit door de aangeslotene.

Naast meterstanden wordt via P1 ook het actueel vermogen elektriciteit gerapporteerd (elke 10 seconden), en statusinformatie over de elektriciteit- en gasaansluitingen (zoals de maximale doorlaatwaarde voor elektriciteit, en of de aansluitingen aan of uitgeschakeld zijn).

3.3.1.2 Interface aangeslotene – netbeheerder (P3)

Het P3 interface laten we buiten beschouwing aangezien zich dit volledig in het domein van de netbeheerder bevindt. Het betreft immers het interface tussen de meter en de netbeheerder. De aangeslotene is hier niet daadwerkelijk bij betrokken.

3.3.2 Netbeheerder

Dit is een marktpartij die op basis van de wet aangewezen is voor het beheer van één of meer

elektriciteits- of gasnetten. De netbeheerder is de partij die verantwoordelijk is voor het beheer van de slimme meter bij aangeslotene, en stelt de verbruiksgegevens uit de slimme meter op de P4-poort op verzoek beschikbaar aan andere partijen zoals leveranciers en ODA's. De netbeheerder verzamelt en verwerkt verbruiksgegevens alleen in opdracht van een leverancier (via het meetbedrijf). In de zin van de Wbp is de netbeheerder dus een bewerker en is de leverancier de verantwoordelijke voor de bewerking.

3.3.3 Interface netbeheerder – leverancier / ODA (P4)

De P4 interface kan worden beschreven in termen van welke informatie wordt uitgewisseld, hoe dit procesmatig is ingericht en welke toegangscontrole wordt toegepast.

Uitgewisselde informatie

De informatie die beschikbaar is via P4 wordt beschreven in verschillende bronnen: NTA 8130 [9], het Detailprocessmodel (DPM) [11], en de Business Specification Requirements (BSR) [12].

De meterstanden die via P4 opgevraagd kunnen worden zijn:

- De *actuele meterstanden* voor elektriciteit en gas.
- De *intervalstanden* van de laatste 10 dagen, met een resolutie van een kwartier voor elektriciteit en een uur voor gas (dwz. de laatste 960 kwartierstanden voor elektriciteit en de laatste 240 uurstanden voor gas).
- De *dagstanden* voor elektriciteit en gas, dwz. de standen aan het begin van de dag, voor de laatste 40 dagen.
- De *recovery maandstanden*, dwz. de laatste 13 maandstanden.

Sommige hiervan, zoals de mogelijkheid van het opvragen van recovery maandstanden en het opvragen van de laatste 40 dagstanden, worden niet in alle brondocumenten ([9], [11] en [12]) genoemd. Dit illustreert dat oudere documenten als [9] geen volledig actuele weergave meer bieden van de meterketen.

Naast meterstanden is ook statusinformatie opvraagbaar via P4, zoals de actuele maximale doorlaatwaarde van elektriciteit en een schakelstand, waaruit afgeleid kan worden of de meter aan of uit is.

Naast informatie opvraging kunnen via de P4 poort ook besturingsopdrachten aan de meter gestuurd worden. Het gaat dan om het aan/afschakelen van de aansluiting of het aanpassen van de doorlaatwaarde (door de leverancier), of het tonen van een boodschap op de display van de meter (door de leverancier of een ODA).

Procesmatige inrichting

De centrale toegang tot de P4 voor een LV, ODA, of mogelijk een RNB Gas wordt beheerd door EDSN die daarvoor een centrale portal heeft ingericht. Bij een verzoek voor data stuurt EDSN dit door naar de desbetreffende RNB, die de gevraagde informatie `vers' ophaalt uit de meter. De gevraagde informatie komt dus uit de meter zelf, en niet uit centrale databases die een RNB heeft aangelegd.

De slimme meter zal middels een logfile de consument inzicht geven in de data die op afstand zijn uitgelezen. Op dit moment is deze logfile nog niet aanwezig; naar verwachting zal de logfile aan het begin van de grootschalige uitrol wel aanwezig zijn in de slimme meter.

Bevinding 3:
Oorspronkelijk was voorzien dat de meetgegevens van alle consumenten zouden worden opgeslagen in een centrale database onder beheer van de netbeheerder. Inmiddels is er voor gekozen om de gegevens bij de consument in de meters te laten zitten, waarbij slechts een beperkt aantal gegevens worden gecached in het netbeheerdersdomein. Vanuit securityperspectief heeft deze keuze voordelen, maar daar staat het nadeel tegenover dat de keten hierdoor nog meer afhankelijk is van het correct functioneren van de meter zelf.

Het opvragen van de dagstanden, intervalstanden of maandstanden via P4 gebeurt door middel van een *batchverzoek* [11,12]. Zo'n batchverzoek bij de centrale P4 portal wordt door EDSN doorgegeven aan de RNBs, die de gevraagde informatie dan volgens een bepaald ophaalschema verzamelt uit de meters. Met een tweede verzoek bij de centrale P4 portal kunnen de gegevens de volgende dag [15] opgehaald worden. Dit betekent dus dat de intervalstanden die een ODA via P4 opvraagt geen realtime inzicht geven in het verbruik, omdat deze gegevens ongeveer een dag later pas beschikbaar zijn.

De overige instructies via P4, waaronder het opvragen van de actuele standen en het geven van schakelinstructies, gebeurt niet middels batchverzoeken maar middels zogenaamde *direct verzoeken*. Deze opdrachten worden in principe zo snel mogelijk uitgevoerd: binnen 1 uur, maar uiterlijk binnen 24 uur [15].

Toegangscontrole op de centrale P4 poort
Toegang tot P4 door leveranciers, ODAs en regionale netbeheerders gas gaat via de centrale P4 portal van EDSN.

Voor toegang tot de P4 portal moeten ODA's aan de RNB een accountantsverklaring afleveren (of,voor de eerste 4 maanden, een directieverklaring) en een ondertekende lijst met EAN codes van klanten door wie ze gemandateerd zijn om de dag- en intervalstanden uit te lezen [10, sectie 4]. EDSN checkt de directieverklaringen centraal voor alle RNBs, maar de individuele RNBs checken de accountantsverklaringen.

Technische authenticatie van leveranciers en ODA's door EDSN gebeurt door middel van client certificaten, zoals beschreven in [10]. Certificaten moeten in persoon worden opgehaald bij EDSN, waarbij legitimatie verplicht is, terwijl een bijbehorende PIN code per e-mail wordt verstuurd. Daarnaast wordt de P4 portal afgeschermd door een firewall die enkel toegang op fixed IP adressen toelaat. Het beschreven mechanisme is identiek voor leveranciers en ODA's.[10,13]

Bij de daaropvolgende toegangscontrole hebben leveranciers en ODA's verschillende autorisaties: in het bijzonder mogen leveranciers opdrachten geven tot het aan/uitschakelen van aansluiting of het veranderen van de maximale doorlaatwaarde (het veranderen van de maximale doorlaatwaarde naar nul ampere is effectief hetzelfde als afsluiten); ODA's mogen dit niet. Als onderdeel van de centrale portal is er een LV en ODA register, aan de hand waarvan gecontroleerd wordt of een partij een bepaalde operatie mag uitvoeren.

ODA's en leveranciers mogen enkel dag- en intervalgegevens opvragen als klanten daar expliciet toestemming voor gegeven hebben. In de huidige opzet van de centrale P4 portal wordt dit niet op het niveau van individuele aangeslotenen bewaakt door EDSN:

- Leveranciers hebben in principe de mogelijkheid om van al hun klanten de intervalgegevens op te vragen. EDSN controleert wel dat een leverancier enkel meetgegevens opvraagt van

zijn eigen klanten, maar kan niet checken of die klant ook toestemming heeft gegeven voor het inzien van intervalgegevens. De leverancier wordt hierbij dus door EDSN vertrouwd, maar in het perspectief van het leveranciersmodel is dat niet onlogisch.

- ODA's moeten weliswaar een lijst van klanten aanleveren, maar EDSN controleert niet of een ODA enkel gegevens van meters in de lijst opvraagt. In het onderzoek is niet gebleken of de individuele RNB's wel zo'n controle uitvoeren. Dit is mogelijk, omdat alle P4 verzoeken uiteindelijk via de RNB lopen, en de RNB beschikt over een door de ODA verstrekte klantenlijst. In ieder geval worden de ODA's dus door EDSN, en mogelijk ook door de RNB's vertrouwd. Naar onze mening is dit onvoldoende, en dient de netbeheerder een vorm van controle in te richten om te borgen dat alleen gegevens worden verstrekt van consumenten die hiervoor een overeenkomst met de ODA zijn aangegaan.

EDSN heeft naast de P4 portal ook een 'generiek portaal' tot de EDSN diensten: een webpagina, die toegankelijk is voor de verschillende partijen, waaronder netbeheerders, leveranciers, meetverantwoordelijken, en ook de beheerders van dit portaal. Via dit portaal kan onder meer toegang worden verkregen tot het centraal aansluitingenregister.

3.3.4 Leverancier

Een leverancier is een organisatie (vaak een bedrijf) die zich bezighoudt met het leveren van elektriciteit [8].

De leverancier verzamelt niet zelf verbruiksgegevens, maar geeft hiertoe opdracht aan een netbeheerder. In de zin van de Wbp is de netbeheerder dus een bewerker, en is de leverancier de verantwoordelijke voor de bewerking

Bevinding 4:
In het leveranciersmodel heeft de consument alleen een relatie met leverancier en eventueel ODA. Juist de netbeheerder heeft echter een centrale rol bij de distributie van meetgegevens. Dit kan leiden tot verwarring bij de consument of kast-muur situaties, bijvoorbeeld als de netbeheerder ten onrechte meetgegevens verstrekt aan een ODA of andere leverancier.

3.3.5 Overige Diensten Aanbieder (ODA)

Een belangrijk doel van het nieuwe marktmodel is het faciliteren van een vrije energiemarkt en nieuwe toetreders op deze energiemarkt. De 'Overige Diensten Aanbieder' (ODA) wordt in veel communicatie van overheid en de energiesector genoemd. Omdat het als een vrije marktrol wordt beschouwd is deze niet scherp ingekaderd (zie bevinding 1). Wel heeft Expert Group 2 (EG2) van de Task Force Smart Grids eind 2011 een aanbeveling aan de Europese Commissie gedaan [18], waarin op blz. 33 en 37 ODA's (Added Value Services) besproken worden. Als definitie wordt gehanteerd 'toegevoegde diensten, buiten energievoorziening, geleverd door een leverancier of derde partij op commerciële basis'. Aangegeven wordt dat op dit moment weinig voorbeelden bekend zijn; twee categorieën diensten worden genoemd:

- Diensten gericht op energiebesparing;
- Aanbiedingen van goederen of diensten door derden gerelateerd aan het energieverbruik (bv. korting op avondjes uit voor huishoudens die 's avonds weinig elektriciteit verbruiken).

Opvallend is dat de rol van 'ODA' een algemene term is die in het kader van de slimme meter keten voor verschillende typen partijen wordt gebruikt:

1. P4 ODA's (door de netbeheerder gecertificeerde partijen die meetgegevens ontvangen via het meetbedrijf;
2. P1 ODA's (derde partijen die de meetgegevens direct verkrijgen via de aangeslotene/kleinverbruiker (P1 poort);

3. Leveranciers (vergunninghouders) die naast hun leveranciersrol ook als P4 ODA en/of P1 ODA optreden.

Vanuit privacy- en securityperspectief hebben deze categorieën een verschillend profiel. Ten eerste omdat aan de P4 ODA's eisen kunnen worden opgelegd voor toegang tot de P4 poort, terwijl zulke eisen bij P1 ODA's niet kunnen worden afgedwongen. Ten tweede omdat de verwerkte informatie (granulariteit en actualiteit van de meetgegevens) verschillend kan zijn. Ten derde omdat de interface tussen de meter en de ODA een geheel ander karakter heeft.

3.3.5.1 Interfaces ODA – aangeslotene

Zoals eerder genoemd kan een ODA zowel via de P1 als de P4 poort aan verbruiksgegevens over consumenten (waar de ODA een overeenkomst mee heeft) komen. De belangrijkste verschillen zijn hierbij:

- Via P1 heeft men toegang tot meer gedetailleerde gegevens dan via P4, vg. de tabel in 3.3. Fysiek een aansluiting maken met de P1 poort bij de consument thuis kan alleen met duidelijke toestemming en medewerking van de klant. De klant kan deze toegang desgewenst zelf weer ontnemen.
- Voor toegang tot P4 geldt het keuzevrijheidmodel waarbij de klant toestemming moet geven aan een leverancier of ODA. Op dit moment heeft de klant geen inzage in informatieverzoeken via de P4-poort. Dit zal veranderen als de voorziene logfunctie in de meter wordt geïmplementeerd.

Bij diensten of producten die gebruik maken van P1 kan een verder onderscheid gemaakt worden tussen

- offline oplossingen, waarbij de gegevens uit P1 onder controle van de consument thuis worden opgeslagen en verwerkt door de consument thuis. Strikt genomen is een ODA in dit geval niet zozeer een dienstaanbieder als wel een productaanbieder.
- online diensten, waarbij deze gegevens door de ODA worden verzameld en waartoe de klant toegang heeft via bijvoorbeeld een webinterface of een smartphone app.

Hierbij zijn er nog allerlei mogelijkheden, bijvoorbeeld diensten die

- enkel de gegevens doorsturen naar de klant,
- deze gegevens in bewerkte vorm aanbieden,
- de gegevens ook bewaren,
- gegevens ook voor andere doeleinden gebruiken, met name in het geval dat de ODA ook leverancier of netbeheerder is.

Bevinding 5:
De uitwerking van het nieuwe marktmodel is nog in volle gang terwijl dit onderzoek loopt. Op basis van de voor dit onderzoek verkregen informatie lijken diverse aspecten van privacy- en security nog onvolledig uitgewerkt, vastgelegd en geïmplementeerd.

3.4 Gegevensbestanden

Bij de verschillende marktpartijen in de slimme meter keten worden verbruiks- en andere gegevens die betrekking hebben op een kleinverbruiker opgeslagen in gegevensbestanden. Deze bespreken we hieronder kort. Het voert te ver binnen het kader van deze studie om deze gegevensbestanden en de *access control* (toegangsbeheer) die daarbij hoort in detail te behandelen. Wel kunnen we in zijn algemeenheid de twee belangrijkste vragen noemen die bij het beoordelen van de kwaliteit van *access control* gesteld dienen te worden:

- Zijn de voorwaarden waaronder een partij bij bepaalde gegevens mag duidelijk geëxpliciteerd, en effectief te controleren? (in het geval van verbruiksgegevens moet de verbruiker waar de gegevens betrekking op hebben bijvoorbeeld toestemming hebben gegeven, en de gegevens mogen alleen gebruikt worden voor het doel waar de verbruiker toestemming voor heeft gegeven).
- Wordt toegang tot het gegevensbestand (voor inzien, wijzigen, verwijderen) gelogd, zodat te controleren is wie voor welk doel toegang heeft gehad? Dit is met name van belang om te kunnen controleren of het doelbindingsprincipe nageleefd wordt.

3.4.1 (Centraal) aansluitingenregister (CAR of C-AR)

Hierin staan de zgn. 'stamgegevens' van elke aansluiting, waaronder de naam van de aangeslotene, GPS coördinaten, en de leverancier. Details hierover staan beschreven in de Informatiecode, Sectie 2.1. Dit zijn duidelijk persoonsgegevens. Dit Centrale Aansluitingenregister (afgekort als C-AR en CAR) wordt verzorgd door EDSN.[10] Alle netbeheerders doen hieraan mee, m.u.v. Gas Transport Services (GTS), de beheerder van het landelijke gastransportnet. Alle mutaties in het CAR worden bewaard, en zijn op te vragen.

Authenticatie:

Er is een 'generiek portaal', beveiligd met username/wachtwoord binnen een VPN . Functioneel beheerders kunnen als supergebruiker via dit portaal de instellingen ervan regelen.

Autorisatie:

Leveranciers hebben enkel toegang tot hun klanten, en voor de mutaties voor de periode dat ze leverancier waren.

3.4.2 EAN codeboek, bestaande uit een 'open' en een 'gesloten' deel.

Hierin staat een deel van de gegevens die ook in het aansluitingenregister staat, maar niet de naam van de aangeslotene of de leverancier.

In het open deel staan de EAN codes per adres. In het gesloten deel staan meer gegevens, waaronder de verantwoordelijke RNB en de wijze van bemeting. Details hierover staan beschreven in de Informatiecode [5], sectie 2.3.

Het EAN codeboek wordt beheerd door EDSN. Beide zijn online beschikbaar. Het open deel via eancodeboek.nl. Het gesloten deel wordt ook via een elektronische gegevensdrager beschikbaar gesteld.

Zowel het open als het gesloten deel van het EAN codeboek bevatten geen persoonsgegevens. Het biedt wel een mogelijkheid om EAN codes aan adressen te koppelen; hiermee zijn dus andere gegevens die naar een EAN code refereren te herleiden tot een adres, en worden zulke gegevens daardoor mogelijk persoonsgegevens.

3.4.3 Toegankelijk Meetregister

Hierin staan meetgegevens, per EAN code van de aansluiting. Het betreft hier meetgegevens van oude meters, die door de meteropnemer dan wel de klant zelf zijn gerapporteerd. Dit geeft dus geen gedetailleerd inzicht in het verbruik. Deze meetgegevens worden volgens de Informatiecode [5] bewaard voor een periode van maximaal 3 jaar, vooral om fouten in de doorgegeven standen te kunnen ontdekken. Het toegankelijk meetregister staat helemaal los van de P4 poort, en de meetgegevens die via de P4 poort uitgelezen kunnen worden.

---

[10] Zie: zie http://www.edsn.nl/default.asp? id=440 of http://www.edsn.nl/edsn/carmovie.wmv

3.4.4 Contracteindegegevensregister

Hierin staat welke leverancier aan welke EAN code levert, en wat de einddatum dan wel opzegtermijn is. Dit zijn persoonsgegevens. Leveranciers hebben inzage in de gegevens van een kleinverbruiker indien ze hiertoe gemachtigd zijn door deze kleinverbruiker.

4 Risicoanalyse

4.1 Methodiek

Bij een risicoanalyse worden eerst dreigingen geïnventariseerd. Als een dreiging daadwerkelijk optreedt dan heeft dit een bepaald gevolg, dit noemen we impact. Verder is de kans dat een dreiging optreedt van belang. De ene dreiging zal een hogere kans van optreden hebben dan de andere. Zo komen we van een dreiging tot een risico. De omvang van een risico wordt bepaald door:

- de kans dat de dreiging zich zal voordoen;
- de verwachte impact indien de dreiging zich voordoet.

Dit kan geformuleerd worden als Risico = (Kans op de dreiging x Impact van de dreiging).

Voor zowel kans als impact kan een kwalitatieve of een kwantitatieve benadering worden gegeven. Zo kunnen kans en impact kwalitatief worden uitgedrukt in bv. hoog – midden – laag. Kans kan kwantitatief worden uitgedrukt in een percentage, terwijl impact bv. kan worden uitgedrukt in euro's.

In deze risicoanalyse doen we een kwalitatieve beoordeling. Dit geeft een goed beeld van het relatieve belang van de diverse risico's. Een kwantitatieve beoordeling is praktisch moeilijk. Dit geldt zeker aan de impactzijde: negatieve impact omvat ook moeilijk te kwantificeren zaken als 'verlies van consumentenvertrouwen'. Maar ook aan de kanszijde is een kwantitatieve beoordeling lastig. De kans wordt beïnvloed door eventuele maatregelen die genomen zijn om de dreiging te voorkomen of de kans daarop te verminderen (preventie), en of het optreden van een dreiging gedetecteerd kan worden (detectie). Dit soort aspecten is in deze uitrolfase nog niet uitgekristalliseerd (dit is juist waar de toezichthouders straks op zullen moeten toezien).

Elke marktrol wordt zowel apart als in samenhang met de andere bekeken. Onderscheid wordt gemaakt tussen dreigingen:

- Vanuit geautoriseerde handelingen door ketenpartijen/marktrollen;
- Vanuit ongeautoriseerde handelingen door op zichzelf geautoriseerde ketenpartijen;
- Vanuit ongeautoriseerde derden (bijv. een aanval van hackers of cybercriminelen).

De focus ligt op de eerste twee categorieën dreigingen.

Zoals genoemd is het netbeheerdersdomein buiten scope. Omdat de netbeheerders wel een centrale functie in de keten innemen als de partij die de meetgegevens via de P4 poort distribueren, ontkomen we er niet aan om wel degelijk de interacties tussen netbeheerders en andere partijen te analyseren.

Deze risico analyse is gebaseerd op een studie van relevante documentatie (zie de lijst met informatiebronnen in de appendix) en een aantal brainstorm sessies met experts. Op basis hiervan is de onderstaande long-list met risico's uitgewerkt. In het volgende hoofdstuk 5 bespreken we de samenhang tussen de verschillende risico's, welke risico's er uit springen door hun potentieel hoge impact of structurele karakter, en identificeren we eventuele fundamentele risico's die aanwezig zijn in de slimme meter keten.

4.2 Risico's voor privacy van aangeslotenen

Zoals in hoofdstuk 2 besproken zijn verbruiksgegevens in potentie zeer privacygevoelige gegevens, met name als ze een hoge granulariteit hebben en actueel zijn. Risico's rond privacy zijn breder dan alleen een "lek" van gegevens. Belangrijk is bijvoorbeeld ook dat aangeslotenen weten waarvoor ze in relatie tot hun privacy toestemming geven als ze een overeenkomst met een marktpartij aangaan.

4.2.1 Gegevenslek in communicatie

(Requirements: R10)

In de slimme meter keten verplaatsen verbruiksgegevens zich van de slimme meter zelf naar de verschillende partijen in de keten. Een voor de hand liggende dreiging tegen de privacy van aangeslotenen is een lek van deze gegevens als ze zich door de keten heen verplaatsen. Hierbij moeten we onderscheid maken tussen de gegevens die via de P3 en P4 poort beschikbaar komen, en de gegevens die via de P1 poort beschikbaar komen. In beide gevallen zullen er bijvoorbeeld andere communicatietechnologieën gebruikt worden en zijn er andere afspraken gemaakt tussen de partijen.

4.2.1.1 Gegevens afkomstig uit P3 / P4

Zoals beschreven in 3.3.1 vindt bij de P4 authenticatie plaats op basis van client certificaten. Daarmee wordt gewaarborgd dat alleen geautoriseerde partijen toegang verkrijgen tot de P4.

Vervolgens is belangrijk dat bij het opvragen van gegevens via de P4 wordt gecontroleerd of de slimme meter in kwestie op dat moment onder verantwoordelijkheid van de betreffende leverancier of ODA valt. Deze eis is opgenomen in de business specification requirements van de P4 [12] pag. 21. Uit gesprekken met EDSN is echter gebleken dat EDSN deze controle niet uitvoert, onduidelijk is of de RNB dit wel doet.

De verbruiksgegevens die afkomstig zijn uit de P4 hebben een relatief lage granulariteit (minimaal een meting per kwartier) en zijn niet real-time (er zit een vertraging van 1 tot 24 uur tussen). Dit maakt de gegevens vanuit privacy-oogpunt minder gevoelig, aangezien er minder uit afgeleid kan worden over het gedrag van bewoners dan bij een hogere granulariteit, en aan de hand van deze gegevens niet betrouwbaar vastgesteld kan worden of bewoners op een specifiek actueel tijdstip thuis zijn.

Tot slot zijn de gegevens die via de P3 en P4 poorten gecommuniceerd worden al relatief uitgebreid gereguleerd, wat de risico's kleiner maakt dat marktpartijen die zich aan deze regulering conformeren de fout in gaan.

4.2.1.2 Gegevens afkomstig uit P1

Anders dan bij de P3/P4 poorten is data uit de P1 poort van een relatief hoge granulariteit en is deze actueler. Dit betekent dat uit deze gegevens meer afgeleid kan worden over het gedrag van bewoners, en bovendien een vorm van real-time surveillance met gegevens uit deze poort mogelijk wordt. Bovendien wordt de P1 poort nadrukkelijk als een "vrij" domein geïnterpreteerd: hier zijn – in tegenstelling tot bij de P3/P4 poort – geen afspraken of bijzondere regels opgesteld over hoe met verbruiksgegevens omgegaan dient te worden. Niettemin is de Nederlandse en Europese wetgeving ook bij deze gegevens gewoon van kracht en is er ook toezicht in de vorm van het CBP.

Een belangrijke factor hierbij is dat de aangeslotene zelf kan besluiten of hij of zij een overige diensten aanbieder toegang geeft tot de P1 poort; hier moet – in tegenstelling tot de P3 / P4 poorten – de aangeslotene een installateur toegang geven tot het eigen huis, dan wel zelf een apparaat op de P1 poort aansluiten. Dit impliceert dat de aangeslotene directe controle heeft over wie tot deze poort toegang krijgt.

Daarbij is het wel van groot belang dat de aangeslotene weet wat er gebeurt met de verbruiksgegevens die door een ODA op deze wijze verzameld worden. Hier komen we later op terug. Reële risico's bij de P1 poort zijn dat de veiligheid van verbindingen die door ODA of aangeslotene gebruikt worden om verbruiksgegevens te communiceren niet toereikend is, of dat apparatuur van een ODA deze gegevens slecht beveiligd opslaat.

4.2.2 Gegevenslek uit systemen marktpartijen

(Requirements: R2, R6, R10, R14)

Verbruiksgegevens zullen worden opgeslagen in databases, en niet alleen in de slimme meter zelf. Leveranciers hebben deze gegevens nodig om hun dienstverlening mogelijk te maken en dit geldt ook voor ODA's die online diensten aanbieden (zie 3.3.5.1). Gegevens uit deze databases kunnen "lekken" naar partijen waarvoor die gegevens niet bedoeld zijn. Dit kan verschillende oorzaken hebben: een technische fout, menselijk falen of een aanval van kwaadwillenden.

4.2.2.1 Menselijk falen

Waar mensen werken worden fouten gemaakt, zij het bewust (vriendendienst) dan wel onbewust (niet goed op de hoogte zijn van de wijze waarop al dan niet met persoonsgegevens omgegaan mag worden). In de backoffice van de verschillende marktpartijen betrokken in het proces van gegevensverwerking kan dan ook een scala aan privacyrisico´s geïdentificeerd worden. Om enkele voorbeelden te noemen: het uitlekken van verbruiksgegevens, uitlekken van afsluitgegevens, lekken van gegevens door bijvoorbeeld het verlies van een gegevensdrager met verbruiks- of afsluitgegevens, communicatielek (bijvoorbeeld via email of per ongeluk registratie in open in plaats van gesloten webomgeving) van verbruiks- of afsluitgegevens.

De kans op het optreden van dit risico is sterk afhankelijk van de wijze waarop de bedrijfsvoering wordt ingericht, welke procedures gevolgd worden, en welke training personeel krijgt. Hierbij moet ook aandacht zijn voor instructie van tijdelijke krachten in het omgaan met persoonsgegevens. De impact is in potentie wel hoog, omdat in een database (verbruiks)gegevens van grote aantallen aansluitingen verzameld worden.

4.2.2.2 Technische fout

Een variant van menselijk falen is een fout bij ontwerp of implementatie van de informatietechnologie. Door fouten kan bijvoorbeeld een database, of delen daarvan, onbeveiligd toegankelijk worden via het internet. Ook hier kan de impact hoog zijn omdat het over gegevens over grote aantallen aansluitingen gaat.

Bij ODA's die online diensten aanbieden zullen de gegevens uit P1 in veel gevallen worden gecommuniceerd via een door de ODA beheerde web-interface. Zowel de web front-end als de achterliggende database kunnen kwetsbaarheden bevatten. Hetzelfde geldt voor toepassingen die door de ODA worden gebruikt om de opgeslagen gegevens te verwerken.

4.2.2.3 Aanval van buitenaf

De hiervoor genoemde risico's van menselijk falen en technische fouten vallen binnen het domein van geautoriseerde marktpartijen. Een aanvullend risico is dat van kwaadwillende derden die actief een informatiesysteem van een marktpartij weten te hacken. Hierbij kan misbruik worden gemaakt van de eerder genoemde menselijke en technische tekortkomingen. Een lange reeks voorvallen waarin systemen van organisaties gehackt zijn en grote hoeveelheden (persoons)gegevens buitgemaakt zijn laat zien dat de kans hierop niet denkbeeldig is. De impact kan hoog zijn als het om gegevens over grote aantallen aansluitingen gaat. Goede beveiligingsmaatregelen zijn daarom noodzakelijk.

4.2.3 Schending van doelbinding principe

(Requirements: R1, R2, R4, R6, R10)

Een belangrijk uitgangspunt bij privacy(wetgeving) is het doelbindingsprincipe: gegevens worden alleen verwerkt voor een helder omschreven doel dat naar het data subject toe duidelijk is gecommuniceerd, en waarvoor van deze toestemming is verkregen. In de slimme meter keten is als

het om verbruiksgegevens gaat zeker het risico aanwezig dat dit doelbindingsprincipe geschonden wordt.

Een ODA of leverancier kan verbruiks- of schakelgegevens gebruiken voor andere doeleinden dan waarvoor de aangeslotene toestemming heeft gegeven. Denk bijvoorbeeld aan gerichte marketing van diensten of producten op basis van verbruiksgegevens. Een andere mogelijkheid is dat verbruiksgegevens van kleinverbruikers worden gedeeld met als doel opsporing, bijvoorbeeld door justitie of overheidsdiensten die (uitkerings)fraude opsporen.

4.2.3.1 Granulariteit niet in overeenstemming met doelbinding

Een bijzondere eigenschap van verbruiksgegevens vanuit privacy oogpunt is dat de granulariteit van de gegevens over het algemeen goed te koppelen is aan een doel. Is het doel bijvoorbeeld maandelijkse facturatie, dan is een maandelijkse meting afdoende. Voor een real-time monitoring dienst door een ODA is een veel hogere granulariteit noodzakelijk. Een risico dat kan optreden is dat ODAs of leveranciers gegevens met een hogere granulariteit bewerken dan noodzakelijk is voor het doel of de dienst waarmee de aangeslotene ingestemd heeft.

4.2.3.2 Gebruik van onvoorziene gegevens

Door een toename in intensiteit van gegevensverwerking door verschillende partijen op verschillende plaatsen voor verschillende doeleinden, kunnen gegevens gegenereerd worden die niet beoogd of voorzien waren, maar welke als bijproduct wel informatie oplevert die voor bepaalde partijen relevant kan zijn. Hoewel doelbinding in principe in de weg staat aan het verdere gebruik van deze gegevens, kan dit bijvoorbeeld wel conflicteren met meldplichten in geval van vermoedens van crimineel gedrag.

4.2.3.3 Koppeling van systemen

Het voorgaande punt betreft nog een groter risico in een scenario waarin de meetgegevens van elektriciteit gekoppeld worden met andere gegevens, bijvoorbeeld meetgegevens van water en gas. Hoewel ook hier het beginsel van doelbinding in beginsel in de weg staat aan een dergelijke koppeling, is een situatie denkbaar waarin een kleinverbruiker hiertoe toestemming geeft in het licht van een bepaalde ODA, of de situatie waarin politie en justitie op basis van bestaande bevoegdheden alle beschikbare meetgegevens op mogen vragen en deze gegevens aldus legitiem kunnen koppelen. Bijvoorbeeld wanneer een netbeheerder/leverancier gedwongen inzage moet geven in gebruiksgegevens van een kleinverbruiker die door justitie wordt verdacht van uitkeringsfraude.

4.2.4 Onduidelijkheid bij aangeslotene over hetgeen waarvoor toestemming gegeven wordt

(Requirements: R1, R3, R4, R6, R10)

Als een consument toestemming geeft om meetgegevens op te vragen via P4, moet het voor deze consument duidelijk zijn waar toestemming voor gegeven wordt: om welke gegevens het gaat en wat ermee gedaan wordt. Dit speelt ook bij toegang via P1 en bij ODA's die niet andere rollen vervullen, maar vooral bij een ODA die ook nog een andere rol heeft (bijv. leverancier) bestaat het risico dat de klant ongemerkt en ongewenst toestemming geeft (bijv. door te vergeten een bepaald hokje aan te vinken bij het afsluiten of verlengen van een contract). De vraag is dan: weet de consument wel waar hij of zij toestemming voor geeft?

De transparantie van de wijze waarop met meetgegevens afkomstig uit de P1 poort wordt omgegaan is grotendeels afhankelijk van de wijze waarop ODA's de dienstverlening inrichten. Een risico hierbij is dat gebruikers geen effectief inzicht hebben in de wijze waarop dit gebeurt, wat een slimme meter via de P1 poort aan gegevens vrijgeeft, en of en voor welke doeleinden dit noodzakelijk is.

Een vergelijkbaar risico speelt in de gereguleerde keten via de P3- en P4-poorten. Technisch gezien heeft de aangeslotene te maken met de netbeheerders, die immers in eerste instantie de

meetgegevens verzamelen via P3 poort en distribueren via P4 poort. Echter, de aangeslotene gaat zelf geen verbintenis aan met netbeheerders, maar alleen met leveranciers en ODA's. Voor een aangeslotene kan het intransparant zijn wat precies met de data uit de P3 en P4 poort gebeurt, en hoe hiermee omgegaan wordt (zie bevinding 4). Het is dus essentieel dat hierover tussen verantwoordelijke voor de verwerking en de verwerker zelf (respectievelijk Leverancier/ODA en netbeheerder) duidelijke afspraken gemaakt worden, en dat deze afspraken op een begrijpelijke wijze naar de aangeslotene toe gecommuniceerd worden.

4.2.4.1 Eén marktpartij twee rollen

Als twee verschillende rollen bij één marktpartij terecht komen, kan deze partij de beschikking krijgen over verschillende data sets die bij de twee verschillende rollen horen en welke niet per definitie gedeeld mogen worden aangezien dit in strijd zou kunnen komen met doelbinding. Feitelijk is het echter eenvoudig om binnen een organisatie deze informatie te delen, en wellicht lastig om door middel van autorisaties te regelen dat medewerkers slechts bij een van de twee data sets kunnen. Zeker indien een functie verschillende taken omvat waarvoor toegang tot beide data sets noodzakelijk is. Juist de combinatie van verschillende data sets kan nieuwe informatie, en daarmee nieuwe privacy risico's, doen ontstaan.

4.2.4.2 Ondoorzichtigheid rolverdeling

Een ander punt dat risico´s met zich brengt is een gebrek aan inzichtelijkheid van de rolverdeling tussen partijen. Niet alleen voor een kleinverbruiker waarvoor het lastiger wordt om te bepalen welke partij voor welk doeleinde gegevens verwerkt, en ook aan welke partijen al dan niet toestemming verleend moet worden voor bepaalde verwerkingen. Maar ook voor de partijen betrokken in het marktmodel. Bijvoorbeeld als een leverancier het daadwerkelijke meten uitbesteedt aan een meetbedrijf, hoe weet de netbeheerder dan aan welk meetbedrijf de leverancier zijn meetverantwoordelijkheid heeft uitbesteed en wie de netbeheerder dus toegang moet verlenen tot bepaalde data? Hetzelfde probleem geldt met de zichtbaarheid, kenbaarheid en verifieerbaarheid van machtigingen. Hoe kan geverifieerd worden of een partij daadwerkelijk gemachtigd is (door een bevoegde partij) om eenmalig inzage te krijgen in de stamgegegevens, contract-eindegegevensregister, meetregister, etc.

4.2.5 Gebrekkige controle bij uitbesteding gegevensbewerking

(Requirements: R2, R4, R6, R10, R14)

Binnen de slimme meter keten kunnen partijen bepaalde activiteiten uitbesteden aan andere partijen. Dit geldt ook voor activiteiten waarbij meetgegevens verzameld of verwerkt worden. Een risico is bijvoorbeeld dat een leverancier onvoldoende controle uitoefent op een meetbedrijf als uitvoerder van een proces waarvoor de leverancier uiteindelijk verantwoordelijk is. Een speciaal geval van dit risico is de mogelijkheid dat gegevens uit de P1 of P4 poort via een ODA richting buitenlandse partijen gaan (bijvoorbeeld Facebook, Google) en zo buiten het toezicht NMA / CBP komen te vallen, al valt de eerste verstrekking naar deze partijen wel degelijk onder toezicht van het CBP.

4.2.6 Gebrekkige invulling van inzage-, correctie-, verwijder- en verzetsrecht van aangeslotene

(Requirements: R1, R3, R4, R6, R10)

Onvoldoende, dubbelzinnige of onduidelijke informatie richting de kleinverbruiker kan het bestaande model in keuzes een wassen neus doen zijn. Alleen als kleinverbruikers de keuzes, en de daaraan verbonden consequenties, daadwerkelijk begrijpen en deze keuzes daadwerkelijk vrij zijn, draagt een model van keuze bij aan de privacyvriendelijkheid van het systeem. Het inzage-, correctie-, verwijder- en verzetsrecht zijn wettelijk vastgelegd om hieraan voor de consument invulling te helpen geven.

4.2.7 Overschrijding van bewaartermijn van gegevens

(Requirements: R1, R2, R4, R5, R6)

In principe dienen verbruiksgegevens niet langer bewaard te worden dan noodzakelijk is voor de dienstverlening die een ODA of Leverancier aanbiedt. Een risico is aanwezig dat dienstenaanbieders verbruiksgegevens langer bewaren dan noodzakelijk is, niet vastleggen wanneer gegevens gewist moeten worden, en daar ook geen procedures voor ingericht hebben.

4.2.8 Gebrekkige data-portabiliteit van gegevens (customer lock-in)

(Requirements: R6, R10)

Een (nieuw) uitgangspunt in data protectie wetgeving is data portabiliteit: kan een gebruiker “zijn” data (waar de waarde van een dienst aan ontleend wordt) eenvoudig meenemen naar een andere dienst, of is dit niet mogelijk? Dit is een risico wat met name bij ODA’s kan spelen. Als de waarde van een dienst bijvoorbeeld grotendeels ontleend wordt aan de mogelijkheid om een verbruikshistorie over langere periode te bekijken, dan wordt het voor een consument lastig om van een concurrerende dienst gebruik te gaan maken als de historische data daaronder niet meegenomen kan worden.

4.2.9 Onduidelijkheid bij uitzonderingsgevallen

(Requirements: R2, R4, R5, R6, R10, R14)

Ook bij de kleinverbruiker kan sprake zijn van een meer complexe rolverdeling, bijvoorbeeld in geval van huurwoningen. Is het bij huurwoningen altijd duidelijk dat de aangeslotene de huurder is en niet de verhuurder? Kan bijvoorbeeld een woningbouwvereniging gegevens over al haar klanten inzien?

4.3 Risico’s voor beschikbaarheid en integriteit meetgegevens

4.3.1 Storing in beschikbaarheid meetgegevens via P4 poort

(Requirements: R11, R12)

Dit risico valt buiten scope van deze analyse omdat de netbeheerder verantwoordelijk is voor de P4 poort. Op het facturatieproces heeft dit (zo lang de beschikbaarheid niet over zeer lange periodes onderbroken wordt) geen invloed omdat verrekening altijd kan gebeuren op het moment dat de meetgegevens weer beschikbaar komen.

Bovendien kunnen meterstanden ook nog steeds door een kleinverbruiker zelf worden afgelezen en op de website worden ingevuld van een energieleverancier.

4.3.2 Storing in beschikbaarheid meetgegevens via P1 poort

(Requirements: R11, R12)

Het tijdelijk niet beschikbaar zijn van meetgegevens heeft voor de aangeslotene meestal een geringe impact, al zal dit afhangen van de overige diensten die de aangeslotene afneemt die van deze gegevens afhankelijk zijn. Eventuele energiebesparings- of andere toegevoegde waarde diensten kunnen tijdelijk verstoord worden. Beschikbaarheidsproblemen bij grotere aantallen gebruikers kunnen wel substantiële impact hebben op ODA’s, immers hun dienstverlening is gebaseerd op het verwerken van actuele meetgegevens.

Uitgaande van correct functioneren van de P1 poort zelf (verantwoordelijkheid van de netbeheerder) kunnen problemen optreden bij de communicatie tussen de P1 poort en de ODA die deze verwerkt:

- In het domein van de kleinverbruiker kunnen verstoringen optreden in de hardware en (draadloze) communicatiemedia;
- De (Internet-) interface van de ODA kan onbeschikbaar raken, bv. door hardware/software storingen in servers, DDoS-aanvallen of overbelasting anderszins.

Vooral in zijn eigen belang kan de ODA maatregelen treffen om de kans en impact van verstoringen te beperken. Voor de aangeslotene zal de impact beperkt blijven.

4.3.3 Integriteit meetgegevens

(Requirements: R7, R8, R9)

Bij de integriteit van verbruiksgegevens is het belangrijk dat meetgegevens via verschillende wegen uit de slimme meter beschikbaar komen: via de P3 poort naar de netbeheerder, via P1 poort naar ODA, en via een display af te lezen door de aangeslotene. De kans dat meetgegevens ergens in de keten *ongemerkt* gewijzigd worden is daardoor laag, tenzij dit in de slimme meter zelf gebeurt.

Door deze verschillende informatiestromen die wellicht op iets verschillende tijdstippen worden gemeten, is de kans wel hoog dat de getallen uit de P3, de P1 en op het display niet precies gelijk zijn.

Hoe meer partijen, applicaties en registraties betrokken zijn in het proces van energielevering en de levering van overige diensten, des te groter de kans op fouten in de gegevens. Foutieve meetgegevens of foutieve koppelingen tussen gegevens en NAW-gegevens kunnen grote gevolgen hebben voor de betrokken data subjecten.

4.3.4 Manipulatie of technische fout bij de meter zelf

(Requirements: R7)

Een ander risico hangt samen met meetfouten. Bij de oude meter lijkt het risico voor meetfouten voor de kleinverbruiker kleiner, aangezien niet op afstand wijzigingen aangebracht kunnen worden door bijvoorbeeld het pushen van nieuwe firmware naar de slimme meter. Voor aanpassingen in de traditionele meter moet iemand fysiek langskomen, de kleinverbruiker kan hierdoor controle uitoefenen. Dus de netbeheerder kan de meter niet ongemerkt aanpassen omdat deze achter de voordeur zit en de kleinverbruiker kan de meter niet aanpassen omdat deze verzegeld is en beide partijen kunnen vragen om ijking (bijv. bij KEMA).

Bij de nieuwe meter, die op afstand geregeld en gelezen wordt is de controle voor de kleinverbruiker beperkter. En hoewel zijn privacy er vanuit een oogpunt van het huisrecht op vooruit gaat, er hoeft niemand meer over de vloer te komen, is zijn bewijspositie in geval van conflicten over de meterstand moeilijker. De inrichting van het systeem is hier mede bepalend voor de positie van de kleinverbruiker: één aanspreekpunt bij conflict (leverancier en niet achterliggende meetbedrijf), duidelijke klachtenprocedures, detectiemechanismen van manipulatie en/of fouten, duidelijkheid over wie de bewijslast draagt, de beschikbaarheid van logbestanden van het pushen van firmware dan wel het wijzigen van instellingen in de meter voor kleinverbruikers.

De integriteit van de meter zelf is dus een cruciale requirement in de slimme meter keten, immers: alleen als het functioneren van de meter boven twijfel verheven is kan deze worden gebruikt om aanpassingen van de meetgegevens elders in de keten vast te stellen. Dus: de impact van ongeautoriseerde meetgegevens in de keten hangt af van de meter als onbetwist ijkpunt. Om deze reden noemen we hier een aantal dreigingen tegen de integriteit van de meter, hoewel deze eigenlijk buiten scope van deze risicoanalyse vallen (verantwoordelijkheid voor de meter valt in het netbeheerderdomein): een inadequaat ijkingsproces voor initiële installatie; ongeautoriseerd aanpassen van de meter door lokale manipulatie door de aangeslotene (bv. met behulp van een ‘kastje en een app’); aanpassen van de meter door een frauderende monteur; verstoring van de werking door een technische fout; fout in firmware-update (bv. door gebrekkig testen); aanpassing van de metersoftware of –configuratie door een externe aanvaller.

4.3.5 Verlies van meetgegevens in leverancierssystemen

(Requirements: R5, R10)

De kans op dataverlies is bij behoorlijk IT-beheer beperkt. Daarnaast zal de impact op het facturatieproces beperkt zijn omdat de laatste 13 maandstanden opnieuw via de P4-poort kunnen worden opgevraagd.

4.3.6 Corruptie van meetgegevens in leverancierssystemen door technische fout
(Requirements: R5, R8, R9)
Dit risico is niet nieuw ten opzichte van de situatie in de traditionele meetketen. De impact is potentieel hoog omdat veel aangeslotenen de facturatiefouten niet of pas na langere tijd zullen constateren, met mogelijk grote imagoschade voor de leverancier.
De leverancier dient dan ook passende maatregelen te treffen om te waarborgen dat eenmaal verkregen meetgegevens niet door systeemfouten kunnen worden gewijzigd. Voorbeelden van maatregelen gericht op detectie van integriteitsschending zijn digitale handtekeningen, *hashing* en CRC checks (de laatstgenoemde zijn technologische oplossingen om wijzigingen in data pakketten te kunnen herkennen).

4.3.7 Corruptie van meetgegevens in leverancierssystemen door menselijke fout
(Requirements: R5, R6, R8, R9)
Ook dit risico is niet nieuw ten opzichte van de situatie in de traditionele meetketen. De leverancier doet er goed aan maatregelen treffen om de integriteit van meetgegevens te beschermen, zodat deze niet per ongeluk kunnen worden gewijzigd.

4.3.8 Corruptie van meetgegevens in leverancierssystemen door kwaadwillende medewerker
(Requirements: R5, R6, R8, R9)
Ook dit risico is niet nieuw ten opzichte van de situatie in de traditionele meetketen. Medewerkers kunnen een motief hebben om de meetgegevens van specifieke of – minder waarschijnlijk – van grote groepen aangeslotenen te manipuleren. Voorbeelden van zulke motieven zijn vriendendiensten voor kennissen, manipulatie door derden (‘social engineering’) en wraakacties tegen de werkgever. Maatregelen gericht op preventie en detectie kunnen de kans en impact beperken.

4.3.9 Corruptie van meetgegevens tijdens overdracht vanuit P4 poort
(Requirements: R8, R9)
Externe aanvallers kunnen meetgegevens die via de P4 worden verstrekt manipuleren. De kans hierop hangt af van de wijze waarop de interface tussen RNB en leverancier is ingericht. Zoals beschreven in 3.3.2 zijn zinvolle maatregelen genomen om de P4 portal te beveiligen. Hierbij spelen zowel de netbeheerder als de leverancier een rol, zo krijgt de leverancier alleen toegang tot de P4 poort wanneer deze zich via een client-certificaat kan authenticeren.

4.3.10 Gebrekkige afhandeling van geschillen
(Requirements: R7, R8, R9, R10)
In het leveranciersmodel is de leverancier verantwoordelijk voor het vaststellen en verwerken van de meetgegevens. De leverancier dient dus een adequaat loket en proces in te richten voor kleinverbruikers die de meetgegevens betwisten.

In de slimme meter keten is dit een reëel risico omdat kleinverbruikers meetgegevens kunnen ontvangen via twee kanalen: uit de P1-poort (al dan niet na verwerking door een ODA) en uit de P4-poort (via ODA of leverancier). Wanneer deze gegevens onderling afwijken kan dit leiden tot aantasting van het vertrouwen met imagoschade voor met name de leverancier.

In geval van geschillen is het voor zowel de aangeslotene als de leverancier van belang dat kan worden teruggevallen op onbetwiste back-up gegevens. In de huidige keten is dit lastig omdat meetgegevens alleen in de meter en bij de leverancier worden opgeslagen, en niet centraal bij de netbeheerder als onafhankelijke derde.

4.4 Risico's voor beschikbaarheid van elektriciteit

Wanneer een meter elektriciteit of gas kan afschakelen als gevolg van een ongeautoriseerd of foutief schakelbericht, waardoor aangeslotenen zonder elektriciteit komen te zitten, kan dit grote impact hebben (zie 2.1.2). Deze dreiging ontstaat door de mogelijkheid om op afstand een meter aan- en af te schakelen, dan wel de doorlaatwaarde te beperken (bijv. tot nul ampère).

Leveranciers kunnen schakelopdrachten geven via de P4-poort, waarna de netbeheerder deze doorvoert. Afhankelijk van hoe leveranciers hun processen en systemen hebben ingericht kan een reëel risico op fouten of bewuste aanvallen bestaan.

Een gedetailleerde beoordeling van de beveiliging van de schakelfunctie is uitgevoerd in [16]. Hieronder worden enkele risico's benoemd.

4.4.1 Onterechte maar geautoriseerde afschakeling

(Requirements: R6, R14)
Een medewerker van de leverancier kan abusievelijk een onterechte (en wellicht intern ongeautoriseerde) afschakelopdracht geven. Hetzelfde kan gebeuren door een systeemfout in het leveranciersdomein. De kans hierop is beperkt en kan verder worden gereduceerd door technische of procedurele maatregelen.

Daarnaast bestaat de mogelijkheid dat een medewerker doelbewust afschakelopdrachten verstuurt. Vanwege de hoge potentiële impact zou de leverancier ook hiertegen maatregelen kunnen treffen (bijv. four-eyes principe, beperken aantal afschakelingen per tijdseenheid)

4.4.2 Afschakeling aansluiting van andere leverancier

(Requirements: R6, R13, R14)
Bij gebrekkige controle op de P4-poort bestaat de mogelijkheid dat een leverancier afschakelopdrachten (of aanschakelopdrachten) verstuurt naar een aansluiting die niet onder zijn eigen verantwoordelijkheid valt.

Wellicht is het mogelijk om eerst een (ongemandateerde) leverancierswitch door te voeren, waarna de leverancier vanuit het perspectief van de netbeheerder verantwoordelijk is geworden voor de aansluiting.

4.4.3 (Grootschalige) afschakeling door externe aanvallers

(Requirements: R6, R13, R14)
Vanwege de enorme potentiële impact die kan worden bereikt met grootschalige afschakelopdrachten, moet rekening worden gehouden met externe aanvallers zoals criminelen of terroristische organisaties met sterke motieven en voldoende middelen om een aanval goed voor te bereiden en uit te voeren. Het is belangrijk om te beseffen dat het hier een geheel ander type aanvalsvector betreft dan bij alle hiervoor genoemde risico's. Creatieve aanvallers moeten in staat worden geacht om zelfs goed beveiligde systemen succesvol aan te vallen. In hun aanpak kunnen de volgende elementen terugkomen:

- Zich toegang verschaffen tot de P4 en de daar toegepaste beveiligingsmaatregelen omzeilen;
- Zich toegang verschaffen tot systemen in het leveranciersdomein om van daaruit 'geautoriseerde' verzoeken naar de P4 te kunnen sturen.
- Social engineering technieken gebruiken om medewerkers van een leverancier te manipuleren tot het aansturen van de P4.

Zowel leveranciers als EDSN dienen sterke beveiligingsmaatregelen te nemen om de kans op zo'n aanval te minimaliseren, maar uit te sluiten is het niet.

4.4.4 Opdracht tot aanschakelen wordt niet doorgevoerd

(Requirements: R15)

Door een storing in de meter of elders in de meter keten wordt een aanschakelopdracht niet doorgevoerd. De kans hierop is beperkt, evenals de impact omdat de meter altijd via een handmatig proces alsnog kan worden aangeschakeld.

5 Discussie risico's

5.1 Analyse

5.1.1 Context van de slimme meter keten

Risico's worden bepaald door kans van optreden en potentiële negatieve impact. Hierbij moeten twee belangrijke factoren worden genoemd die kenmerkend zijn voor de context van de slimme meter keten:

Aan de impactzijde moet rekening worden gehouden met imagoschade. Dit betreft schade aan het vertrouwen in de slimme meter of zelfs schade aan het maatschappelijk draagvlak voor het onderliggende marktmodel. Deze vorm van impact treft partijen in het energiedomein en de overheid, en laat zich daarom moeilijk afwegen tegen de directe impact die specifieke aangeslotenen kunnen ondervinden van security- of privacy-incidenten. Wrang genoeg heeft deze mogelijke imagoschade ook gevolgen voor de waarschijnlijkheid van sommige typen incidenten, omdat beveiligingsonderzoekers en hackers er een uitdaging in zullen zien om kwetsbaarheden in de slimme meter keten aan te tonen. Denk bijvoorbeeld aan iemand die het marktmodel onderuit wil halen en zich meldt bij een P1 ODA onder een andere naam, om de hoogfrequente meetgegevens van een Bekende Nederlander op die manier naar zichzelf te laten sturen en daar tenslotte een sappig stuk over schrijft in de nationale pers.

Een omstandigheid die ook bijdraagt aan de waarschijnlijkheid van diverse typen risico's, is het feit dat de slimme meter keten nog in de fase van uitrol(-voorbereiding) verkeert. Hierdoor lopen uitwerking van de regels, nadere invulling en feitelijke implementatie nog door elkaar. Op basis van de voor dit onderzoek verkregen informatie lijken diverse aspecten van privacy- en security nog onvolledig uitgewerkt, vastgelegd en geïmplementeerd.

5.1.2 Risico's voor privacy van aangeslotenen

De *waarschijnlijkheid* dat privacy-incidenten zullen optreden moet als zeer hoog worden beoordeeld. Hierbij kan onderscheid worden gemaakt tussen de 'P1 keten' en de 'P3/P4 keten'.

In de P3/P4 keten wordt goede authenticatie toegepast zodat ongeautoriseerde partijen niet eenvoudig toegang kunnen krijgen tot de P4. Bij informatieverzoeken door leverancier/ODA lijkt echter onvoldoende getoetst te worden of de leverancier/ODA voor die specifieke informatie gemandateerd is. Heeft hij daadwerkelijk een overeenkomst met die aangeslotene? Vraagt hij de informatie op vanuit zijn leveranciersrol of vanuit zijn ODA-rol? Op dit moment hebben de aangeslotene (en de leverancier die verantwoordelijk is voor de meetgegevens) geen inzicht in gegevensverstrekking aan derden, echter de voorziene logfunctie op de meter kan hierin verandering brengen.

De P1 keten is minder gereguleerd. Echter: omdat een aangeslotene zijn ODA actief toegang moet verlenen tot de P1 zal dit steeds op basis van onderlinge overeenstemming gebeuren. Cruciaal hierbij is 'informed consent': weet de aangeslotene waarvoor hij toestemming geeft? Een reële kans bestaat dat de aangeslotene hierover verkeerde verwachtingen heeft, al dan niet doordat de ODA onvolledig of onduidelijk communiceert .

Mede omdat diverse aspecten van privacy- en security nog onvolledig uitgewerkt, vastgelegd en geïmplementeerd zijn binnen de slimme meter keten is er een groot risico op schending van het doelbindingsprincipe: spelers in de keten kunnen meetgegevens voor andere doeleinden gaan

gebruiken dan waarvoor de consument toestemming heeft gegeven (voorbeelden zijn marketing, surveillance).

Een ander waarschijnlijk type privacy-risico is het lekken van meet- of schakelgegevens uit de database van een leverancier of ODA door onvoldoende aandacht voor informatiebeveiliging. Dit geldt voor P4 ODA's, maar wellicht nog meer voor P1 ODA's die in veel gevallen hun meetgegevens via een publiek bereikbaar Internet-frontend zullen ontvangen.

De *impact* van privacy-incidenten voor aangeslotenen kan in bepaalde scenario's substantieel zijn. Vanwege de grotere actualiteit en granulariteit geldt dit in veel hogere mate voor P1 informatie dan voor P4 informatie, hoewel via de P4 grootschaliger misbruik mogelijk is (theoretisch toegang tot meet- en schakelgegevens van alle kleinverbruikers).

Naast directe impact voor de kleinverbruiker moet zeker ook rekening worden gehouden met imagoschade, zoals benoemd in 5.1.1.

Gezien bovenstaande beoordelen we het risico op misbruik van hoogfrequente meetgegevens uit de P1 als **zeer hoog** en het risico van ongeoorloofde toegang tot laagfrequente meetgegevens of schakelgegevens via de P4 als **gemiddeld**.

Leveranciers die een dubbelrol als ODA gaan vervullen kunnen misbruik maken van hun positie als leverancier, bijvoorbeeld door vanuit hun leveranciersrol uit te zoeken welke aansluitingen het meest in aanmerking komen voor een ODA aanbod. Dit kan concurrentievoordeel opleveren ten opzichte van andere ODA's en daarmee gevolgen hebben voor het gewenste level playing field dat in het nieuwe marktmodel beoogd wordt.

De kans hierop is hoog omdat de dubbelrol leverancier/ODA in de praktijk al voorkomt en het effectief inrichten van 'Chinese walls' in andere domeinen vaak moeilijk blijkt. Ook de impact is hoog omdat deze dreiging het draagvlak voor het marktmodel kan ondergraven. Daarom wordt het risico als **hoog** beoordeeld.

5.1.3 Risico's voor beschikbaarheid en integriteit meetgegevens

Bij informatieverzoeken via de P4 worden de gevraagde meetgegevens vanuit de meter opgehaald. De netbeheerder is dus afhankelijk van de meter voor het tijdig kunnen aanleveren van accurate meetgegevens.

De *waarschijnlijkheid* dat de meter (en dus de netbeheerder) op enig moment de gevraagde meetgegevens niet kan aanleveren of dat deze niet correct zijn kan binnen de scope van dit onderzoek niet beantwoord worden. Het voorkomen van technische fouten, fouten in het ijkingsproces en externe manipulatie van de meter is cruciaal.

Omdat de meter historische gegevens tot slechts 13 maanden terug bewaart zullen oudere meetgegevens door de netbeheerder nooit kunnen worden verstrekt aan de leverancier. Dit in tegenstelling tot de meetgegevens van traditionele meters waarvan jaarstanden worden opgeslagen in het meetregister.

Natuurlijk is het mogelijk dat meetgegevens na initiële levering via de P4 of P1 elders in de keten worden gecompromitteerd. Leveranciers en ODA's dienen hun beveiliging en IT-beheer zodanig in te richten dat de kans hierop beperkt wordt.

De *impact* van het tijdelijk niet beschikbaar zijn van meetgegevens is beperkt. De impact van niet-integere meetgegevens en incorrecte facturen kan potentieel zeer groot zijn. Zowel voor de kleinverbruiker, die de afwijking wellicht niet of pas na lange tijd constateert, als voor de leverancier en meter keten als geheel, die forse reputatieschade kunnen oplopen.

Voor zowel kleinverbruiker als leverancier is van belang dat geschillen, wanneer de gegevens van beiden niet overeenkomen, eenduidig kunnen worden beslecht. Omdat de meetgegevens niet centraal bij de netbeheerder worden opgeslagen is de meter de enige (onafhankelijke) backup waar op teruggevallen kan worden. Zeker in gevallen waarbij het dispuut wordt veroorzaakt door disfunctioneren van de meter zal dit onvoldoende zijn. Naar ons oordeel bestaat hierop een **gemiddeld** risico.

5.1.4 Risico's voor continuïteit elektriciteitsvoorziening

Afsluiting van huishoudens door onterechte schakelopdrachten kunnen binnen de scope van deze opdracht worden veroorzaakt door twee typen actoren:

- Medewerkers of systemen in het leveranciersdomein (opzettelijk, onopzettelijk of door systeemfouten)
- Externe aanvallers die zich toegang verschaffen tot de P4 of tot systemen of medewerkers in het leveranciersdomein. Hierbij kan het gaan om criminelen of terroristische organisaties met sterke motieven en voldoende middelen om een aanval goed voor te bereiden en uit te voeren.

Voor beide gevallen geldt dat de *waarschijnlijkheid* sterk afhankelijk is van de kwaliteit van beveiligingsmaatregelen door de leverancier (in techniek, proces en organisatie). Evenzeer geldt dat beide typen dreigingen niet volledig kunnen worden weggenomen.

Voor deze klasse van risico's is strikte kwaliteitsborging van access control tot de P4 nog essentiëler dan voor andere risico's. Het huidige authenticatiemechanisme biedt voldoende bescherming tegen de meeste aanvallers, maar wellicht niet tegen een vastberaden organisatie met terroristisch oogmerk. Naast authenticatie dienen ook autorisaties te worden beperkt en afgedwongen. Voorkomen moet bijvoorbeeld worden dat een leverancier schakelopdrachten geeft aan consumenten die geen klant van de leverancier zijn, door eerst een leverancierswitch uit te voeren en ze zo klant te maken. Op basis van de verkregen informatie is niet duidelijk in hoeverre zulke risico's zijn afgedekt.

Duidelijk is wel dat de *impact* van onterecht schakelen enorm kan zijn, zeker bij doelbewuste acties door externe aanvallers. EDSN of netbeheerders kunnen maatregelen nemen om de gevolgen te beperken, bijvoorbeeld het limiteren van het aantal schakelopdrachten per tijdseenheid. Echter, ook hier geldt dat een substantieel restrisico altijd blijft bestaan, zeker wanneer men zich moet wapenen tegen vastberaden aanvallers.

Gezien bovenstaande levert de aanwezigheid van een schakelaar die op afstand bediend kan worden een **zeer hoog** risico op.

5.2 Toezicht

Het verschil in toezicht en regulering rond verbruiksgegevens uit de "vrije" P1 poort en de "gereguleerde" P4 poort kan risico's met zich mee brengen voor de privacy van consumenten. Een advies aan de toezichthouders is dan ook om richtlijnen te formuleren voor de omgang met verbruiksgegevens door ODA's die rekening houden met de potentiële gevoeligheid van die gegevens voor de privacy van consumenten. Waar persoonsgegevens het "nieuwe goud" zijn, dient voor bedrijven die als ODA willen werken met verbruiksgegevens volledig duidelijk te zijn wat wel en wat niet mag. Daar bij de ODA gegevens uit de P1 poort (alleen toezicht door CBP) en de P4 poort

(tevens toezicht door NMa) samen komen, is het aan te raden voor CBP en NMa om dergelijke richtlijnen in samenwerking op te stellen om onduidelijkheden te voorkomen. Een startpunt voor deze richtlijnen kan zijn de requirements zoals deze in hoofdstuk 2 geformuleerd zijn. Speciale aandacht verdient daarbij de vraag of er adequate processen zijn ingericht door leveranciers en ODA's voor consumentenrechten zoals het inzage-, en correctierecht, en de afhandeling van geschillen met betrekking tot meetgegevens of facturen.

Een tweede advies voor toezicht, voornamelijk relevant voor de NMa, is om specifiek aandacht te schenken aan de kwaliteitsborging van access control op gegevens uit de P4 poort en op schakelacties via de P4 poort. Een aantal vragen die daarbij van belang zijn, en waar een duidelijk antwoord noodzakelijk is:

- Zijn er goede criteria voor toegang door ODA en leverancier tot de P4 poort geformuleerd? Behelzen deze zowel eisen aan technologie, als aan organisatie? Wordt het naleven van deze criteria daadwerkelijk gecontroleerd, en is de rolverdeling bij deze handhaving duidelijk?
- Vinden bij ODA's en leveranciers security management audits plaats? Vinden er technische security audits op ICT systemen plaats? Is er aandacht voor maatregelen om misbruik door medewerkers te voorkomen? (kans beperking)
- Zijn afdoende maatregelen getroffen om de impact van incidenten, met name rond de schakelfunctie, te beperken? Bijvoorbeeld: een maximum aan een aantal afsluitingen per tijdseenheid. (impact beperking)
- Via welk proces wordt afgedwongen dat ODA's alleen gegevens ontvangen van aangeslotenen door wie zij gemandateerd zijn? Hoe kan hierop controle plaatsvinden door de aangeslotene zelf of de leverancier die in het leveranciersmodel verantwoordelijk is voor de meetgegevens?

6 Conclusies en aanbevelingen

6.1 Bevindingen slimme meter keten

Allereerst is het van belang om de belangrijkste bevindingen samen te vatten omdat die voor een groot deel de context bepalen van de risico's.

- De uitwerking en de nadere invulling van het nieuwe marktmodel zijn nog in volle gang terwijl dit onderzoek loopt. Op basis van de voor dit onderzoek verkregen informatie lijken diverse aspecten van privacy- en security nog onvolledig uitgewerkt, vastgelegd en geïmplementeerd.
- Omdat de rol van overige diensten aanbieder (ODA) als een vrije marktrol wordt beschouwd, wordt deze in de geraadpleegde brondocumenten niet gedefinieerd of ingeperkt. Als gevolg hiervan ontbreekt wel een helder kader voor toetredingscriteria en toezicht op de ODA's.
- In de slimme meter keten zijn feitelijk verschillende categorieën van ODA's ontstaan met een eigen risicoprofiel:
  - Enerzijds is er een belangrijk onderscheid tussen een ODA die de P1 poort (hoogfrequente gegevens via de klant zelf) gebruikt en een ODA die de P4 poort (laagfrequente gegevens via Netbeheerder/EDSN) gebruikt.
  - Anderzijds blijken dubbelrollen frequent voor te komen. Er zijn een aantal ODA's die ook de rol van leverancier vervullen.
- In het leveranciersmodel heeft de consument alleen een relatie met leverancier en eventueel ODA. Juist de netbeheerder heeft echter een centrale rol bij de distributie van meetgegevens. Dit kan leiden tot verwarring bij de consument of kast-muur situaties, bijvoorbeeld als de netbeheerder ten onrechte meetgegevens verstrekt aan een ODA of andere leverancier.
- Oorspronkelijk was voorzien dat de meetgegevens van alle consumenten zouden worden opgeslagen in een centrale database onder beheer van de netbeheerder. Inmiddels is er voor gekozen om de gegevens bij de consument in de meters te laten zitten, waarbij slechts een beperkt aantal gegevens worden gecached in het netbeheerdersdomein. Vanuit securityperspectief heeft deze keuze voordelen, maar daar staat het nadeel tegenover dat de keten hierdoor nog meer afhankelijk is van het correct functioneren van de meter zelf.

6.2 Belangrijkste risico's

Rekening houdende met de hierboven genoemde observaties identificeert dit onderzoek een aantal belangrijke risico's van de slimme meter keten en het nieuwe marktmodel.

Bij het beoordelen van de impact van privacy- en securityrisico's moet rekening worden gehouden met mogelijke imagoschade. Die kan gevolgen hebben voor het vertrouwen in de slimme meter of zelfs voor het maatschappelijk draagvlak voor het onderliggende marktmodel.

- Het risico op verlies van vertrouwen van consumenten in de slimme meter of het marktmodel als gevolg van misbruik van hoogfrequente meetgegevens uit de P1 wordt als **zeer hoog** beoordeeld. Mogelijke scenario's zijn:
  - Derden verkrijgen toegang tot meetgegevens via slecht beveiligde systemen van de ODA;
  - Schending van het doelbindingsprincipe: meetgegevens worden verwerkt voor andere doelen dan waar de consument toestemming voor heeft gegeven;
  - Er is geen sprake van 'informed consent': de kleinverbruiker beseft niet hoe zijn P1-gegevens gebruikt zullen worden.

- Het risico van misbruik van de schakelfunctie wordt als **zeer hoog** ervaren vanwege de grote potentiële impact en het feit dat met geavanceerde externe aanvallers rekening moet worden gehouden.
- Een **hoog** risico bestaat dat leveranciers hun (informatie-)positie misbruiken ten behoeve van hun dubbelrol als ODA. Dit kan het level playing field bedreigen dat in het marktmodel wordt beoogd.
- Er bestaat een **gemiddeld** risico op ongeoorloofde toegang tot laagfrequente meetgegevens of schakelgegevens via de P4. De indruk bestaat dat authenticatie op de P4 goed geregeld is, maar dat daarnaast extra kwaliteitsborging nodig is:
  - Om vermenging van rollen (leverancier / ODA) te voorkomen
  - Om te borgen dat alleen gegevens van eigen klanten kunnen worden verkregen
  - Om te controleren dat een ODA daadwerkelijk door een aangeslotene is gemandateerd
- Een **gemiddeld** risico bestaat dat conflicten tussen aangeslotene en leverancier niet kan worden beslecht door het ontbreken van goede en neutrale backup voorzieningen

Naast deze genoemde risico's is nog een long-list aan (lagere) risico's benoemd in hoofdstuk 4.

6.3 Aanbevelingen

De onderzoeksopdracht beperkte zich tot het inventariseren van risico's. Niettemin wordt hieronder een aantal maatregelen genoemd die de gevonden risico's aanzienlijk kunnen verkleinen.

1. Richt toezicht in om te waarborgen dat meetgegevens en andere persoonsgegevens alleen op basis van 'informed consent' worden verwerkt:
   - De consument dient helder en eenduidig te worden geïnformeerd over welke gegevens zullen worden verwerkt en op welke wijze;
   - Gegevens die niet noodzakelijk zijn voor de basisdiensten energielevering en facturatie dienen slechts te worden verwerkt op basis van expliciete toestemming door de consument;
   - Persoonsgegevens dienen niet voor andere doeleinden dan waar de consument toestemming voor heeft gegeven gebruikt te worden.

2. Draag zorg voor voorlichting aan marktpartijen over welke bevoegdheden en verantwoordelijkheden zij vanuit hun rol hebben. Hierbij kunnen tenminste de volgende onderwerpen geadresseerd worden:
   - Welke gegevens mogen worden verwerkt, welke bewerkingen zijn toegestaan en welke voorwaarden gelden daarbij?
   - Aan welke beveiligingseisen dient invulling te worden gegeven? (eventueel met suggesties voor maatregelen).

3. Ga de dialoog aan met partijen in de meterketen om de in deze analyse benoemde risico's nader te onderzoeken en waar zinvol risicobeperkende maatregelen uit te werken. De volgende onderwerpen kunnen hierbij tenminste aan de orde kunnen worden gesteld:
   - Hoe kunnen de risico's verbonden met de schakelfunctie worden geadresseerd?
   - Hoe kan de kwaliteit van access control op de P4-poort worden geborgd? (bijvoorbeeld via regels voor EDSN en netbeheerder en eventueel een controlemechanisme op naleving);
   - Welke mechanismes kunnen worden ingericht om eventuele conflicten tussen consument en leverancier over de factuur te beslechten? (bijvoorbeeld: backup van jaar- of maandgegevens die via de P4 zijn opgevraagd).

Informatiebronnen

[1]	NMA, *Offerteaanvraag risicoanalyse privacy & security slimme meter*, 21 maart 2012 (kenmerk: 104114/1.B827)
[2]	TNO / LaQuSo / TILT, *Risicoanalyse Privacy & Security Slimme Meter*, offertenr TNO-OFF-DTS-2012-150747, 3 april 2012
[3]	*Wet van 2 juli 1998, houdende regels met betrekking tot de productie, het transport en de levering van elektriciteit* (Elektriciteitswet 1998)
[4]	Wijziging van de Wet houdende wijziging van de Elektriciteitswet 1998 en de Gaswet ter verbetering van de werking van de elektriciteits- en gasmarkt (Stb. 2011, 131)
[5]	NEDU, *Informatiecode Elektriciteit en Gas (Integrale versie)*, concept-versie verkregen via NMa, 13 april 2012
[6]	NMA, *Bijlage 1: Behorende bij het besluit nr. 103834 van de Raad van Bestuur van de Nederlandse Mededingingsautoriteit tot wijziging van diverse voorwaarden ex artikelen 27, eerste en tweede lid; 31, eerste lid van de E-wet* (Aanpassingen Meetcode Elektriciteit)
[7]	*Besluit van 27 oktober 2011, houdende regels over op afstand uitleesbare meetinrichtingen (Besluit op afstand uitleesbare meetinrichtingen)*, Stb. 2011, 511.
[8]	Energiekamer NMa, *Begrippenlijst Elektriciteit als bedoeld in de voorwaarden ex artikel 31, lid 1, sub a, b en c van de Elektriciteitswet 1998*, 12 mei 2012
[9]	Nederlands Elektrotechnisch Comite (NEC), *Basisfuncties voor de meetinrichting voor elektriciteit, gas en thermische energie voor kleinverbuikers*, Nederlandse Technische Afspraak NTA 8130, NEN, 2007.
[10]	EDSN, *Procedurebeschrijving Portal P4 Leveranciers en ODA's*, versie 1.4 (definitief), 7 juni 2012.
[11]	EDSN, *Detailprocesmodel (DPM) P4 (Centrale toegangsserver), "Stroomopwaarts" Gezamenlijk stapsgewijs naar een beter functionerend marktmodel voor kleinverbruik,* versie 3.0, 14 april 2011.
[12]	EDSN, *Business Requirements Specifications (BSR) P4,* versie 5.0 (vastgesteld door ALV NEDU), 25 mei 2011.
[13]	Sogeti, *Technisch Ontwerp Portal P4*, versie 1.1, Sogeti Nederland B.V, 2 september 2011.
[14]	EDSN, *Centrale Marktfacilitering Portal P4 – kaders en uitgangspunten*, versie 1.0, slides van presentatie, 27 januari 2011.
[15]	EDSN, *Doorlooptijden en rapportages P4*, versie 3.0, 25 mei 2011.
[16]	Baris Ege, Lejla Batina, Klaus Kursawe, Marko van Eekelen, Harold Weffers, *Risk review of the remote-off meter switch functionality in smart meters for Netbeheer Nederland by LaQuSo*, 31 mei 2012.
[18]	Task Force Smart Grids Expert Group 2, *Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety and Consumer Protection*, recommendation to the European Commission, 5 december 2011
[19]	Colette Cuijpers and Bert-Jaap Koops, *Smart metering and privacy in Europe: lessons from the Dutch case*, paper accepted for CPDP 2012.
[20]	Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet, and David Irwin Department of Computer Science University of Massachusetts Amherst, *Private Memoirs of a Smart Meter*, BuildSys 2010 2 november 2010, Zurich, Switzerland.

[21]	Greveler U./Justus, B./Löhr, D. Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“. Arbeitspapier – Technischer Report, Status: ENTWURF, Version 0.6. Fachhochschule Münster, 20. September 2011.
[22]	Het wetsvoorstel ‘slimme meters’: een privacytoets op basis van art. 8 EVRM. Colette Cuijpers en Bert-Jaap Koops, TILT. In opdracht van Consumentenbond, 2008.
[23]	Paul de Hert, Dariusz Kloza, *The challenges to privacy and data protection posed by smart grids. Europaische Projektkultur als Beitrag zur Rationalisierung des Rechts*, Tagungsband des 14. Internationalen Rechtsinfromatik Symposions IRIS 2011, pp. 191-196.
[25]	Colette Cuijpers, *Slim kiezen bij slimme meters*, Privacy & Informatie, 2011-3, p. 131-141.
[26]	Rainer Knyrim, Gerald Trieb, *Smart metering under EU Data Protection Law, International Data Privacy Law*, March 2011.
[27]	Elias Leake Quinn, *Smart Metering and Privacy: Existing Laws and Competing Policies*, beschikbaar via SSRN: http://ssrn.com/abstract=1462285 of http://dx.doi.org/10.2139/ssrn.1462285, 9 mei 2009
[28]	Elias Leake Quinn, *Privacy and the New Energy Infrastructure*, beschikbaar via SSRN: http://ssrn.com/abstract=1370731 of http://dx.doi.org/10.2139/ssrn.1370731, 15 februari 2009
[29]	Rebecca Herold, *Smart Grid Privacy Concerns*, NIST Smart grid Privacy Report first draft 2009.
[30]	Lockstep Consulting, 2011, PIA Report Advanced Metering Infrastructure (AMI)

Bijlage A – Begrippenlijst

Aansluiting: één of meer verbindingen tussen een net en een onroerende zaak.

Aansluitingenregister: een register, ingericht en beheerd door de netbeheerder voor de aansluitingen op zijn net, waarin per netaansluiting die gegevens zijn vastgelegd die nodig zijn voor de communicatie tussen netbeheerders en marktpartijen aangaande programma-verantwoordelijkheid, de facilitering van het switchproces en de productie van duurzame elektriciteit. EDSN noemt dit het Centrale Aansluitingen Register, afgekort C-AR.

Aanschakelen: beperkingen op de elektriciteitslevering van een aansluiting opheffen.

Afschakelen: de levering van stroom bij een aansluiting stopzetten of in vermogen beperken.

Actualiteit: de actualiteit van meetgegevens geeft aan hoe lang geleden de meting waarop de gegevens betrekking hebben verricht is.

Analoge meter: een (traditionele) niet op afstand uitleesbare of schakelbare meetinrichting, die dus niet voldoet aan het Besluit op afstand uitleesbare meetinrichtingen.

Granulariteit: de granulariteit (‘resolutie’) van meetgegevens geeft aan welk detailniveau de gegevens hebben, bijv. één meting per minuut (hoge granulariteit) of één meting per 2 maanden (lage granulariteit).

Impact: de (negatieve) gevolgen van het optreden van een risico.

Kleinverbruiker: aangeslotene met een kleinverbruikaansluiting.

Kleinverbruikaansluiting: een aansluiting met een capaciteit kleiner dan of gelijk aan 3x80 A op laagspanningsniveau.

Leverancier (LV): een organisatorische eenheid die zich bezighoudt met het leveren van elektriciteit.

Meetinrichting: het gehele samenstel van apparatuur dat ten minste tot doel heeft de uitgewisselde elektriciteit te meten. De meetinrichting bestaat uit 1 meetsysteem en meerdere meetinstrumenten.

Meetbedrijf: een organisatorische eenheid die zich bezighoudt met het collecteren, valideren en vaststellen van meetgegevens betreffende elektriciteit.

Meetgegevens: zie verbruiksgegevens

Meetverantwoordelijkheid: de verantwoordelijkheid van aangeslotenen voor het aanwezig zijn op de netaansluiting van een vereiste meetinrichting, alsmede voor het correct en tijdig (doen) vaststellen en (doen) doorgeven van de meetgegevens. De meetverantwoordelijke (MV) is of wordt aangewezen door de leverancier.

Meterbeheerder: een organisatorische eenheid die verantwoordelijk is voor ontwerp, plaatsing, beheer, onderhoud en verwijdering van de meetinrichting. Bij een kleinverbruikaansluiting is dit de netbeheerder.

Meterplaatser: een door een daartoe bevoegde instantie als erkende persoon, niet zijnde een netbeheerder, die op verzoek van een kleinverbruiker een meetinrichting plaatst bij een kleinverbruikaansluiting.

Meterregister: register met gegevens (EAN-code, meternummers, datum ingebruikname, etc…) van elke door een meetverantwoordelijke beheerde meetinrichting. Deze wordt bijgehouden door een meetverantwoordelijke.

Net: één of meer verbindingen voor het transport van elektriciteit en de daarmee verbonden transformator-, schakel-, verdeel- en onderstations en andere hulpmiddelen, behalve wanneer deze verbindingen en hulpmiddelen liggen binnen de installatie van een producent of van een afnemer.

Netbeheerder: een vennootschap die op basis van de wet aangewezen is voor het beheer van een of meer netten.

Programma-verantwoordelijkheid: de verantwoordelijkheid van afnemers om programma's met betrekking tot de productie, het transport en het verbruik van elektriciteit op te stellen. De programmaverantwoordelijke (PV) is vaak de leverancier, maar kleine leveranciers besteden dit soms uit.

Risico: een risico is, eenvoudig gezegd, de kans dat een incident optreedt, en de impact die het optreden van dit incident kan hebben.

Regionale netbeheerder (NB): een netbeheerder die is aangewezen voor het beheer van één of meer netten, anders dan het landelijk hoogspanningsnet.

Schakelgegevens: gegevens die in de slimme meter keten worden verwerkt ten behoeve van het op afstand aan/afschakelen van een aansluiting of het aanpassen van de doorlaatwaarde van een slimme meter.

Slimme meter: een op afstand uitleesbare en op afstand schakelbare meetinrichting, die voldoet aan het Besluit op afstand uitleesbare meetinrichtingen[7].

Stamgegevens: gegevens over een verbruiker die in het aansluitingenregister staan.

Verbruiker: een aangeslotene die elektrische energie afneemt van het net.

Verbruiksgegevens: meetgegevens die het verbruik van elektriciteit, gas, of andere zaken over een periode weergeven. Deze gegevens hebben een bepaalde granulariteit (detailniveau) en actualiteit.

Bijlage B – WBP toetsingskader

Het voert te ver om de Wbp hier in detail te bespreken. Verwezen wordt naar de *Handleiding Wet bescherming persoonsgegevens*.[11] Om toch enig inzicht te verschaffen in de achtergrond van de hieronder weergegeven requirements die voortvloeien uit de Wbp, wordt gewezen op de 8 OESO-privacybeginselen die de basis vormen van de Wbp.[12]

Deze in 1980 gepubliceerde privacybeginselen zijn te verdelen in twee groepen. Eerst vier beginselen die de voorwaarden betreffen waaronder persoonsgegevens mogen worden verwerkt: 1. Collection Limitation; 2. Data Quality; 3. Purpose Specification; and 4. Use Limitation. Daarna vier beginselen betreffende de verplichtingen van de voor de gegevensverwerking verantwoordelijken en de rechten van individuen: 5. Security Safeguards; 6. Openness; 7. Individual Participation; and 8. Accountability.

De eerste vier beginselen zijn met name in het tweede hoofdstuk van de Wbp vertaald in concrete vereisten waaraan de verwerking van persoonsgegevens moet voldoen. De kern wordt gevormd door het vereiste dat gegevensverwerking enkel is toegestaan op basis van een legitieme verwerkingsgrond en met het oog op een legitiem doel. Er mogen niet meer gegevens verzameld worden dan noodzakelijk is voor het doel, en de gegevens mogen niet voor een ander doel gebruikt worden. Met deze vereisten hangt de kwaliteit van de te verwerken gegevens nauw samen, waarbij het gaat om toereikende, ter zake dienende niet bovenmatige, juiste en nauwkeurige gegevens. In het tweede hoofdstuk van de Wbp is ook de beveiligingsplicht (security safeguards beginsel) verankerd.

Het beginsel van openness vind vooral zijn weerslag in de hoofdstukken 3, 4 en 5 van de Wbp betreffende gedragscodes, melding en voorafgaand toezicht, en informatie aan betrokkenen. Hoofdstuk 6 van de Wbp betreft de rechten van betrokkenen en geeft invulling aan het beginsel van individual participation. In hoofdstuk 2 is een algemene bepaling betreffende accountability opgenomen waarin de verantwoordelijke benoemd wordt als zorgdrager voor de naleving van de rechten en plichten uit de Wbp, waarbij deze zelfs verantwoordelijk is voor verwerkingshandelingen die een bewerker ten behoeve van de verantwoordelijke uitoefent. Verder liggen mechanismen voor accountability vooral besloten in de hoofdstukken 8, 9 en 10 van de Wbp betreffende rechtsbescherming, toezicht en sancties.[13]

De vereisten van de Wbp kunnen vertaald worden in een vragenlijst die als toetsingsinstrument gehanteerd kan worden. Wil een verantwoordelijke in overeenstemming met de Wbp handelen moeten deze vragen adequaat beantwoord kunnen worden (bewustzijn/verantwoording) en moet aan de vereisten die hieruit voortvloeien adequaat invulling zijn gegeven.(daadwerkelijke implementatie).

1) Worden persoonsgegevens verwerkt? Worden gevoelige gegevens verwerkt?

---

[11] Deze handleiding bevat naast inhoudelijke informatie tevens informatie over de wijze waarop de Wbp in de praktijk toegepast moet worden. De handleiding is beschikbaar via: http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html

[12] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, beschikbaar via: http://www.oecd.org/sti/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatabackground.htm

[13] De oplettende lezer mist de hoofdstukken 1(algemene bepalingen), 7 (uitzonderingen), 11 (gegevensverkeer met derde landen) en 12 (slotbepalingen) Wbp.

2) Wat is het doel van de verwerking van deze gegevens? Dit doel moet uitdrukkelijk en specifiek omschreven zijn. Voor elke afzonderlijke verwerking van gegevens moet het doel apart gespecificeerd zijn.
3) Hoe verschaft de verantwoordelijke welke informatie? Er bestaat een informatieplicht met betrekking tot de eigen organisatie alsmede over de verwerking van persoonsgegevens, inclusief het doel en de verwerkingsgrond, de wijze waarop rechten in dit verband door betrokkenen geëffectueerd kunnen worden en de wijze waarop aan bepaalde verplichtingen uit het recht op gegevensbescherming wordt voldaan. Kortom, alle informatie moet verschaft worden die noodzakelijk is om een rechtmatige verwerking van persoonsgegevens te waarborgen.
4) Op basis van welke legitieme verwerkingsgrond(en) worden de gegevens verwerkt?
    a) In het kader van de levering van de basisdienst zal de verwerking van gegevens gebaseerd kunnen worden op het leveringscontract, maar alleen voor zover de verwerking van de gegevens daadwerkelijk noodzakelijk is voor de uitvoering van het contract.
    b) Bij overige diensten zal de verwerkingsgrond toestemming van de kleinverbruiker moeten zijn.
    c) In het kader van de verwerking van gevoelige gegevens zal toestemming van de kleinverbruiker de verwerkingsgrond moeten zijn.
5) Hoe wordt invulling gegeven aan het rechtsgeldig verkrijgen van toestemming? Rechtsgeldige toestemming is een vrije, specifieke en op deugdelijke informatie berustende wilsuiting.
6) Hoe worden de rechten van betrokkenen geëerbiedigd? Dit betekent niet alleen op papier, maar ook vanuit organisatorisch en technisch oogpunt voorzien in deugdelijke procedures om rechten op inzage, correctie, afscherming en verzet te kunnen waarborgen.
7) Welke mechanismen zijn voorzien om te garanderen dat niet meer gegevens verwerkt worden dan noodzakelijk is met het oog op het doel? Welke waarborgen bestaan er om te voorkomen dat gegevens gebruikt worden voor een ander doel dan waarvoor zij verzameld zijn? Als data voor een ander doel gebruikt worden dan voor het oorspronkelijke doel, wie beoordeeld of er sprake is van verenigbaar gebruik?
8) Welke procedures zijn aanwezig om te garanderen dat de verwerkte gegevens accuraat, niet bovenmatig, actueel en relevant zijn met betrekking tot het doel van verwerking?
9) Hoe wordt gegarandeerd dat gegevens niet langer bewaard worden dan noodzakelijk is met het oog op het verwerkingsdoel? Zijn er bewaartermijnen gespecificeerd? Zijn er procedures om gegevens te verwijderen na verloop van de bewaartermijn? Wie is verantwoordelijk voor de uitvoering/naleving hiervan?
10) Welke beveiligingsmaatregelen zijn er genomen? Het gaat hier om zowel technische als organisatorische maatregelen die ongeautoriseerde en onrechtmatige verwerking van persoonsgegevens tegengaan, alsmede ongewenste schade (verlies, wijziging of vernietiging) aan gegevens. Zijn er procedures voor ´data recovery´?
11) Zijn er (technische/organisatorische) waarborgen/procedures aanwezig met het oog op geautoriseerde toegang en gebruik van gegevens?
12) Heeft de organisatie een privacy policy zodat medewerkers op de hoogte (kunnen) zijn van de wijze waarop binnen de organisatie met gegevens moet/mag worden omgegaan?
13) Indien gebruik wordt gemaakt van bewerkers, hoe/wie bepaald de keuze voor een bewerker? Op welke wijze wordt hierbij aandacht besteed aan het waarborgen van privacycompliance door de bewerker? Zijn er maatregelen/procedures om de naleving van de privacyregels door bewerkers te garanderen/controleren/af te dwingen?
14) Grensoverschrijdend gegevensverkeer lijkt niet noodzakelijk in relatie tot slimme energiemeting en moet voorkomen worden, welke mechanismen zijn hiervoor aanwezig? Indien de markt zich ontwikkelt en aanbieders wel grensoverschrijdend diensten gaan aanbieden hoe wordt dan voorzien in waarborgen dat gegevens enkel worden doorgegeven aan partijen die voorzien in een adequaat beschermingsniveau?

15) Is voldaan aan vereisten van melding bij het CBP of de functionaris gegevensbescherming of is sprake van toepasselijkheid van het Vrijstellingsbesluit Wbp?

De requirements die voortvloeien uit de Wbp kunnen als volgt kort worden weergegeven:

- Uitdrukkelijke, specifieke gedocumenteerde doelspecificatie: welke gegevens worden verwerkt voor welk doel.
- Er dient invulling te worden geven aan de informatieplichten.[14]
- De verwerkingsgrond dient uitdrukkelijk te worden vastgesteld.
- Invulling moet worden gegeven aan hoe toestemming verkregen, beheerd en ingetrokken wordt.
- Invulling moet worden gegeven aan het inzage-, correctie-, verwijder-, en verzetsrecht van betrokkenen.
- Invulling moet worden gegeven aan garanties/waarborgen betreffende doelbinding.
- Invulling moet worden gegeven aan garanties/waarborgen met betrekking tot kwaliteit van gegevens.
- Invulling moet worden gegeven aan bewaartermijnen.
- Invulling moet worden gegeven aan het vereiste van adequate, kostenefficiënte beveiliging.
- Invulling moet worden gegeven aan een systeem van geautoriseerde toegang tot gegevens.
- Er dient een duidelijk privacy beleid voor medewerkers te worden opgesteld.
- Er dienen beleid, contracten en toezicht/handhavingmechanismen betreffende in te huren bewerkers worden opgesteld.
- Er moet invulling worden gegeven aan garanties/waarborgen om doorgifte van gegevens naar derde landen (buiten de EU) te voorkomen.
- Indien geen sprake is van vrijstelling op basis van het Vrijstellingsbesluit Wbp moet de gegevensverwerking gemeld worden bij de functionaris voor de gegevensbescherming of het CBP.

[14] Indien gesproken wordt van ´invulling geven aan´ wordt gedoeld op een uitdrukkelijke op schrift stelling van alle technische, organisatorische, procedurele en praktische aspecten van de daadwerkelijke implementatie van de betreffende requirement.

Bijlage C – Artikel 8 EVRM toetsingskader

De in dit rapport geïdentificeerde risico´s laten duidelijk zien dat slimme energiemeting de privacy van burgers raakt. Daarom is het overkoepelende recht op privacy, verankerd in art. 8 EVRM, van toepassing. Hoewel dit recht van toepassing is op verticale verhoudingen, is door de Hoge Raad erkend dat dit recht doorwerkt in horizontale verhoudingen.[15] In tegenstelling tot de Wbp ziet niet primair het CBP toe op de naleving van artikel 8 EVRM. Indien inbreuken andere dan de informationele privacy dimensie raken, zoals bijvoorbeeld het huisrecht of de relationele privacy, dan kan dit vallen binnen het toezichtsdomein van de NMa. Echter, een toets van de NMa zal zich niet specifiek richten op de requirements die voortvloeien uit art. 8 EVRM, maar op de vraag of de schending van privacy gevolgen heeft voor marktwerking en/of consumentenbescherming. Een onderdeel van artikel 8 EVRM betreft een toets aan de beginselen van proportionaliteit en subsidiariteit, beginselen die niet specifiek zijn voor het privacyrecht maar op tal van juridische terreinen een belangrijk afwegingskader vormen.

Voor meetinrichtingen met de eerder genoemde functionaliteit van uitleesbaarheid en schakelen op afstand, heeft een eerdere privacytoets uitgewezen dat, voor zover deze functies puur worden aangewend met het oog op de basisdienst energielevering en het noodzakelijk beheer van het netwerk – en niet meer gegevens verwerkt worden dan noodzakelijk is met het oog op deze doeleinden – er sprake is van overeenstemming met art. 8 EVRM [22]. Hiertoe zijn gedurende het wetgevingsproces enkele aanpassingen gemaakt ten einde een meer privacyvriendelijke meterketen te waarborgen, zoals beschreven in paragraaf 2.2.3. Dit neemt niet weg dat in de toekomst de meter voor andere doeleinden gebruikt kan worden of dat er nieuwe of andere functionaliteiten aan de meter worden toegevoegd. Ook de waarborgen en garanties die de slimme energieketen omgeven kunnen in de toekomst wijzigen. In een dergelijke situatie zal de privacytoets voor wat betreft de wijzigingen opnieuw uitgevoerd moeten worden. Als we kijken naar die situaties waarin andere doeleinden of functionaliteiten een rol spelen, volgt uit het wettelijk kader dat hier in principe altijd toestemming van de kleinverbruiker voor nodig is. Vanuit privacyperspectief staat dan al snel de informationele privacydimensie centraal, ofwel de vraag of op rechtmatige wijze met persoonsgegevens wordt omgegaan. Door het geven van toestemming rechtvaardigen kleinverbruikers immers zelf een mogelijke inbreuk op de privacy die toegevoegde waardediensten met zich kunnen brengen. Zoals hierboven aangegeven valt het toezicht op de naleving van de Wbp primair in het domein van het CBP. Gezien het voorgaande zijn ook de requirements voortvloeiend uit art. 8 EVRM weergegeven in een Bijlage. In paragraaf 2.3 zijn alleen die requirements benoemd die volgen uit zowel het privacy- en persoonsgegevenskader als uit andere wettelijke kaders voor zover deze vallen binnen het toezichtsdomein van de NMa. Voor de volledigheid wordt hier het gehele toetsingskader van art. 8 EVRM weergegeven.

Artikel 8 EVRM luidt:
1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

[15] Arrest Edamse Bijstandmoeder, HR 9 januari 1987, NJ 1987/928.

Uit deze wetsbepaling volgen onderstaande vragen op grond waarvan toelaatbaarheid van een privacyinbreuk getoetst moet worden:

1. Is het recht op privacy aan de orde?
2. Is er een wettelijke basis die voor de burger voldoende inzichtelijk maakt of en hoe zijn privacy kan worden geraakt?
   De implementatie van slimme meters is op Europees niveau voorzien in Richtlijn 2009/72/EC en in Nederland in de Elektriciteitswet en Gaswet en onderliggende regelingen. Er is dus een wettelijke grondslag. Daarbij geldt als eis dat de wettelijke regeling ook voldoende kwalitatief moet zijn, dat wil zeggen voldoende gedetailleerd zodat de burger weet wat hij kan verwachten in relatie tot zijn privacy.
3. Is er sprake van één van de in artikel 8 lid 2 genoemde belangen?
   Voor slimme energiemeting in zijn algemeenheid kan gesteld worden dat dit ziet op belangen als economisch welzijn en mogelijk ook nationale veiligheid en gezondheid.
4. Is er sprake van een noodzaak in een democratische samenleving?
   Dit komt neer op een proportionaliteits- en subsidiariteitstoets. Het uitlezen of schakelen van energiemeters raakt de privacy van kleinverbruikers; dat is gerechtvaardigd als het doel van het uitlezen of schakelen niet met andere middelen kan worden bereikt die de privacy minder raken. Het gaat dus om maatwerk. In de keten betekent dit bijvoorbeeld dat meetgegevens niet verder moeten worden verspreid dan noodzakelijk is voor het doel van de slimme energiemeting.

Hieruit kunnen de volgende requirements gedestilleerd worden:

- De wettelijke basis op grond waarvan een privacyinbreuk plaatsvindt dient duidelijk kenbaar te zijn voor kleinverbruikers.
- Degene die inbreuk op privacy maakt moet kunnen onderbouwen waarom deze inbreuk noodzakelijk is in een democratische samenleving.
- Er dient te worden beargumenteerd dat het doel met het gekozen middel bereikt kan worden.
- Er dient te worden beargumenteerd dat er geen minder ingrijpende alternatieven zijn die het doel kunnen bereiken.[16]

[16] Dit kan sterk samenhangen met de specificaties van het systeem, bijvoorbeeld de vraag of het voor de basis energielevering wel noodzakelijk is om zeer frequent energiestanden uit te lezen, zie in dit verband [11, 14 en 18].