Privacy en Security slimme-meterinfrastructuur

Hoofddocument

Werkgroep Privacy & Security
pgUSM, Technology Center
Arnhem, 17 september 2010
Versie 1.50 NL

netbeheer nederland

Versiebeheer en auteurs

Versie	Status	Belangrijkste wijzigingen	Auteurs
0.1	Concept	Overzetten maatregelen uit Excel lijst	IvV
0.2	Concept	Uniformeren documenten	SvB
0.3	Concept	Maatregelen GPRS en PLC verplaatst	IvV
0.8	Concept	Review en uniforme opmaak	IV
0.92	Concept	Consensus werkgroep	BvD, IvV, IV
0.980	Final Draft	Verwerken feedback interviews	IvV
0.986	Final Draft	Update van inleidende hoofdstukken	PM, BvD
0.99	Final review	Feedback netbeheerders verwerkt	Werkgroep P&S
1.0	Eerste versie	Ter goedkeuring pgUSM	Werkgroep P&S
1.30	Reviewversie	Explicatie link risico's, eisen en maatregelen; stakeholderanalyse toegevoegd. Ter review externe experts	Werkgroep P&S
1.37	Concept	Reviews TNO en RUN verwerkt	Werkgroep P&S
1.40	Reviewversie	Woordenlijst niet meer apart	JR, BvD
1.48	Final Draft	Reviews netbeheerders verwerkt	Werkgroep P&S
1.490	Final Draft	Voorgelegd aan stuurgroep-TC 18/5	Werkgroep P&S
1.499	Final	Voorgelegd aan MT's slimme meters	Werkgroep P&S
1.50	Final	(geen)	Werkgroep P&S

Distributie

Versie	Aan	Uitgave	Medium
0.1	Werkgroep Privacy en Security		
0.8	Werkgroep Privacy en Security	29-5-09	e-mail
0.91	Werkgroep Privacy en Security en pgUSM	12-6-09	e-mail
0.92	Werkgroep Privacy en Security	16-6-09	e-mail
0.980	Werkgroep Privacy en Security	21-7-09	e-mail
0.986	Netbeheerders, werkgroepen pgUSM	29-7-09	e-mail
0.99	Netbeheerders, werkgroepen pgUSM	24-8-09	e-mail
1.0	pgUSM	8-9-09	e-mail
1.30	Netbeheerders, PWC, TNO, Radboud Universiteit (RUN)	14-12-09	e-mail
1.37	Werkgroep Privacy en Security	1-3-10	e-mail
1.40	Netbeheerders, deelnemers ronde tafel, overige reviewers	3-3-10	geprint
1.48	Werkgroep, MT Slimme Meter bij netbeheerders	13-5-10	e-mail
1.490	Werkgroep, struugroep-TC	18-5-10	e-mail
1.499	Werkgroep, struugroep-TC, MT's slimme meters, pgUSM, Ledenraad Netbeheer Nederland	9-6-10	e-mail
1.50	Publicatie	17-9-10	Web

Samenstelling van de werkgroep

Versies	Naam	Organisatie	Rol	Initialen
0.1 tot 1.0	Bram Reinders	Alliander	Trekker	BR
	Anne Spoelstra	Eneco	Lid	AS
	Bram van Driel	Enexis	Lid	BvD
	Erwin Kooi	Alliander	Lid	EK
	Ivo van Vessem	Enexis	Lid	IvV
	Pieter Meijers	Kleine netbeheerders	Lid	PM
	Stefan van den Broek	Alliander	Support	SvdB
	Tom Vermeulen	Delta	Lid	TV
1.0 tot 1.5	Bram Reinders	Alliander	Trekker	BR
	Anne Spoelstra	Stedin (Eneco)	Lid	AS
	Boas Bierings	Enexis	Lid	BB
	Johan Rambi	Alliander	Lid	JR
	Marjolein Mulder	Stedin (per 1 mei 2010)	Lid	MM
	Tom Vermeulen	Delta Netwerkbedrijf	Lid	TV
	Bram van Driel	Netbeheer Nederland	Support	BvD
	Danielle Goudswaard	PWC	Expert	DG

netbeheer nederland

Inhoudsopgave

1. Inleiding

De komende jaren staat de Nederlandse energie-infrastructuur voor een groot aantal veranderingen, waaronder de inrichting van een slimme-meterinfrastructuur voor kleinverbruikmeters. Recente debatten in de Eerste Kamer hebben duidelijk gemaakt dat de Nederlandse samenleving veel belang hecht aan privacybescherming bij slimme meters. Netbeheerders hebben er belang bij om risico's met betrekking tot privacy en security sectorbreed en adequaat af te dekken.

Potentiële incidenten op het gebied van privacy en security zullen impact hebben op alle netbeheerders en hun klanten, en niet enkel op de netbeheerder waar het incident zich voordoet. Netbeheer Nederland heeft daarom besloten een gezamenlijk beleid op te stellen waaraan alle netbeheerders moeten voldoen. Hiertoe is de landelijke werkgroep 'Privacy en Security slimme meters' opgericht, die belast is met het ontwikkelen van eisen voor het beheersen van privacy- en securityrisico's rond slimme meters.

De landelijke werkgroep is opgericht met de volgende doelstelling[1]: het ontwikkelen van gezamenlijke standpunten en aanbevelingen op het gebied van informatiebeveiliging die door alle aangesloten regionale netbeheerders worden gedragen. De werkgroep richt zich daarbij op de totale keten voor de aanschaf, installatie, operatie, onderhoud en verwijdering van de slimme meter.

In dit document definieert de werkgroep Privacy en Security namens Netbeheer Nederland het beveiligingsraamwerk dat als fundament dient voor de slimme-meterinfrastructuur. Dit fundament moet het mogelijk maken om de beschikbaarheid, integriteit en vertrouwelijkheid van in de keten voorkomende informatie te waarborgen en eventuele schade door beveiligingsincidenten te minimaliseren. De werkgroep Privacy en Security definieert hiermee het informatiebeveiligingsbeleid voor de slimme-meterinfrastructuur. Dit beleid biedt kaders voor iedere netbeheerder om de beveiligingseisen en maatregelen te implementeren. De netbeheerder geeft zelf een tijdschema aan wanneer aan de beveiligingseisen en maatregelen wordt voldaan.

[1] Bron: ProjectInitiatieDocument werkgroep Privacy en Security, oktober 2008

2. Uitgangspunten

Europese context

Uitgangspunten en verwachtingen ten aanzien van de invoering van slimme meters (vrij naar de Europese richtlijn 2006/32/EG):

- Vanuit de samenleving en politiek is er behoefte aan meer energie-efficiëntie bij eindgebruik, onder andere om afhankelijkheid van (ingevoerde) fossiele energiebronnen terug te dringen, emissie van broeikasgassen te reduceren en innovatie- en concurrentievermogen te vergroten.
- Om eindgebruikers in staat te stellen met kennis van zaken beslissingen te nemen over hun verbruik is het verstrekken van informatie over energieverbruik en energiebesparingmogelijkheden noodzakelijk. Bovendien is het gewenst dat marktpartijen eindafnemers kunnen adviseren en informeren over energiebesparing op basis van kwalitatief goede en gedetailleerde verbruiksinformatie.
- Energiemeters voor elektriciteit, gas, water, warmte en koeling die het energieverbruik van eindafnemers nauwkeurig registreren en beschikbaar stellen (‘slimme meters’) zijn een goed middel om eindgebruikers te informeren en te stimuleren energie te besparen en om marktpartijen die energiebesparingdiensten aanbieden van informatie te voorzien.

Nederlandse situatie

Uitgangspunten ten aanzien van de Nederlandse situatie zijn de volgende:

- In Nederland zijn netbeheerders belast met het plaatsen en uitlezen van slimme meters en met het aanbieden van diensten die samenhangen met marktfacilitering. De daarvoor ontworpen slimme-meterinfrastructuur is vastgelegd in de NTA 8130 van het Nederlands Normalisatie Instituut (NEN).
- Vanwege de extra informatie- en communicatietechnologie die aan meters wordt toegevoegd ten opzichte van de ouderwetse ‘domme’ meter worden nieuwe risico’s ten aanzien van privacy en informatiebeveiliging geïntroduceerd. Het is aan de netbeheerders deze risico’s beheersbaar te maken.
- Netbeheer Nederland stelt voor haar leden privacy- en securityrichtlijnen met betrekking tot de slimme-meterinfrastructuur op. De ambitie is om met deze richtlijnen (1) het betrouwbaar functioneren van de slimme-meterinfrastructuur te waarborgen en (2) de privacy van de klanten met een slimme meter te beschermen en te voldoen aan de wettelijke eisen met betrekking tot de bescherming van de persoonsgegevens (WBP).
- Netbeheerders dragen gemeenschappelijk zorg voor een veilige slimme-meterinfrastructuur en streven naar een eenduidig en kwalitatief hoog beveiligingsniveau binnen hun invloedsfeer.

Informatiearchitectuur

In de NTA 8130 is de informatiearchitectuur van de Nederlandse slimme-meterinfrastructuur vastgelegd. Deze is verder uitgewerkt in de ‘Dutch Smart Metering Requirements’ (DSMR). Hoewel beide documenten aan verandering onderhavig zijn, gaan we in deze documenten uit van de architectuur zoals die nu is gedefinieerd (februari 2010).

3. Scope

Privacybescherming en informatiebeveiliging zijn geen los van elkaar staande activiteiten. Er bestaat tussen beide begrippen overlap; informatiebeveiliging is bijvoorbeeld nodig om privacy te kunnen beschermen. Het verschil zit in de scope:

- Informatiebeveiliging is breder dan privacybescherming als het gaat om de scope van maatregelen. Naast maatregelen gericht op bescherming van persoonsgegevens zijn informatiebeveiligingsmaatregelen ook gericht op de beveiliging van andere informatietypen
- Privacybescherming is breder dan informatiebeveiliging als het gaat om de te bereiken doelstellingen. Naast het waarborgen van de betrouwbaarheid van persoonsgegevens, gaat het ook om het beschermen van persoonsgegevens tegen enige vorm van onrechtmatige verwerking en onnodige verdere verwerking van persoonsgegevens. Daarnaast moet worden voldaan aan wettelijke eisen met betrekking tot de bescherming van de persoonsgegevens.

Binnen scope vallen privacy- en security-aspecten die betrekking hebben op het deel van de slimme meterinfrastructuur waarvoor de netbeheerder verantwoordelijk is.

3.1 Afbakening verantwoordelijkheden en organisatie

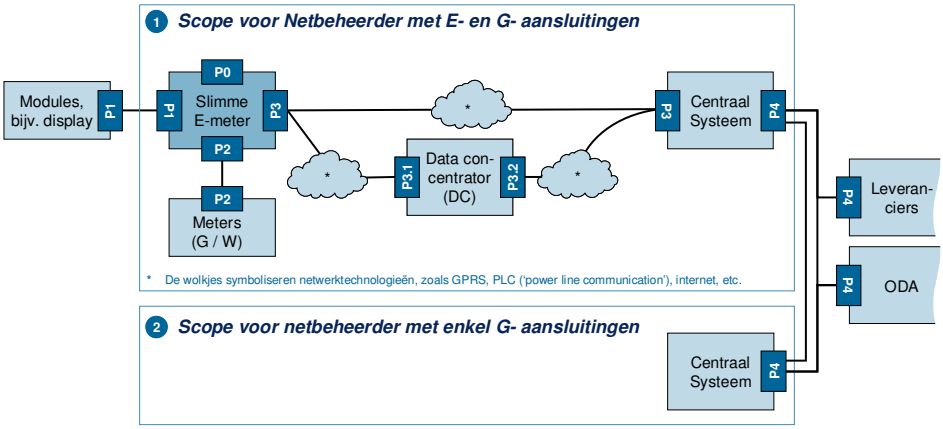
Organisatorische aspecten van het inrichten en beheren van de slimme-meterinfrastructuur binnen netbeheerders zijn in scope. Netbeheerders kunnen niet of slechts in zeer beperkte mate dwingende eisen opstellen aan partijen buiten hun invloedssfeer, zoals energieleveranciers, ODA's en EDSN.

De werkgroep Privacy en Security heeft de volgende veronderstellingen gedaan ten aanzien van de verantwoordelijkheden van bij de slimme-meterinfrastructuur betrokken organisaties:

- Netbeheerders zijn verantwoordelijk voor implementatie van eisen en maatregelen en onderhouden van een betrouwbare slimme meter infrastructuur.
- Netbeheer Nederland is, in opdracht van de netbeheerders, verantwoordelijk voor het ontwikkelen van beleid en ziet toe op correcte implementatie. Tevens richt Netbeheer Nederland een meldpunt in waar netbeheerders privacy- en security-incidenten melden.
- Energie Data Services Nederland B.V. (EDSN) is, in opdracht van de NEDU, verantwoordelijk voor het ontwerpen en specificeren van P4-berichtenverkeer en daarbij behorende procesmodellen. Daarmee is EDSN ook verantwoordelijk voor ontwikkelen van voor dit berichtenverkeer relevante privacy- en security-eisen.

3.2 Scope van techniek

In de huidige architectuur beheren netbeheerders de meeste functionaliteit in de slimme-meterinfrastructuur, waaronder de informatie- en communicatietechnologie op de slimme meter. Binnen scope vallen alle systemen en apparaten in de slimme-meterinfrastructuur vanaf de meter tot en met de P4-interface van netbeheerders. Deze definitie geldt voor alle netbeheerders. De situatie voor netbeheerders met enkel gasaansluitingen verschilt in die zin van de overige netbeheerders dat zij enkel een Centraal Systeem (CS) onderhouden, dat via P4 gevoed wordt vanuit andere Centrale Systemen (Zie figuur 1).



Figuur 1: scope van eisen en maatregelen met betrekking tot slimme meter techniek

3.3 Scope van informatietypen

De volgende tabel geeft een overzicht van doelen van slimme meters en (globaal) de informatie welke daartoe verzonden wordt tussen partijen en/of apparaten. Deze informatie wordt nu of mogelijk in de toekomst in de slimme-meterinfrastructuur gebruikt door klanten, netbeheerders, leveranciers of derden (via de P4-poort):

Doelstelling	Taak	Benodigde data	Van	Naar	Frequentie	Gebruik
Beheer van net	Instellen doorlaatwaardes	Besturingsopdrachten	Netbeheerder	Meter	~ 1 / jaar	toekomst
	Monitoren netkwaliteit, lokaliseren storingen	Monitoringinformatie[1]	Meter	Netbeheerder	Dagelijks	toekomst
	Uitkeren bij storingen	Monitoringinfo[1] (last gasp)			Na storing	toekomst
	Leveringszekerheid bij calamiteiten (code rood)	Afschakelcommando	Tennet (LNB)	Meter	< 1 / jaar	toekomst
Beheer van meters	Bij plaatsing testen of meters goed functioneren	Intervalstanden, ...	Meter	Netbeheerder	1 x 5 dagen	nu
	Monitoren kwaliteit meters, detecteren storingen	Monitoringinformatie[1]	Meter	Netbeheerder	Dagelijks	nu
	Verbeteren meterfunctionaliteit, beveiliging, …	Firmwareupdate	Netbeheerder	Meter	< 1 / jaar	nu
	Tijdafhankelijke functionaliteit mogelijk maken	Tijdinstellingen	Netbeheerder	Meter	Dagelijks	nu
Marktfacilitering, waaronder mogelijk maken van variabele tarifering (VT)	Jaarlijks factureren (op een maandeinde)	Verbruik (stand)	Meter	Leverancier	Jaarlijks	nu
	Factureren bij verhuizen, switchen of opzeggen	Dagstand (op aanvraag)		Leverancier(s)	< 1 / jaar	nu
	VT, optie 1: Instellen tarief op meter (hoog/laag)	Tariefschema	Leverancier	Klant	~ 1 / jaar	toekomst
	VT, optie 2: Afrekenen o.b.v. intervalstanden	Intervalstanden	Klant	Leveranciers	Wekelijks	toekomst
	Informeren klant	Tekstberichten	Leverancier	Klant	Wekelijks	toekomst
Beperking net-verlies, fraudebe-strijding, aanpak wanbetalers	Inschakelen bij nieuw contract (start levering)	Inschakelcommando	Leverancier	Klant	< 1 / jaar	nu
	Afschakelen bij einde contract of wanbetaling	Afschakelcommando	Leverancier		< 1 / jaar	nu
	Detecteren van fraude en 'events' (als kap los)	Monitoringinformatie[1]	Meter	Netbeheerder	Dagelijks	toekomst
Stimulering van energiebesparing	Inzicht geven in actueel verbruik	Actueel verbruik	Meter	Klant	Continu	nu
	Ondersteunen bij verbruiksanalyse en besparen (op verzoek klant, b.v. via website)	Intervalstanden	Meter	Leverancier of ODA	Wekelijks	toekomst
	Zes maal per jaar verbruik terugkoppelen	Verbruik (stand)	Meter	Leverancier	6 / jaar	toekomst
Facilitering van energietransitie	Nog niet bekend wat nodig is voor 'smart grids', decentrale opwek en faciliteren energietransitie	?	?	?	?	toekomst
Allocatie / reconciliatie	Was en is geen doel van slimme meter	Uurstanden	?	?	?	toekomst

1: Onder monitoringinformatie wordt onder andere verstaan: spanning en spanningsonder-breking ('last gasp'), stroomsterkte, cos phi en varh (voor E); druk, temperatuur, flow en stand gasklep (voor G); kwaliteitsrapportages

Mogelijk zijn er nog andere informatietypen die door slimme meters opgehaald of verwerkt kunnen worden. Bovendien kunnen toekomstige slimme meters ook nieuwe functionaliteit, zoals voor smart grids, bevatten. Indien hier gerechtvaardigde doelen voor bestaan, moeten deze doelen en de bijbehorende informatiestromen worden toegevoegd aan deze tabel.

Om eisen en richtlijnen enigszins onafhankelijk van de architectuur te kunnen formuleren, worden in dit document informatietypes in meer generieke termen benoemd, te weten:

- Privacygevoelige informatie, waaronder ten minste gerekend wordt:

  - Persoonsgegevens, zoals naam, geslacht, leeftijd, etc.;
  - Aansluitinformatie, waaronder adres, woonplaats, aansluittype en EAN-code, omdat deze informatie herleid kan worden naar een specifieke locatie en personen;
  - Verbruikgegevens ('meetdata') op het detailniveau van kwartier-, dag- of weekstanden, omdat deze informatie bevatten over de persoonlijke levenssfeer; en
  - Monitoringinformatie, mits deze dusdanige details bevat of met een zodanige frequentie verzonden wordt dat hieruit informatie over de persoonlijke levenssfeer af te leiden is;
- Schakelopdrachten, zijnde aan-, uit- of terugschakelopdrachten ('beperken' of 'knijpen'), waarmee levering op een specifieke aansluiting aangestuurd kan worden;
- Software, waaronder firmware op slimme meters, dataconcentrators, netwerkapparatuur, routers, en servers, waarmee onder andere de werking en mate van beveiliging van de slimme-meterinfrastructuur bepaald wordt;
- Sleutels en wachtwoorden, nodig om authenticiteit en vertrouwelijkheid van informatie te waarborgen en toegang te verkrijgen tot systemen of de inhoud van berichten;
- Apparaatinstellingen, waaronder firmwareconfiguraties en instelling van tijd- en volume-eenheden, welke onder andere bepalen hoe de meter informatie opslaat en verwerkt.
- Overige informatie op applicatieniveau, zoals niet-privacygevoelige monitoringinformatie, opdrachten om te controleren of de meter nog bereikt kan worden, tariefstructuren, registratie van speciale gebeurtenissen ('events'), etc.

Bovenstaande afbakening van wat privacygevoelige informatie betreft is gebaseerd op informatietypes welke nu in de slimme-meterinfrastructuur voorkomen. In meer generieke termen is de vuistregel toegepast dat alle data waaruit af te leiden is of iemand een week lang wel of niet thuis is geweest als privacygevoelig wordt beschouwd. Dit is uiteraard een nogal grove vuistregel; in specifieke gevallen zal de afweging telkens weer zorgvuldig (moeten) worden gemaakt.

3.4 Scope van Processen

De volgende processen die gerelateerd zijn aan het inrichten en beheren van de infrastructuur rondom slimme meters zijn in scope:

- Aanlevering (inkoop, testen, pre-commissioning, logistiek);
- Installatie;
- Asset management;
- Operatie (continu en ad hoc uitlezen, schakelen en doorlaatwaardes beperken, muteren, storingen en onderhoud);
- Deïnstallatie (en vernietiging);
- Systeembeheer (IT).

3.5 Beschikbaarheid, integriteit en vertrouwelijkheid van informatie

In algemene zin dienen de volgende drie aspecten beschermd te worden om de betrouwbaarheid van informatie te kunnen waarborgen:

- Beschikbaarheid ('availability'): geautoriseerde partijen kunnen op de juiste momenten tijdig beschikken over informatie en het informatieverwerkend systeem

- Integriteit (‘integrity’): correctheid en volledigheid van informatie en informatieverwerking, waarbij in het specifieke geval van meetstanden niet-weerlegbaarheid belangrijk is omdat op basis daarvan gefactureerd wordt.
  Niet-weerlegbaarheid (‘non-repudiation’) is de mogelijkheid voor derden om aan te kunnen tonen dat bepaalde gebeurtenissen hebben plaatsgevonden en daarmee samenhangende informatie van de juiste oorsprong en integer is.
- Vertrouwelijkheid (‘confidentiality’): informatie is alleen toegankelijk voor geautoriseerde partijen

Zowel bij de risicoanalyse als bij het opstellen van eisen en maatregelen heeft de werkgroep de nadruk gelegd op het beschermen van integriteit en vertrouwelijkheid van informatie. Beschikbaarheid van informatie raakt zowel aan beveiligingsrisico’s als aan algemene, operationele risico’s en is daarom niet altijd met eisen en maatregelen afgedekt:

- Daar waar beschikbaarheid van informatie direct te relateren is aan informatiebeveiliging zijn in deze documenten informatiebeveiligingseisen opgenomen, zoals tegen ‘Denial of Service-aanvallen’.
- Daar waar beschikbaarheid van informatie niet direct de privacy of het informatiebeveiligingsniveau aantast zijn geen eisen opgenomen, zoals tegen het niet tijdig beschikbaar zijn van meetdata door het verkeerd installeren van slimme meters. Het is om meer redenen dan enkel privacy en security in het belang van netbeheerders hier maatregelen op te treffen.

3.6 Buiten scope

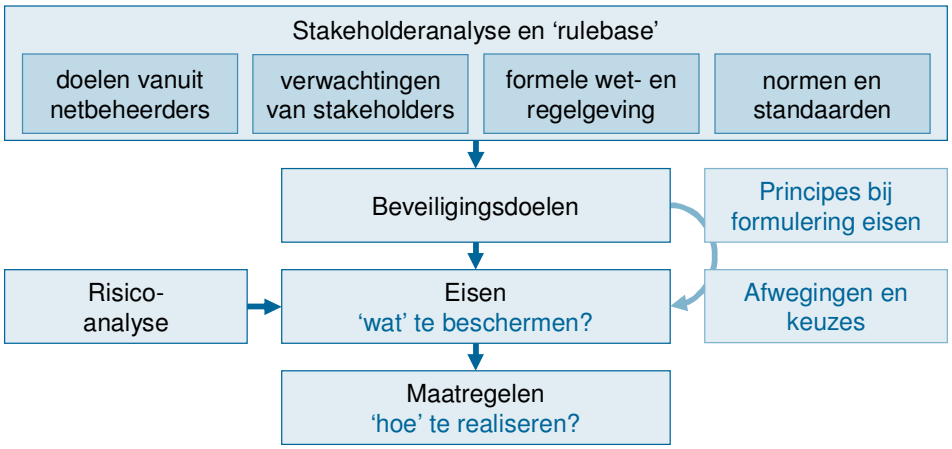
Slimme-metertechnologie zal zich in de toekomst blijven ontwikkelen. Deze documenten zijn daarom zoveel mogelijk generiek opgesteld, zodat ze ook op deze nieuwe ontwikkelingen van toepassing kunnen zijn. Desondanks is er een aantal technieken in ontwikkeling waarvan de werkgroep verwacht dat toepassing ervan specifieke aanpassing van de eisen en maatregelen noodzakelijk zal maken. De volgende ontwikkelingen zijn in deze versie expliciet buiten scope geplaatst:

- Smart grids – het is de verwachting dat lokale apparaten deze netwerken zullen aansturen, maar deze vallen niet onder de definitie van ‘data concentrators’;
- Geavanceerd netmanagement op basis van informatie over kleinverbruikaansluitingen
- Volgende generatie PLC-communicatie;
- Volgende generatie datacommunicatie;
- ‘Meshed-RF’ en (andere) ‘ad hoc’ netwerktechnieken;

4. Verantwoording en totstandkoming eisen en maatregelen

De werkgroep Privacy en Security heeft in een zorgvuldig proces een set van beveiligings-eisen en –maatregelen opgesteld welke een voldoende hoog beveiligingsniveau van de slimme-meterinfrastructuur mogelijk maken. Daarbij zijn de volgende stappen doorlopen:

- Uitvoeren stakeholderanalyse en bepalen 'rulebase';
- Vertalen van 'rulebase' naar een set van beveiligingsdoelen ('hoog-over' doelstellingen van het privacy- en securitybeleid);
- Uitvoeren van een risicoanalyse, identificatie van belangrijkste risico's, expliciet maken welke risico's geaccepteerd zijn en welke niet (kunnen) worden afgedekt;
- Formuleren van eisen (op tactisch niveau) en maatregelen (op operationeel niveau) op basis van af te dekken risico's en opgestelde beveiligingsdoelen.



Figuur 2: samenhang tussen de resultaten van verschillende stappen

Om te beoordelen of de opgestelde eisen en maatregelen inderdaad een 'voldoende hoog' niveau van privacybescherming en (informatie)beveiliging mogelijk maken zijn de stakeholderanalyse, beveiligingsdoelen, risicoanalyse, eisen en maatregelen ter beoordeling voorgelegd aan experts van binnen en buiten de energiesector. Resultaten van deze beoordelingen zijn in opeenvolgende versies van de genoemde documenten verwerkt door de werkgroep.

4.1 Samenvatting stakeholderanalyse en 'rule base'

In het bijlage document 'Netbeheer Nederland - stakeholderanalyse privacy en security slimme meters', versie 1.5, zijn stakeholders beschreven. Op basis daarvan is een overzicht van wetgeving, verplichtingen en enige andere eisen (waaronder normen, standaarden en verwachtingen van stakeholders) ten aanzien van privacy en security gedefinieerd, de 'rule base':

Ref.	Eisen en verwachtingen ('rule base')
R1 Formele wet- en regelgeving	
R1.1	Europese richtlijn 2006/32/EG Wetsvoorstel implementatie EG-Richtlijnen energie-efficiëntie (31320) Wetsvoorstel wijziging elektriciteitswet en gaswet (31374) ter verbetering van de werking van de elektriciteits- en gasmarkt Aanpassing op wetsvoorstel 31374 (Novelle)
R1.1.1	Informatieverzoek NMA
R1.1.2	Meetcode Elektriciteit, Voorwaarden als bedoeld in artikel 31, lid 1, sub b van de Elektriciteitswet 1998 – Zodra aangepast aan gewijzigde wetgeving.
R.1.1.3	Informatiecode Elektriciteit en Gas, Voorwaarden als bedoeld in artikel 31, eerste lid van de Elektriciteitswet 1998 en artikel 12b, eerste lid van de Gaswet – Zodra aangepast aan gewijzigde wetgeving
R1.2	Europees Verdrag Rechten van de Mens (artikel 8) Nederlandse Grondwet (artikel 10)
R1.3	Europese richtlijn 95/46/EG inzake het verwerken van / de bescherming van persoonsgegevens Wet bescherming persoonsgegevens, 2001
R.1.3.1	Raamwerk Privacy Audit, Samenwerkingsverband Audit Aanpak, Werkgroep Privacy Audit, April 2001
R.1.3.2	Beveiliging van persoonsgegevens, Achtergrondstudies en Verkenningen 23, Registratiekamer, Den Haag, april 2001
R.1.3.3	Contouren voor compliance, Handreiking bij het Raamwerk Privacy Audit, College bescherming persoonsgegevens i.s.m. Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) en Nederlandse Orde van Register EDP-Auditors (NOREA), 24 mei 2005
R.1.3.4	In toekomst: Richtsnoeren voor de beveiliging van persoonsgegevens
R1.4	In toekomst: door CBP goedgekeurde gedragscode van Netbeheer Nederland
R2 Standaarden en Best Practices	
R2.1	**Beveiligingsstandaarden**
R2.1.1	IEC/ISO 27000
R2.1.2	NEN-ISO/IEC 27001, Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging – Eisen (ISO/IEC 27001:2005, IDT) - Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005, IDT) ICS 35.040 november 2005.
R2.1.3	NEN-ISO/IEC 27002 - Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging (ISO/IEC 27002:2005, IDT) - Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005, IDT) (Vervangt NEN-ISO/IEC 17799:2005) ICS 35.040 november 2007.
R2.2	**Smart Metering Requirements**
R2.2.1	Nederlandse Technische Afspraak, NTA 8130, Basisfuncties voor de meetinrichting voorelektriciteit, gas en thermische energie voor kleinverbruikers. Minimum set of functions for metering of electricity, gas and thermal energy for domestic customers, ICS 17.120.10, augustus 2007.
R2.2.2	Dutch Smart Metering Requirements 2.2

Ref.	Eisen en verwachtingen ('rule base')
R.2.2.3	Dutch Smart Metering Requirements 3.0 (Nog in ontwikkeling)
R.2.2.4	DLMS / COSEM
R2.2.5	In toekomst: CWA about measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability
R3 Contracten en overeenkomsten, inclusief die met bewerkers in de zin van de WBP	
R3.1	Eisen gesteld aan dienstverleners welke optreden als bewerker in de zin van de Wbp.
R3.2	Eisen gesteld aan overige dienstverleners.
R3.3	Eisen gesteld aan overige business partners in het slimme meter netwerk / in de slimme-meterinfrastructuur.
R4 Verwachtingen en wensen	
R4.1	Passend beveiligingsniveau zoals gebruikelijk in de bancaire sector (Min EZ)
R4.2	Privacy thema uitwerken t.b.v. nuchtere discussie. (Min EZ)
R4.3	Externe uitingen van de netbeheerders m.b.t. doelstellingen en maatregelen inzake privacy en security in relatie tot slimme-meterinfrastructuur (denk hierbij aan brieven zoals verstuurd aan klanten, privacy statement op websites, etc.)
R4.4	Netbeheerders dienen PET (Privacy Enhancing Technologies) maatregelen te implementeren. (CBP)
R4.5	Netbeheerders moeten waar mogelijk dataminimalisatie toepassen (CBP)
R4.6	Geef consumenten zeggenschap over hun persoonsgegevens (CBP)
R4.7	Indien netbeheerders zelf bewerker zijn: periodieke toetsing van de door de verantwoordelijke opgelegde eisen door (of namens) de verantwoordelijke (WBP)
R4.8	Informeer klanten: - dat ze niet verplicht zijn een slimme meter in hun woning aan te laten brengen; - dat, als ze al een slimme meter hebben, zij niet verplicht zijn om deze op afstand uit te laten lezen (VEH).
R4.9	Realisatie en beheer van de slimme-meterinfrastructuur tegen maatschappelijk aanvaardbare kosten en financiële risico's

4.2 Beveiligingsdoelen

Op basis van de rule base zijn beveiligingsdoelen geformuleerd voor privacy- en security voor de slimme-meterinfrastructuur. Deze beveiligingsdoelen geven op het hoogste niveau aan wat het privacy- en securitybeleid binnen de slimme-meterinfrastructuur beoogt te realiseren. De beveiligingsdoelen zijn afgeleid van de stakeholderanalyse en de rule base; zie de referentie.

Referentie	Onderwerp	Id	Doel
R.1	Compliance	B1	Voldoen aan relevante wetgeving, wettelijke en regelgevende verplichtingen, contractuele verplichtingen en overige van toepassing zijnde eisen met betrekking tot privacy en informatiebeveiliging
R1.1; R.2.2	Leverings-zekerheid	B2	Ongestoorde dienstverlening, waaronder met name de levering van energie, en minimaliseren van het risico op ongeautoriseerd of onterecht schakelen
R.2; R.4.1; R.4.4; R.4.5; R.4.8	Beveiliging	B3	Beperking van toegang tot de logische en fysieke slimme-meterinfrastructuur tot bevoegden, voorkomen van toegang door onbevoegden, detecteren van en acteren op toegang door onbevoegden (waaronder fraudedetectie)
		B4	Richting geven aan beveiliging middels een actueel gedefinieerd, vastgesteld en geïmplementeerd beleid
		B5	Richting geven aan privacybescherming middels een actueel gedefinieerd, vastgesteld en geïmplementeerd beleid
R.1.1; R.2.1	Betrouwbaar-heid van informatie	B6	Waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van informatie in de slimme-meterinfrastructuur (waaronder meetgegevens)
R1.2; R1.3; R1.4; R.4.2; R.4.3; R.4.6; R.4.7; R.4.8	Privacy	B7	Respecteren en beschermen van de privacy van klanten, zorg dragen voor behoorlijke en zorgvuldige verwerking van persoonsgegevens
		B8	Medewerkers en relevante externe partijen bekend maken met het vastgestelde privacybeleid
R.3	Derden	B9	Beheersen van de dienstverlening en het beveiligingsni-veau van derden voor zover deze te maken hebben met (elementen in) de slimme-meterinfrastructuur.
	Inkoop	B10	Bij inkoop van slimme-metergerelateerde (informa-tie)systemen en diensten expliciet meenemen van normen en standaarden met betrekking tot privacybe-scherming en informatiebeveiliging
R.1.1; R.2; R.4.4;	Incidenten	B11	Tijdig detecteren en adequaat adresseren van privacy- en beveiligingsincidenten, zorg dragen voor adequate registratie, leren van incidenten

4.3 Identificatie belangrijkste risico's

Tijdens de risicoanalyse zijn, binnen de eerder genoemde scope, 62 risico's gedefinieerd met een significante waarschijnlijkheid en impact. Deze risico's zijn meegenomen bij het opstellen van de eisen en maatregelen. Drie van de 62 risico's zijn niet afgedekt, ofwel omdat deze minder waarschijnlijk bleken dan eerder ingeschat, of omdat afdekking niet mogelijk is. Alle risico's zijn beschreven in het document 'Netbeheer slimme meter risico-inventarisatie v1.5'.

Het verdient aanbeveling dit document te lezen alvorens de eisen en maatregelen door te nemen. Om relevantie en noodzaak van de opgestelde maatregelen te onderstrepen worden de belangrijkste risico's hier samengevat en genoemd:

- Slimme meters bevatten meterstanden, waaronder intervalstanden. Dit is privacygevoelige informatie welke bij slechte beveiliging van de meter kan leiden tot misbruik. Een voorbeeld van misbruik is het op basis van meetdata op afstand bepalen welke mensen op vakantie zijn, om vervolgens in hun woningen in te breken.
- Komende jaren zullen miljoenen slimme meters geplaatst worden met een beoogde levensduur van minimaal 15 jaar. De werkgroep heeft tijdens de analyse en bij het opstellen van eisen en maatregelen aangenomen dat gedurende die tijd ieder type slimme meter eens 'gehackt' zal worden, ongeacht hoe ingewikkeld of onwaarschijnlijk dat nu lijkt. Omdat fraude met meterstanden loont, zal een hack die gemakkelijk te kopiëren is, zich snel verspreiden. Het gevolg is dat meterstanden onbetrouwbaar worden.
- Onderdeel van de slimme-meterinfrastructuur zijn dataconcentrators die direct kunnen communiceren met slimme meters. Deze dataconcentrators staan door het hele land opgesteld en zijn benaderbaar, zowel fysiek als (bijvoorbeeld) via PLC. Als dataconcentrators in staat zijn schakelopdrachten te versturen, dan zouden enkele honderden huishoudens vanaf één 'gehackte' dataconcentrator afgeschakeld kunnen worden.
- Bij productie, installatie, onderhoud, deïnstallatie en vernietiging van slimme meters zijn veel partijen betrokken. Allen krijgen op verschillende manieren toegang tot delen van de slimme-meterinfrastructuur. Elk van hen kan potentieel schade veroorzaken, bijvoorbeeld door bij installatie de slimme meters verkeerd te configureren.

Deze risico's kunnen vrijwel allemaal resulteren in schade voor betrokkenen, zoals:

- klanten die onterecht afgeschakeld worden of in hun privacy geschonden worden;
- leveranciers die onjuist factureren; en
- netbeheerders en leveranciers die imagoschade leiden bij inbreuk op de privacy.

4.4 Rol netbeheerder in slimme-meterinfrastructuur

Recente en aanstaande wijziging van de energiewet leiden er toe dat de taken van netbeheerders op het gebied van meten worden uitgebreid. De netbeheerder wordt verantwoordelijk voor het realiseren van een infrastructuur voor het registreren, collecteren, transporteren en beschikbaar stellen van meetdata. Tevens verandert de rol van de netbeheerder in het zogenaamde 'nieuwe marktmodel' zo dat de netbeheerder in het facturatieproces geen waardeoordeel meer geeft over meterstanden. Deze taak verschuift van de netbeheerder naar de leverancier.

Netbeheerders zijn zich bewust van de bijzondere positie die zij in de wetgeving en in de huidige informatiearchitectuur innemen in de keten. Om verantwoording af te leggen en transparantie te creëren over deze rol zullen netbeheerders:

- een melding doen bij het CBP over verwerking van privacygevoelige gegevens;
- een voor de hele sector geldende privacygedragscode opstellen en deze van een instemmende verklaring laten voorzien door het College Bescherming Persoonsgegevens (CBP);
- transparantie over informatiebeveiliging in de tijd vergroten; en
- tijdens de proefperiode onderzoek doen naar fundamentele verbeteringen van de architectuur, zodat privacy- en securityincidenten in de toekomst minder waarschijnlijk of onmogelijk worden 'by design'

4.5 Principes bij het formuleren van eisen en maatregelen

De stakeholderanalyse, rule base, beveiligingsdoelen en risicoanalyse hebben als basis gediend voor het formuleren van eisen en maatregelen. Tijdens het formuleren van eisen en maatregelen is bovendien uitgegaan van de volgende principes:

- Hoe minder privacygevoelige informatie en kritieke systemen te beveiligen, hoe beter:
  - Informatie die niet nodig is, wordt niet gecommuniceerd
  - Informatie die niet nodig is, wordt niet opgeslagen
  - Informatie die niet langer nodig is, wordt gewist
  - Informatie wordt zoveel mogelijk opgeslagen op één plaats
- Beveiliging van informatie en systemen is 'gelaagd':
  - allereerst wordt het bemoeilijkt voor onbevoegden om bij informatie te komen ('afscherming')
  - lukt dit toch, dan wordt het bemoeilijkt om schade aan te richten ('beperking') of om informatie te interpreteren ('encryptie')
  - als er iets ongewenst gebeurt, gebeurt dat niet zonder dat de netbeheerder dat weet (detectie)
- De impact van incidenten wordt zoveel mogelijk ingeperkt:
  - wachtwoorden en beveiligingssleutels zijn per meter uniek
  - schakelen kan enkel met per meter unieke opdrachten
  - één persoon heeft nooit voldoende toegangsrechten om grote groepen meters of informatie over groepen klanten te kunnen benaderen
- Beveiliging is waar mogelijk centraal en door de netbeheerder te beheren:
  - beveiligingsfunctionaliteit moet 'geüpdate' kunnen worden
  - beveiliging van de infrastructuur berust niet op de beveiliging van elementen in de infrastructuur buiten de directe invloedssfeer van de netbeheerder

4.6 Toelichting op end-to-end encryptie

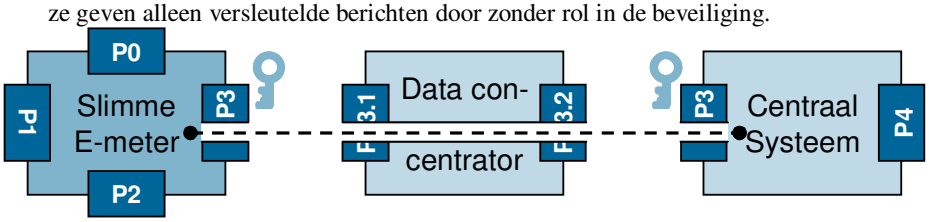
In de eisen en maatregelen heeft de werkgroep ervoor gekozen communicatie op applicatieniveau end-to-end te beveiligen, waarbij de eindpunten liggen in het centraal systeem (CS) en de elektriciteitsmeter. End-to-end-beveiliging, waaronder encryptie, is een vertaling van de volgende uitgangspunten:

- Beveiliging van de infrastructuur berust niet op de beveiliging van elementen in de infrastructuur buiten de directe invloedssfeer van de netbeheerder

- Het wordt bemoeilijkt voor onbevoegden om bij informatie te komen of om berichten te verzenden
- Indien dit toch lukt, dan wordt het bemoeilijkt om schade aan te richten of om informatie te interpreteren
- Eén enkele persoon heeft nooit voldoende toegangsrechten om grote groepen meters of informatie over groepen klanten te kunnen benaderen

End-to-end encryptie van privacygevoelige communicatie tussen het CS en E-meter

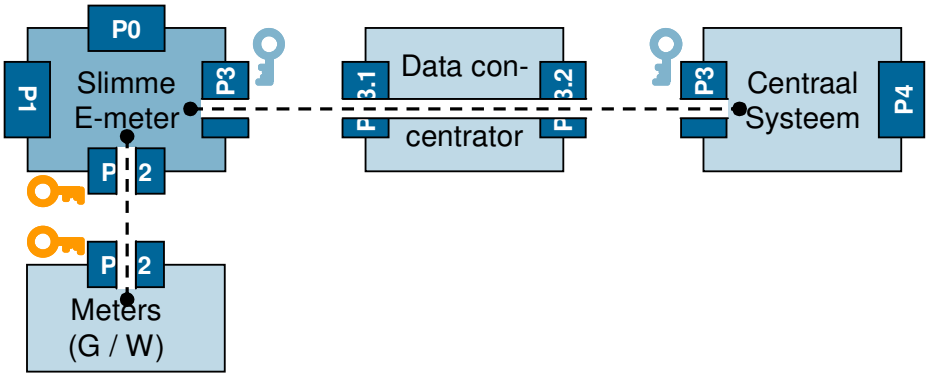
- Eindpunten liggen in het CS en de E-meter
- De inhoud van berichten is daardoor alleen in deze systemen ongecodeerd beschikbaar
- 'Onderweg' kunnen berichten wellicht worden 'afgetapt', maar het is praktisch niet mogelijk deze te interpreteren
- Dataconcentrators fungeren als 'doorgeefluik' van communicatie op applicatieniveau; ze geven alleen versleutelde berichten door zonder rol in de beveiliging.



Figuur 3: end-to-end encryptie bij communicatie tussen CS en E-meter

Encryptie van communicatie tussen CS en G/W-Meter via E-meter

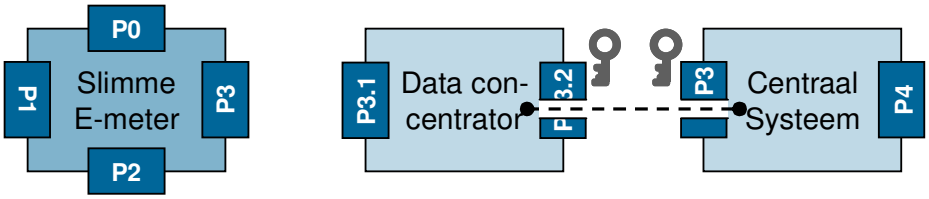
- Eindpunten liggen in het CS en de E-meter.
- De dataconcentrator is daarmee een 'doorgeefluik' van communicatie op applicatieniveau en geeft alleen versleutelde berichten door. De dataconcentrator heeft dus geen actieve rol in de beveiliging
- E-meter is geen doorgeefluik, maar is in staat om berichten van en naar de G/W meter te bewerken. De inhoud van berichten op applicatieniveau kan binnen de E- en G/W-meter onversleuteld beschikbaar zijn. Dit is een acceptabele situatie, omdat op dit punt de schaal van mogelijke incidenten al is beperkt tot één huishouden. Anders gezegd: als iemand zijn eigen meter 'hackt' is nog niet de meter van de buren gehackt.



Figuur 4: end-to-end encryptie bij communicatie tussen CS en G/W-meter. Encryptie van de P2-poort is enkel vereist bij een draadloze verbinding.

End-to-end encryptie van communicatie tussen CS en dataconcentrator

- Eindpunten liggen in het CS en de dataconcentrator.
- De inhoud van berichten is daardoor alleen in deze systemen onversleuteld beschikbaar
- Communicatie is bestemd voor / afkomstig van dataconcentrator; de inhoud van het bericht bevat geen informatie afkomstig van of bestemd voor slimme meters.



Figuur 5: end-to-end encryptie bij communicatie tussen CS en dataconcentrator

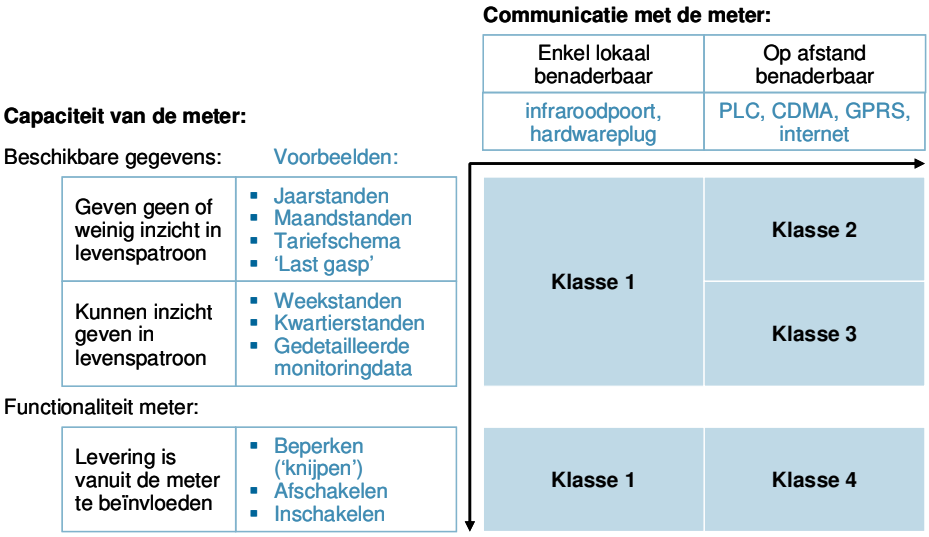
4.7 Afwegingen en keuzes tijdens formuleren eisen

De eisen en maatregelen zijn in verschillende iteraties tot stand gekomen. Bij iedere iteratie heeft de werkgroep feedback van verschillende bronnen geregistreerd, afgewogen en verwerkt. Afwegingen welke meespeelden om voor de ene of andere formulering te kiezen zijn bijgehouden in een log. Hierin zijn afwegingen, keuzes en ontwikkeling van eisen en maatregelen van versie 0.98 tot en met de huidige versie terug te vinden. Dit bestand is op aanvraag bij de werkgroep beschikbaar.

4.8 Koppeling tussen risico's en eisen

De in de risicoanalyse genoemde risico's veronderstellen een geavanceerde slimme meter (zoals die beschreven in de NTA 8130) en bijbehorende infrastructuur. Mede op basis hiervan heeft de werkgroep Privacy en Security een set van beveiligingseisen en -maatregelen opgesteld. Voor de meeste risico's zijn meerdere eisen geformuleerd, en sommige eisen dekken meerdere risico's (deels) af.

Bij de werkgroep is op aanvraag een document beschikbaar waarin de koppeling tussen risico's en maatregelen vastgelegd is. Omdat dit document nogal omvangrijk is, heeft de werkgroep er voor gekozen om risico's en maatregelen op een hoger abstractieniveau aan elkaar te koppelen, te weten via 'risicoklasses'. Hierbij is er vanuit gegaan dat risico's van een slimme-meterconfiguratie vooral gedreven worden vanuit (1) de technische mogelijkheden van de meter en (2) de mogelijkheid om met de meter te kunnen communiceren. Op basis hiervan zijn de volgende vier risicoklasses gedefinieerd:



Figuur 6: bepaling risicoklasse van een configuratie op basis van wat een slimme meter kan (capaciteit) en hoe deze benaderd wordt (communicatie). Gegeven voorbeelden van informatietypes of functionaliteit zijn niet uitputtend; zie hoofdstuk 3.3 voor een gedetailleerde behandeling.

Hoe hoger de risicoklasse, hoe meer eisen en maatregelen van toepassing zijn. Maatregelen van toepassing bij een lagere risicoklasse zijn ook van toepassing bij hogere klasses. Maatregelen bij risicoklasse 0 (niet in Figuur 6 weergegeven) zijn altijd van toepassing. Onderstaande tabel geeft ter indicatie per risicoklasse een overzicht van maatregelen en overwegingen. Deze tabel is in geen enkel opzicht volledig – zie de risicoklasse-indeling bij de eisen en maatregelen voor een volledig overzicht.

Klasse	Indicatie toepasselijke maatregelen	Overwegingen
0	Verzegeling van apparaten, …	Minimale of wettelijke verplichting
1	Beveiliging van toegangspoorten met unieke loginnamen en wachtwoorden, …	Weinig privacyrisico's; fraude-risico nauwelijks hoger dan bij klassieke gas- en elektriciteitsmeters
2	Geen adres- of persoonsgegevens in de meter, bemoeilijking van toegang tot communicatiekanalen, …	Meeluisteren is ongewenst, maar het privacyrisico is beperkt; onbevoegd configureren van meter is wel een risico
3	Versleuteling van alle draadloze communicatie, privacyeisen vanuit netbeheerder aan installatiebedrijven, …	Er wordt privacygevoelige informatie verzonden, maar levering is nog niet in gevaar
4	Alle maatregelen, waaronder 'end-to-end' encryptie met enkel het Centraal Systeem en de meter als eindpunten	Vanuit ieder punt in de keten waar informatie onversleuteld aanwezig is kunnen meters afgeschakeld worden

5. Toepassing en structuur eisen en maatregelen

5.1 Link met bestaand beveiligingsbeleid

In deze documenten is verondersteld dat er bij netbeheerders een beveiligingsbeleid conform ISO27002 is geïmplementeerd. Als dit het geval is, zijn deze eisen en maatregelen een aanvulling voor specifieke hoofdstukken. Als een netbeheerder geen invulling heeft gegeven aan ISO27002 kunnen de eisen en maatregelen een begin zijn om voor wat betreft de slimme-meterinfrastructuur hieraan te voldoen.

De werkgroep heeft er voor gekozen om niet een volledig ISO-document op te leveren, maar slechts een aanvulling daarop om:

- de focus op specifiek slimme-metergerelateerde risico's te houden en geen opsomming te maken van IT-beheersmaatregelen die al geïmplementeerd zouden moeten zijn;
- leesbaarheid en beheersbaarheid van het document te vergemakkelijken.

5.2 Comply or explain

Voor alle eisen en maatregelen geldt het principe 'comply or explain', ofwel 'pas toe of leg uit'. Uitgangspunt daarbij is dat netbeheerders volledig aan in deze documenten gestelde eisen en maatregelen voldoen, maar dat er flexibiliteit is als dat vanuit risicomanagement-perspectief of bedrijfskundig perspectief niet haalbaar of niet zinnig is. Eventuele afwijkingen van eisen en maatregelen dienen wel gemotiveerd en gedocumenteerd te worden, waarbij ook expliciet gemaakt dient te worden welke (rest)risico's overblijven en door de netbeheerder geaccepteerd worden.

5.3 Structuur eisen en maatregelen

Alle in hoofdstuk 0 genoemde beveiligingsdoelen zijn vertaald naar een of meerdere eisen. Onder 'eis' wordt in deze documenten bedoeld: een concretisering van de beveiligingsdoelen voor een specifieke techniek, component, proces of informatietype in de slimme-meterinfrastructuur. Een eis geeft antwoord op de vraag: "wat wil je bereiken?". Daarnaast zijn voor een deel van de eisen maatregelen gedefinieerd. Onder 'maatregel' is een manier om een eis te realiseren en geeft antwoord op de vraag: "hoe ga je het bereiken?". Eisen zijn bepalend, maatregelen zijn richtinggevend.

Figuur 7: Schematische weergave van structuur eisen en maatregelen; e-nr staat voor het unieke nummer dat aan een eis is toegekend

Iedere eis voorzien van een uniek nummer. Van elke eis is aangegeven welk(e) doel(en) er mee worden bereikt en in welke risicoklasse deze valt. Van een deel van de eisen is bovendien aangegeven waar deze ondergebracht zou kunnen worden. Dit is aangegeven met 'Borging: <documentnaam>'. Hiermee geeft de werkgroep Privacy en Security een suggestie voor verdere borging. Daadwerkelijke overname van de richtlijn is en blijft afhankelijk van de betreffende documenteigenaren.

Verder is van iedere eis aangegeven waar deze past in het beveiligingsbeleid van netbeheerders als deze conform ISO27002 is opgesteld. Omwille van leesbaarheid zijn sommige ISO-hoofdstuktitels afgekort. Onderstaande tabel toont de volledige naam:

H	ISO-hoofdstuktitel (afgekort)	Volledige hoofdstuktitel
5	Beveiligingsbeleid	Beveiligingsbeleid
6	Organisatie van […]	Organisatie van informatiebeveiliging
7	Beheer van bedrijfsmiddelen	Beheer van bedrijfsmiddelen
8	Beveiliging van personeel	Beveiliging van personeel
9	Fysieke beveiliging en …	Fysieke beveiliging en beveiliging van de omgeving
10	Beheer van communicatie- en …	Beheer van communicatie- en bedieningsprocessen
11	Toegangsbeveiliging	Toegangsbeveiliging
12	Verwerving, ontwikkeling en onderhoud ...	Verwerving, ontwikkeling en onderhoud van informatiesystemen
13	Beheer van […]incidenten	Beheer van informatiebeveiligingsincidenten
14	Bedrijfscontinuïteitsbeheer	Bedrijfscontinuïteitsbeheer
15	Naleving	Naleving

5.4 Formulering van maatregelen

Maatregelen vallen onder dezelfde risicoklasse als de bovenliggende eis, tenzij anders aangegeven. Maatregelen zijn ‘richtinggevend’, maar afhankelijk van de formulering zijn deze meer of minder limiterend:

- Bij gebruik van formuleringen als ‘hierbij geldt’ en ‘bovendien geldt’ is de maatregel een belangrijke invulling op de eis.
- Bij gebruik van de formulering ‘ten minste’ is er sprake van een minimale opsomming; het staat netbeheerders vrij om maatregelen te nemen die breder van toepassing zijn.
- Bij gebruik van formuleringen als ‘bijvoorbeeld’, ‘zoals’ en ‘ter illustratie’ geeft de maatregel een of meerdere oplossingsrichtingen aan. Het is aan netbeheerders of deze overgenomen wordt / worden, of dat voor een andere, gelijkwaardige oplossing gekozen wordt om aan de eis invulling te geven.

6. Eisen en maatregelen

6.1 Algemeen geldende en ketenoverstijgende maatregelen

1.01	ISO: 6 Organisatie van [...]	Doel: B4, B5	Klasse: 1	Borging: -

De netbeheerder dient een privacybeleid en informatiebeveiligingsbeleid te hebben gedefinieerd, vastgelegd en geïmplementeerd.

1.02	ISO: 5 Beveiligingsbeleid	Doel: B4	Klasse: 0	Borging: -

De netbeheerder dient het privacy- en informatiebeveiligingsbeleid ten minste jaarlijks en zodra zich belangrijke ontwikkelingen voordoen, te beoordelen en wanneer nodig bij te stellen om te zorgen dat het geschikt, toereikend en doeltreffend blijft.

> Hieraan ten grondslag ligt een periodieke risicoanalyse om te verzekeren dat juiste en volledige maatregelen voor gecontroleerd beheer zijn geïdentificeerd, goedgekeurd en geïmplementeerd.

1.03	ISO: 5 Beveiligingsbeleid	Doel: B5; B7	Klasse: 0	Borging: -

De netbeheerder dient zorg te dragen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden inzake de verzameling en verwerking van gegevens verzameld middels de slimme meter ('doelbinding').

> Hierbij geldt dat het centraal systeem dient te beschikken over functionaliteit om te monitoren welke data (waaronder intervalstanden) over welke periode bij klanten zijn opgehaald.

1.04	ISO: 5 Beveiligingsbeleid	Doel: B7	Klasse: 0	Borging: -

Netbeheerder draagt er voor zorg dat persoonsgegevens, waaronder de meetgegevens, worden verwerkt conform de gespecificeerde doeleinden (verenigbaarheid van de gegevensverwerking).

> Hierbij geldt dat intervalstanden en dagstanden niet worden opgehaald van of verzonden door de slimme meter, tenzij hier een legitieme reden voor is of instemming is gegeven door de klant. Intervalstanden worden slechts opgehaald gedurende de periode waarin dit noodzakelijk is.
>
> De netbeheerder dient maatregelen te treffen welke er in voorzien dat de verwerking en verstrekking van intervalstanden, dagstanden en maandstanden geschiedt conform de genoemde grondslagen.

1.05 ISO: 5 Beveiligingsbeleid Doel: B1 Klasse: 0 Borging: -

Netbeheerder treft maatregelen welke waarborgen dat persoonsgegevens niet worden verwerkt als een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat (geheimhoudingsverplichting)

1.06 ISO: 5 Beveiligingsbeleid Doel: B7 Klasse: 0 Borging: -

Netbeheerder treft maatregelen welke waarborgen dat gegevens toereikend, ter zake dienend en niet bovenmatig zijn, en dat niet meer gegevens worden verwerkt dan nodig.

1.07 ISO: 5 Beveiligingsbeleid Doel: B1, B8 Klasse: 0 Borging: -

Netbeheerder draagt zorg voor de melding inzake het verzamelen en verwerken van persoonsgegevens verzameld middels de slimme meter bij het CBP.

1.08 ISO: 5 Beveiligingsbeleid Doel: B1, B8 Klasse: 0 Borging: -

Netbeheerder heeft maatregelen getroffen die er in voorzien dat de 'melding van verwerking persoonsgegevens' bij CBP actueel blijft en in voorkomende gevallen wordt aangepast.

1.09 ISO: 10 Beheer van communicatie- en ... Doel: B7 Klasse: 1 Borging: -

Netbeheerder dient maatregelen te treffen welke waarborgen dat persoonsgegevens, inclusief de meetgegevens, niet langer worden bewaard dan noodzakelijk is gezien de doeleinden waarvoor zij worden verzameld of worden verwerkt.

> Hierbij geldt dat bewaartermijnen van meterstanden in het centraal systeem zijn gemaximeerd:
>
> - voor intervalstanden: 10 kalenderdagen.
> - voor dagstanden: 40 kalenderdagen.
> - voor maandstanden: 13 maanden
>
> Hierbij geldt dat ongeacht de capaciteit van apparaten om meterstanden op te slaan de bewaartermijnen van data hardwarematig of via de configuratie zijn gemaximeerd:
>
> - voor intervalstanden: 10 kalenderdagen
> - voor dagstanden: 40 kalenderdagen
> - voor maandstanden: 13 maanden

1.10 ISO: 6 Organisatie van [...] Doel: B4, B5 Klasse: 1 Borging: -

Verantwoordelijkheden en taken van medewerkers binnen de netbeheerder betreffende privacy en informatiebeveiliging dienen te zijn gedefinieerd, vastgelegd en geïmplementeerd.

1.11 ISO: 10 Beheer van communicatie- en ... Doel: B2 Klasse: 1 Borging: DSMR

Binnen de netbeheerder dient wijzigingsbeheer voor componenten binnen de slimme-meterinfrastructuur te zijn gedefinieerd, vastgelegd en geïmplementeerd.

Hierbij geldt dat wijzigingsbeheerprocedures dienen te worden verwerkt in het kwaliteitsbeheersysteem van de netbeheerder.

1.12	ISO: 10 Beheer van communicatie- en …	Doel: B11	Klasse: 2	Borging: DSMR

Netbeheerder dient ongeautoriseerde toegang tot, en wijzigingen aan de slimme-meterinfrastructuur te detecteren.

Hierbij geldt dat:

- functionaliteit op apparaten niet in of uit te schakelen is zonder dat de netbeheerder dit opmerkt.
- fysieke en logische koppelingen tussen apparaten en systemen en tussen componenten in apparaten op afstand verifieerbaar zijn door de netbeheerder
- bij storing of ontkoppeling van een P2-verbinding door de elektriciteitsmeter een waarschuwing gegenereerd wordt voor het centraal systeem

1.13	ISO: 10 Beheer van communicatie- en …	Doel: B2, B3, B6	Klasse: 1	Borging: DSMR, P4

Het meerdere malen versturen van hetzelfde bericht dient niet te mogen leiden tot het meer dan eenmaal accepteren van dat bericht (‘replay attacks’).

1.14	ISO: 10 Beheer van communicatie- en …	Doel: B2, B6, B11	Klasse: 3	Borging: DSMR

Netbeheerder dient kritieke beveiligingsfunctionaliteit van geïnstalleerde apparaten snel te kunnen updaten.

Hierbij geldt dat onder kritieke beveiligingsfunctionaliteit van apparaten minimaal wordt verstaan: encryptiealgoritmes en authenticatiealgoritmes.

1.15	ISO: 10 Beheer van communicatie- en …	Doel: B2; B6	Klasse: 2	Borging: DSMR

Netbeheerder dient te borgen dat de firmwareversie en aanwezige beveiligingsfunctionaliteit op apparaten regelmatig gecontroleerd wordt.

Hierbij geldt dat de netbeheerder in ieder geval op afstand de firmwareversies en de aanwezige beveiligingsfunctionaliteit in de slimme-meterinfrastructuur kan opvragen en controleren.

Hierbij geldt dat apparaten bijvoorbeeld beschikken over functionaliteit om de versie van de firmware en de configuratie naar het CS te sturen, mits dit voldoende informatie geeft over aanwezige beveiligingsfunctionaliteit.

1.16	ISO: 11 Toegangsbeveiliging	Doel: B3, B4	Klasse: 1	Borging: -

Binnen de netbeheerder dient autorisatiebeheer voor componenten binnen de slimme-meterinfrastructuur te zijn gedefinieerd, vastgelegd en geïmplementeerd waarbij alleen de netbeheerder toegang heeft tot de slimme-meterinfrastructuur.

Hierbij geldt dat:

- de autorisatiebeheerprocedures dienen te worden verwerkt in het kwaliteitsbeheersysteem van de netbeheerder; en
- ten minste eenmaal per jaar gecontroleerd wordt of de rechten van medewerkers nog kloppen met hun functie.

Bovendien geldt dat maatregelen getroffen dienen te zijn om ongeautoriseerde wijzigingen van fysieke en logische ('softwarematige') koppelingen tussen apparaten en systemen en tussen componenten in apparaten te voorkomen;

1.17 ISO: 11 Toegangsbeveiliging Doel: B3 Klasse: 1 Borging: -

Medewerkers van de netbeheerder dienen enkel toegang te hebben tot die functionaliteit en informatie in de slimme-meterinfrastructuur die nodig is voor de werkzaamheden die zij verrichten uit hoofde van hun functie

Hierbij geldt expliciet dat netbeheerder autorisaties vastlegt in een autorisatiematrix die up-to-date wordt gehouden. Toegang wordt alleen binnen een vastgelegd autorisatieproces toegekend en ontnomen. Dit geldt ook voor alle betrokken externen.

1.18 ISO: 11 Toegangsbeveiliging Doel: B2, B3 Klasse: 1 Borging: -

Toegang tot en activiteiten met kritieke systeemfuncties in de slimme-meterinfrastructuur dienen alleen onder verhoogd toezicht en op basis van maximale functiescheiding plaats te vinden waarbij, waar technisch mogelijk, logging van de uitgevoerde activiteiten plaatsvindt. Logging dient te herleiden te zijn naar unieke natuurlijke personen.

Hierbij geldt dat ten minste de volgende activiteiten als kritieke systeemfuncties worden beschouwd:

- de mogelijkheid tot het schakelen van meters en instellen van doorlaatwaardes;
- het updaten van firmware; en
- het beheer van sleutels en wachtwoorden.

Wanneer meters geschakeld worden geldt het vier-ogenprincipe, ook als dit schakelopdrachten betreft vanaf de P4-poort.

1.19 ISO: 11 Toegangsbeveiliging Doel: B3 Klasse: 1 Borging: DSMR

Voor apparaten, systemen, software en netwerken in de slimme-meterinfrastructuur dient de netbeheerder schriftelijk te hebben vastgelegd welke diensten, poorten en koppelingen aanwezig zijn, welke noodzakelijk zijn en waarom deze noodzakelijk zijn. Niet-noodzakelijke functionaliteit dient uitgeschakeld te zijn of is door de netbeheerder op afstand uit te schakelen ('hardening').

1.20 ISO: 12 Verwerving, ontwikkeling en onderhoud ...Doel: B2, B3, B9 Klasse: 1 Borging: DSMR

De netbeheerder dient te borgen dat iedere leverancier van apparaten, systemen, software of netwerken een verklaring oplevert dat zijn producten geen ‘backdoors’ bevatten waarmee ongeautoriseerd toegang tot de slimme-meterinfrastructuur kan worden verkregen.

1.21 ISO: 12 Verwerving, ontwikkeling en onderhoud …Doel: B2, B3, B9 Klasse: 1 Borging: -

Netbeheerder dient te borgen dat alle leveranciers van apparaten, systemen, software en netwerken in de slimme-meterinfrastructuur en alle leveranciers van advies en beheer op het gebied van slimme meters meewerken aan audits door of namens de netbeheerder voor zover deze betrekking hebben op privacy- en informatiebeveiligingsaspecten van de slimme-meterinfrastructuur.

1.22 ISO: 12 Verwerving, ontwikkeling en onderhoud …Doel: B2, B3, B6 Klasse: 2 Borging: DSMR

In de slimme-meterinfrastructuur is alle communicatie op applicatieniveau en communicatie betreffende privacygevoelige informatie 'end-to-end' beveiligd, zodanig dat integriteit, authenticiteit, vertrouwelijkheid en uniekheid beschermd worden. De eindpunten van de beveiligde communicatie liggen in de elektriciteitsmeter en in het CS. Voor het aansturen van dataconcentrators liggen de eindpunten in de dataconcentrator en in het CS.

> Hierbij geldt dat het technisch onmogelijk is om met de meter over genoemde informatietypes te communiceren buiten het end-to-end beveiligde kanaal.
>
> Dit betreft ten minste de volgende informatietypes:
>
> - privacygevoelige informatie;
> - apparaatinstellingen;
> - firmwareupdates;
> - opdrachten voor het instellen van doorlaatwaardes; en
> - schakelopdrachten

1.23 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3 Klasse: 2 Borging: DSMR

Apparaten en systemen in de slimme-meterinfrastructuur dienen enkel berichten van geauthenticeerde apparatuur en partijen te accepteren.

1.24 ISO: 12 Verwerving, ontwikkeling en onderhoud …Doel: B3, B4, B5 Klasse: 3 Borging: DSMR

Toegepaste beveiligingsoplossingen dienen voor beoordelende instanties op aanvraag beschikbaar te zijn waarbij er geen sprake is van geheimhouding van ontwerp of broncode van (onderdelen van) de toegepaste beveiligingsoplossingen.

> Hierbij geldt dat gebruikte cryptografische technieken alleen op publiek beschikbare standaarden (zoals NIST) dienen te zijn gebaseerd en de techniek breed getoetst en geaccepteerd is.

1.25 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3, B6 Klasse: 3 Borging: DSMR

Netbeheerder dient periodiek te beoordelen of de op dat moment gebruikte versleutelings-technieken voldoende sterk zijn. Als gebruikte versleutelingstechnieken niet meer voldoende sterk zijn, dienen netbeheerders maatregelen te definiëren en implementeren.

Cryptografische algoritmes kunnen symmetrisch of asymmetrisch zijn, mits deze ten minste zo sterk zijn als AES met een sleutellengte van 128 bit. Vergelijking van encryptiesterktes kan gebaseerd worden op NIST Technical Report 800-57 part I (2007).

1.26 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3 Klasse: 3 Borging: DSMR

Het verkrijgen van ongeoorloofde toegang tot één apparaat mag niet leiden tot het verkrijgen van toegang tot meerdere apparaten.

Hierbij geldt dat wachtwoorden en beveiligingssleutels altijd per apparaat uniek dienen te zijn vanaf het moment van installatie van het apparaat. Dit betreft ook expliciet APN-logingegevens.

1.27 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3 Klasse: 2 Borging: DSMR

Alle apparaten dienen te zijn voorzien van voldoende sterke wachtwoorden.

Hierbij geldt dat wachtwoorden aan de volgende eisen dienen te voldoen:

- minimaal 10 karakters lang,
- samengesteld uit de set met alfanumerieke tekens (kleine letters, hoofdletters en cijfers), en
- willekeurig en niet-afleidbaar gegenereerd.

1.28 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3, B4 Klasse: 3 Borging: DSMR

Netbeheerder dient elk wachtwoord en elke gebruikte beveiligingssleutel in alle in de slimme-meterinfrastructuur voorkomende apparaten op afstand te kunnen wijzigen. Niemand buiten de netbeheerder kan genoemde wachtwoorden en sleutels wijzigen.

Hierbij geldt dat de zogenaamde 'master key', is uitgezonderd, mits met deze sleutel niets in de meter te wijzigen is zonder ook een andere sleutel te kennen.

1.29 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4 Klasse: 2 Borging: DSMR

Netbeheerder dient alle af-fabriek wachtwoorden en wijzigbare sleutels voor of tijdens installatie, of bij de eerste communicatie met het CS, te vervangen.

1.30 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3, B4 Klasse: 3 Borging: -

Netbeheerders hebben een sleutel- en wachtwoordbeleid gedefinieerd, vastgelegd en geïmplementeerd voor ten minste alle sleutels en wachtwoorden in de slimme-meterinfrastructuur.

Hierbij geldt dat netbeheerders sleutels en wachtwoorden minimaal eens per vastgestelde termijn dienen te wijzigen.

Wachtwoorden en beveiligingssleutels dienen vervangen te worden na bekendwording, verlies of diefstal.

1.31 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3, B4 Klasse: 3 Borging: -

Netbeheerder dient een proces te hebben gedefinieerd, vastgelegd en geïmplementeerd om wachtwoorden en beveiligingssleutels snel te kunnen vernieuwen.

1.32 ISO: 13 Beheer van […]incidenten Doel: B4, B5, B11 Klasse: 0 Borging: -

Netbeheerders en Netbeheer Nederland dienen procedures hoe wordt omgegaan met privacy- en informatiebeveiligingsincidenten die schade aan de hele sector zouden kunnen veroorzaken onderling te hebben gedefinieerd, vastgelegd en geïmplementeerd.

> Hierbij geldt dat netbeheerders dienen te beschikken over een register waarin zowel privacygerelateerde incidenten als informatiebeveiligingsincidenten betreffende de slimme-meterinfrastructuur worden geregistreerd. Dit register voorziet een landelijk incidentregister tijdig en juist van informatie over incidenten.
>
> Netbeheerders dienen incidenten conform eigen incidentmanagement te registreren en af te handelen.
>
> Netbeheer Nederland dient alle gemelde incidenten te beoordelen op sectorbrede impact en, wanneer van toepassing, sectorbreed af te handelen.
>
> Hierbij geldt dat zowel het register bij de netbeheerder als het landelijk incidentregister enkel toegankelijk moet zijn voor functionarissen van netbeheerders.
>
> De netbeheerders die het incident meldt dient over privacygerelateerde incidenten te communiceren met betreffende klanten.

1.33 ISO: 13 Beheer van […]incidenten Doel: B4, B11 Klasse: 0 Borging: -

Netbeheerder dient procedures en instructies, die beschrijven hoe medewerkers dienen om te gaan met privacy- en informatiebeveiligingsincidenten, te hebben gedefinieerd, vastgelegd en geïmplementeerd en actief uit te dragen naar haar medewerkers.

1.34 ISO: 14 Bedrijfscontinuïteitsbeheer Doel: B6 Klasse: 2 Borging: -

De netbeheerder dient te borgen dat met consumenten afgesproken is dat zij de communicatie met de slimme meter niet bewust blokkeren of storen.

> Deze bepaling kunnen netbeheerders bijvoorbeeld opnemen in de aansluitvoorwaarden.

1.35 ISO: 15 Naleving Doel: B1, B7 Klasse: 2 Borging: -

Netbeheerder dient zijn klanten juist, tijdig en volledig te informeren over het verzamelen en verwerken van slimme-metergerelateerde gegevens conform de eisen gesteld in de WBP

1.36	ISO: 15 Naleving	Doel: B1, B7	Klasse: 2	Borging: -

Netbeheerder dient te borgen dat rechten van klanten worden gerespecteerd, waaronder rechten vastgelegd in de Wet bescherming persoonsgegevens (WBP) en de 'novelle' op de 'Wet tot wijziging elektriciteitswet uit 1998 en gaswet ter verbetering van de werking van de elektriciteits- en gasmarkt (31374)'.

Hierbij geldt dat minimaal maatregelen dienen te worden getroffen ten aanzien van:

- recht op inzage, correctie en wanneer mogelijk verwijdering van persoonsgegevens;
- recht op inzage in persoonsgegevens en meetdata;
- recht op inzage aan wie en wanneer welke meetdata zijn verstrekt;
- recht om toestemming om intervaldata te verstrekken aan energieleveranciers weer in te trekken (recht van verzet);
- recht om zich te verzetten tegen installatie slimme meter;
- recht om de uitleesfrequentie van de slimme meter te beperken (in afwachting van de novelle).

6.2 Apparaatspecifieke eisen en maatregelen (meter en DC)

2.01	ISO: 6 Organisatie van [...]	Doel: B9	Klasse: 2	Borging: -

Netbeheerder dient te borgen dat installatiebedrijven pas met apparaten werken als zij een garantie hebben gegeven en aannemelijk hebben gemaakt een voldoende beveiligingsniveau te realiseren, in lijn met het beveiligingsniveau van de netbeheerder.

Hierbij geldt dat bijvoorbeeld de volgende maatregelen onderdeel uitmaken van de afspraken tussen de netbeheerder en de installatiebedrijven:

- het installatiebedrijf tekent een geheimhoudingsverklaring
- het installatiebedrijf beschikt over een adequate gedragsrichtlijn en procedures ten aanzien van omgang met (gevoelige) informatie en draagt deze actief uit naar haar medewerkers
- privacygevoelige informatie wordt vernietigd na gebruik, of zo gauw de netbeheerder daar om vraagt.
- netbeheerder heeft recht tot audit om (steekproefsgewijs) te controleren of installatiebedrijven en monteurs werken volgens de geldende privacy- en informatiebeveiligingsrichtlijnen. De netbeheerder maakt ten minste gebruik van dit recht bij vermoedens van niet handelen conform afspraken.

2.02	ISO: 9 Fysieke beveiliging en ...	Doel: B3	Klasse: 0	Borging: DSMR

Apparaten die operationeel in gebruik zijn dienen altijd verzegeld te zijn.

2.03	ISO: 9 Fysieke beveiliging en ...	Doel: B3	Klasse: 2	Borging: -

Netbeheerder dient dataconcentrators te beschermen tegen fysieke manipulatie.

Hierbij geldt dat dataconcentrators ten minste in fysiek afsluitbare ruimtes geïnstalleerd worden en dat het mogelijk is fysieke manipulatie te detecteren, bijvoorbeeld omdat toegang niet mogelijk is zonder een zegel te verbreken of zonder dat een 'tamper alert' gegenereerd wordt.

2.04 ISO: 10 Beheer van communicatie- en … Doel: B6 Klasse: 2 Borging: -

Netbeheerder heeft maatregelen vastgesteld, gedefinieerd en geïmplementeerd om te borgen dat tijdens of na installatie gecontroleerd wordt of de meter juist is ingesteld en of apparaten juist gekoppeld zijn.

Hierbij geldt dat de maatregelen minimaal dienen te voorzien in de volgende controles:

- apparaatnummer, EAN-code en adresgegevens in het meterregister of aansluitregister correct gekoppeld;
- communicatie met het CS beveiligd met gebruik van sleutels die vervangen zijn; en
- alle wachtwoorden in de apparaten vervangen zijn.

2.05 ISO: 10 Beheer van communicatie- en … Doel: B10, B11 Klasse: 3 Borging: DSMR

Netbeheerder dient te borgen dat in het ontwerp van apparaten rekening wordt gehouden met toekomstvastheid van de beveiligingsfunctionaliteit.

In het ontwerp van apparaten dient bijvoorbeeld rekening gehouden te worden met toekomstige, complexere beveiligingsalgoritmes die meer rekenkracht of meer geheugen nodig hebben, zoals ruimte voor AES-256 of 'elleptic curve cryptography'.

2.06 ISO: 10 Beheer van communicatie- en … Doel: B2, B6 Klasse: 4 Borging: DSMR

Netbeheerders dienen te borgen dat slimme meters berichten of firmware welke verspreid is via broadcast enkel accepteren na ontvangst van een door het CS gegenereerd, end-to-end-beveiligd, meterspecifiek bericht, waarmee de authenticiteit en integriteit van het broadcastbericht vast te stellen is.

2.07 ISO: 10 Beheer van communicatie- en … Doel: B6 Klasse: 2 Borging: DSMR

Alle draadloze communicatie vanaf de slimme meter dient beveiligd te zijn zodat integriteit, authenticiteit, vertrouwelijkheid en uniekheid van berichten is gewaarborgd.

Hierbij geldt dat voor encryptie van draadloze communicatie unieke sleutels worden gebruikt. Dit is nadrukkelijk ook van toepassing op draadloze oplossingen voor de P2-poort.

2.08 ISO: 10 Beheer van communicatie- en … Doel: B7 Klasse: 1 Borging: -

In een apparaat dienen nooit persoonsgegevens, lokatiespecifieke informatie of EAN-codes opgeslagen te zijn, uitgezonderd meetstanden.

2.09 ISO: 10 Beheer van communicatie- en … Doel: B7 Klasse: 1 Borging: -

Identificatie van apparaten dient plaats te vinden op basis van apparaatnummer of combinatie van een apparaattype en serienummer.

2.10 ISO: 10 Beheer van communicatie- en … Doel: B7 Klasse: 1 Borging: DSMR

Het dient niet mogelijk te zijn verbruikspatronen af te leiden van de frequentie of omvang van berichtenverkeer vanaf de slimme meter, waaronder het P2 of P3-dataverkeer.

> Hierbij geldt dat berichten waar mogelijk een vaste grootte en verzendinterval dienen te hebben.

2.11 ISO: 10 Beheer van communicatie- en … Doel: B3, B11 Klasse: 2 Borging: DSMR

Dataconcentrators dienen ongeautoriseerd dataverkeer op te merken en een waarschuwing te genereren voor het centraal systeem.

> Hierbij dienen DC's bijvoorbeeld op te merken:
>
> – dat een onbekende DC is geïnstalleerd; of
> – dat een onbekend apparaat de DC probeert te benaderen.

2.12 ISO: 10 Beheer van communicatie- en … Doel: B7 Klasse: 4 Borging: DSMR

Netbeheerders borgen dat dataconcentrators geen toegang hebben tot persoonsgegevens, meterstanden of sleutels die gebruikt worden voor end-to-end beveiligde communicatie tussen het CS en de slimme meters.

> Hierbij geldt dat dataconcentrators versleutelde berichten die tussen het Centraal Systeem en slimme meters verzonden worden niet kunnen ontsleutelen; dergelijke berichten worden versleuteld doorgezonden.

2.13 ISO: 10 Beheer van communicatie- en … Doel: B2, B9 Klasse: 3 Borging: DSMR

Als apparaten gebruik maken van standaard besturingssystemen dienen netbeheerders te borgen dat securitypatches snel en consequent worden toegepast en de volgende functionaliteiten geimplementeerd zijn: intrusion detection, logging (aanmaken van logbestanden) en firewall.

> Hierbij geldt dat onder 'standaard besturingssystemen' ten minste verstaan worden: alle windowsvarianten en alle Unix- en Linuxgebaseerde besturingssystemen.
>
> Door betreffende apparaten gegenereerde logbestanden dienen door netbeheerder geregeld opgehaald en onderzocht te worden op ongebruikelijke acties en gebeurtenissen.

2.14 ISO: 11 Toegangsbeveiliging Doel: B3 Klasse: 1 Borging: DSMR

Toegang tot alle poorten op apparaten dient alleen mogelijk te zijn na authenticatie.

Hierbij geldt dat de P1 poort is uitgezonderd van deze eis zolang dit een alleen-lezen poort is.

Als authenticatie op een poort driemaal achter elkaar mislukt, wordt alle toegang tot de betreffende poort gedurende minimaal 15 minuten geblokkeerd en wordt een waarschuwing gegenereerd voor het Centraal Systeem. Dit geldt voor alle poorten, waaronder ook P0.

2.15 ISO: 11 Toegangsbeveiliging Doel: B2 Klasse: 0 Borging: DSMR

De instellingen van het metrologische gedeelte van de meter en alle in het metrologisch gedeelte opgeslagen informatie, waaronder meetstanden, dienen door de netbeheerder niet aangepast te kunnen worden

2.16 ISO: 11 Toegangsbeveiliging Doel: B3 Klasse: 2 Borging: DSMR

Alle binnenkomende communicatie op alle poorten dient te worden gecontroleerd om correctheid en validiteit vast te stellen alvorens de communicatie wordt geaccepteerd

Hierbij geldt dat ter controle van correctheid de meter geen communicatie buiten een per poort gedefinieerde, beperkte set van toegestane berichten dient te accepteren.

2.17 ISO: 11 Toegangsbeveiliging Doel: B3, B11 Klasse: 2 Borging: DSMR

Een dataconcentrator dient enkel aan te sturen en te configureren te zijn via de P3.2-poort en dient maximaal één lokaal toegankelijke, voldoende beveiligde beheerpoort te hebben. Vanaf P3.1 is een dataconcentrator niet aan te sturen.

Hierbij geldt dat deze lokaal toegankelijke beheerpoort beveiligd dient te zijn met ten minste een unieke combinatie van een gebruikersnaam en wachtwoord welke voldoet aan het wachtwoordbeleid.

Bovendien geldt dat bij het aansluiten van een apparaat aan een beheerpoort een waarschuwing wordt gegenereerd voor het centraal systeem.

2.18 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B10 Klasse: 1 Borging: -

Netbeheerder dient te borgen dat fabrikanten ten behoeve van het productieproces van apparaten adequate beveiligingsprocessen hebben gedefinieerd, vastgelegd en geïmplementeerd.

Hierbij geldt dat netbeheerders afspraken moeten hebben met alle fabrikanten van apparaten over generatie, installatie, opslag, verzending en verwijdering van sleutels en wachtwoorden. Onderdeel van de afspraken is dat fabrikanten alle door hen gegenereerde sleutels en wachtwoorden direct en voorgoed verwijderen uit alle systemen op aangeven van de netbeheerder. Netbeheerders vragen hier ten minste om als zij de sleutels en wachtwoorden goed ontvangen en verwerkt hebben.

2.19	ISO: 15 Naleving	Doel: B10	Klasse: 1	Borging: -

Netbeheerder dient een acceptatieproces te hebben gedefinieerd, vastgelegd en geïmplementeerd om vast te stellen dat beveiligingsfunctionaliteit van geleverde apparaten juist en volledig is geïmplementeerd.

> Hierbij geldt dat elk type apparaat pas wordt gebruikt na het succesvol doorlopen van een serie tests, uitgevoerd door één van de door Netbeheer Nederland aan te wijzen instituten (typegoedkeuring). Deze tests omvatten ten minste:
>
> - een penetratietest op ten minste alle gedefinieerde poorten; en
> - een controle op de juistheid van implementatie van de beveiligingsfunctionaliteit zoals gedefinieerd in deze beveiligingsmaatregelen.
>
> De kwaliteit van de programmacode (broncode) met betrekking tot beveiligingsfunctionaliteit dient door een gekwalificeerde en onafhankelijke partij te worden gecontroleerd.
>
> Individuele, te installeren apparaten dienen steekproefsgewijs te worden getest op juistheid van de implementatie van beveiligingsfunctionaliteit volgens vooraf vastgestelde criteria door een door Netbeheer Nederland aan te wijzen instituut.

2.20	ISO: 13 Beheer van […]incidenten	Doel: B2	Klasse: 4	Borging: DSMR

Het is technisch niet mogelijk om op afstand een meter in- of af te schakelen, of doorlaatwaardes te veranderen, anders dan via een end-to-end-beveiligd, per meter uniek bericht vanaf het CS.

> Hierbij geldt dat deze eis nadrukkelijk ook 'Code Rood' betreft.

6.3 Eisen en maatregelen ten aanzien van datacommunicatie

3.01	ISO: 10 Beheer van communicatie- en …	Doel: B9	Klasse: 3	Borging: -

Netbeheerders dienen te borgen dat datacommunicatieleveranciers netwerkbeveiligingsmaatregelen hebben getroffen om de beveiliging en privacy van de slimme-meterinfrastructuur te waarborgen.

> Hierbij geldt dat:

- netwerkinfrastructuur adequaat beschermd dient te zijn tegen aanvallen, door middel van firewalling.
- systemen adequaat beschermd dienen te zijn tegen bedreigingen zoals virussen door middel van anti-virusprogrammatuur.
- er monitoring dient te zijn op relevante netwerksegmenten door middel van 'Intrusion Detection Systems' om aanvallen en andere onregelmatigheden te detecteren en passende tegenmaatregelen te kunnen nemen.

3.02 ISO: 10 Beheer van communicatie- en ... Doel: B6, B9 Klasse: 2 Borging: -

Netbeheerders dienen te borgen dat datacommunicatie zo veel als redelijkerwijs en economisch mogelijk is over netwerkverbindingen lopen die (fysiek) gescheiden zijn van andere aangeboden diensten en toepassingen.

Hierbij geldt dat indien fysiek gescheiden verbindingen niet mogelijk zijn de datacommunicatie over logisch gescheiden netwerkverbindingen verloopt.

3.03 ISO: 10 Beheer van communicatie- en ... Doel: B6, B9 Klasse: 2 Borging: -

De netbeheerder dient te borgen dat in het geval dat een deel van de slimme-metercommunicatie verloopt over een kanaal dat ook voor andere communicatie gebruikt wordt, de datacommunicatieleverancier er op toe ziet dat de kwaliteit, beschikbaarheid en beveiliging van dit kanaal voldoende is.

3.04 ISO: 10 Beheer van communicatie- en ... Doel: B9 Klasse: 2 Borging: -

De netbeheerder dient te borgen dat datacommunicatieleveranciers enkel data tussen slimme meters en CS en tussen dataconcentrator en CS routeren.

3.05 ISO: 10 Beheer van communicatie- en ... Doel: B3 Klasse: 2 Borging: -

Opslag van logingegevens voor geautomatiseerde toegang tot een netwerk dient alleen in het apparaat plaats te vinden.

In het geval van gebruik van een SIM-kaart voor identificatie geldt dus dat APN-logingegevens nooit op de SIM-kaart mogen worden geplaatst.

3.06 ISO: 10 Beheer van communicatie- en ... Doel: B3 Klasse: 3 Borging: -

In het geval de communicatie met behulp van een SIM-kaart opgebouwd dienen maatregelen getroffen te zijn om de koppeling tussen SIM-kaart en communicatiemodule te controleren en in stand te houden.

Om te controleren of sprake van een juiste koppeling is dient de datacommunicatieleverancier te controleren dat de SIM-kaart geïnstalleerd is in een apparaat uit de juiste reeks modemnummers (IMEI-nummers)

Om de koppeling in stand te houden geldt dat:

- of de SIM-kaart is verlijmd met de communicatiemodule;
- of de SIM-kaart zodanig is ingesteld dat deze, na in het ene apparaat gebruikt te zijn, nooit meer in een ander apparaat gebruikt kan worden;
- of datacommunicatieleveranciers SIM-kaarten blokkeren als deze geplaatst zijn buiten een bepaalde set van modemnummers.

3.07 ISO: 10 Beheer van communicatie- en … Doel: B3, B9 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat datacommunicatieleveranciers de toegang tot een (deel van een) netwerk tot enkel en alleen de afnemende netbeheerder beperken (exclusieve toegang, zoals een 'private APN').

3.08 ISO: 10 Beheer van communicatie- en … Doel: B3 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat datacommunicatieleveranciers de toegang tot diensten, netwerkpoorten en systemen beperken tot wat noodzakelijk is voor het functioneren van de slimme-meterinfrastructuur.

Hierbij geldt dat het overige is geblokkeerd, zoals bijvoorbeeld spraakdiensten.

3.09 ISO: 13 Beheer van […]incidenten Doel: B9, B11 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat datacommunicatieleverancier procedures hebben gedefinieerd, vastgelegd en geïmplementeerd om in het geval van calamiteiten het deel van het datacommunicatienetwerk gebruikt voor slimme meters snel te kunnen afschakelen.

Voorbeeld maatregel: in het geval SIM-kaarten gebruikt worden dient de datacommunicatieleverancier op verzoek van de netbeheerder SIM-kaarten of APN-login te kunnen blokkeren.

3.10 ISO: 13 Beheer van […]incidenten Doel: B9, B11 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat datacommunicatieleveranciers geconstateerde beveiligingslekken in de datacommunicatie-infrastructuur pro-actief melden en zo snel mogelijk oplossen.

3.11 ISO: 14 Bedrijfscontinuïteitsbeheer Doel: B6, B9, B10 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat er afspraken zijn met datacommunicatieleveranciers om de beschikbaarheid van het netwerk op de lange termijn te garanderen.

6.4 Eisen en maatregelen specifiek voor het centraal systeem

4.01 ISO: 10 Beheer van communicatie- en … Doel: B6 Klasse: 1 Borging: -

Alle wijzigingen aan gegevens in het CS dienen te worden gelogd.

4.02 ISO: 10 Beheer van communicatie- en … Doel: B2, B6 Klasse: 2 Borging: -

De netbeheerder dient te monitoren dat apparaten bereikbaar zijn.

Hierbij geldt dat het CS een waarschuwing dient te genereren als een slimme meter of dataconcentrator langer dan een vastgestelde termijn niet bereikt kan worden. De vastgestelde termijn is ten hoogste zeven kalenderdagen.

4.03 ISO: 10 Beheer van communicatie- en ... Doel: B11 Klasse: 2 Borging: -

Het CS dient alle door apparaten gegenereerde waarschuwingen (‘alerts’) en berichten te registeren, onverminderd het bepaalde in maatregel 4.17

4.04 ISO: 10 Beheer van communicatie- en ... Doel: B11 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat processen gedefinieerd, vastgelegd en geïmplementeerd zijn om alle door apparaten gegenereerde waarschuwingen te beoordelen en om passende acties te ondernemen wanneer beveiliging of privacy in gevaar zou kunnen zijn.

4.05 ISO: 10 Beheer van communicatie- en ... Doel: B6 Klasse: 2 Borging: -

Geregistreerde meterstanden in het CS dienen niet gewijzigd te kunnen worden.

Hierbij geldt dat het CS een herstelmogelijkheid dient te hebben in geval van bijzondere situaties, zoals uitval van de database.

4.06 ISO: 10 Beheer van communicatie- en ... Doel: B6 Klasse: 2 Borging: -

De netbeheerder borgt dat de tijd van de centrale systemen zoals gebruikt voor tijdsynchronisatie van slimme meters niet meer afwijkt dan een seconde van de vastgestelde tijd van een onafhankelijke bron.

Hierbij geldt dat de tijd op apparaten minimaal eens per week dient te worden gecontroleerd en, indien nodig, bijgewerkt. Als tijdens tijdsynchronisatie afwijkingen van meer dan 1 minuut gesignaleerd worden moeten deze onderzocht worden.

4.07 ISO: 10 Beheer van communicatie- en ... Doel: B9, B10 Klasse: 3 Borging: -

Netbeheerder dient te borgen dat partijen, die als bewerkers namens de netbeheerder aan de slimme meter gerelateerde privacygevoelige informatie werken een bewerkersovereenkomst tekenen en aannemelijk maken dat zij een voldoende beveiligingsniveau realiseren, in lijn met het beveiligingsniveau van de netbeheerder.

Betreffende partijen dienen regelmatig een privacy- en informatiebeveiligingsaudit te doorstaan.

Hierbij geldt dat ook installatiebedrijven gezien worden als 'bewerkers' in de zin van WBP.

4.08 ISO: 10 Beheer van communicatie- en … Doel: B1, B9, B10 Klasse: 0 Borging: -

Als een bewerker zich bevindt in een land buiten de EU dient voorafgaand aan de doorgifte, de netbeheerder er zorg voor te dragen dat aan alle eisen van de WBP wordt voldaan. Doorgifte vindt pas plaats nadat aan de netbeheerder een vergunning voor doorgifte is verleend door de minister van Justitie. De netbeheerder treft maatregelen welke erin voorzien dat de doorgifte plaatsvindt conform de voorschriften die aan de vergunning zijn verbonden.

> De netbeheerder draagt zorg voor een overeenkomst, gebruik makende van de standaard EU modelcontracten en dient een aanvraag voor een vergunning in bij het CBP.
>
> Verder geldt dat de netbeheerer periodiek vaststelt of nog aan de voorschriften van de vergunning wordt voldaan.

4.09 ISO: 11 Toegangsbeveiliging Doel: B3, B11 Klasse: 3 Borging: -

De netbeheerder dient de P3- en P4-poort te beveiligen tegen aanvallen, waaronder DoS-aanvallen, en maatregelen te treffen die de gevolgen van aanvallen minimaliseren.

> Tegen DoS-aanvallen kan bijvoorbeeld geregeld worden dat IP-ranges bij de Internet Service Provider geblokkeerd kunnen worden en dat SIM-kaarten bij de datacommunicatieleverancier geblokkeerd kunnen worden.

4.10 ISO: 11 Toegangsbeveiliging Doel: B11 Klasse: 4 Borging: -

Alle schakelopdrachten dienen te worden gelogd door het centraal systeem (CS), ongeacht waar ze vandaan komen (vanuit de netbeheerder zelf of via de P4-poort van derden).

4.11 ISO: 11 Toegangsbeveiliging Doel: B9 Klasse: 2 Borging: -

Partijen die van de P4-poort gebruik willen maken, dienen door EDSN gecertificeerd te zijn.

> Hierbij geldt als voorwaarde dat EDSN ter certificering van betreffende partijen heeft vastgesteld en daarna jaarlijks controleert:
>
> - dat deze legitiem opereren;
> - dat zij een voor P4-afnemers voldoende beveiligingsniveau gerealiseerd hebben in lijn met het beveiligingsniveau van netbeheerders; en
> - dat zij voldoende privacybeschermende maatregelen geimplementeerd hebben
>
> Bovendien geldt dat bij geconstateerd misbruik of bij geconstateerde lage beveiliging door EDSN de certificering wordt ingetrokken.

4.12 ISO: 11 Toegangsbeveiliging Doel: B3, B9 Klasse: 2 Borging: -

Het CS dient op de P4-poort alleen communicatie van door EDSN gecertificeerde partijen te accepteren.

4.13 ISO: 12 Verwerving, ontwikkeling en onderhoud …Doel: B3, B6, B9 Klasse: 0 Borging: -

Communicatie over P4 dient beveiligd te zijn, zodanig dat integriteit, authenticiteit, vertrouwelijkheid en uniekheid beschermd worden.

4.14 ISO: 11 Toegangsbeveiliging Doel: B3 Klasse: 2 Borging: -

Netbeheerders mogen bij redelijke vermoedens van misbruik de toegang tot P4 tijdelijk blokkeren. Zij melden dit met een motivatie aan EDSN en aan de betreffende P4-afnemer.

> Hierbij geldt dat misbruik op de P4-poort wordt beschouwd als een privacy- of securityincident (zie maatregelen omtrent melden hiervan).

4.15 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4 Klasse: 0 Borging: -

Netbeheerder heeft verantwoordelijkheden en taken ten aanzien van de beveiligingsfunctionaliteit van het CS gedefinieerd, vastgelegd en geïmplementeerd.

> Hierbij geldt dat minimaal jaarlijks de beveiliging van de P3-poort en de P4-poort wordt getoetst door een onafhankelijke instelling. Een penetratietest is een verplicht onderdeel van deze toets.

4.16 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4, B9 Klasse: 1 Borging: -

Verzoeken op de P4-poort van netbeheerders met betrekking tot aansluitingen die niet tot hun voorzieningsgebied behoren, dienen te worden geweigerd.

> Hierbij geldt dat in voorkomende gevallen contact dient te worden gezocht met de betreffende netbeheerder.

4.17 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3, B6 Klasse: 1Borging: DPM en BRS (P4)

Alle binnenkomende communicatie op alle poorten van het CS dient te worden gecontroleerd om correctheid en validiteit vast te stellen alvorens de communicatie wordt geaccepteerd.

> Hierbij geldt dat het CS van ieder apparaat (via P3) of van derden (via P4) geen communicatie buiten een per poort gedefinieerde, beperkte set van toegestane berichten dient te accepteren.

4.18 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B3 Klasse: 1 Borging: -

Er dient slechts een beperkt aantal rollen te zijn gedefinieerd op de P4-poort waarbij voor elk van deze rollen een beperkte set van toegestane communicatie en type berichten (opdrachten) dient te zijn gedefinieerd.

> Hierbij geldt dat toegestane communicatie met ODA's zich dient te beperken tot enkel het opvragen van meetdata.

4.19 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4, B11 Klasse: 0 Borging: -

De netbeheerder dient processen te hebben gedefinieerd, vastgelegd en geïmplementeerd om verdachte en niet-correcte communicatie van zowel apparaten (via P3) als van derden (via P4) te registreren, beoordelen en om passende actie te ondernemen.

Hierbij dient verdachte en niet-correcte communicatie (‘anomaliedetectie’) van zowel apparaten (via P3) als van derden (via P4) gesignaleerd en gelogd te worden.

4.20 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B2, B6 Klasse: 4 Borging: -

Er dient een maximum gesteld te zijn aan het aantal opdrachten dat per dag door het CS via de P4-poort geaccepteerd wordt voorzover deze opdrachten de doorlaatwaarde van meters verminderen, waaronder schakelopdrachten.

Hierbij geldt dat dit aantal ligt in de orde van 0,05% per dag van het totaal aantal aansluitingen van de netbeheerder.

Hierbij geldt dat het centraal systeem het maximum aantal schakelopdrachten dat per dag binnenkomt dient te herkennen, blokkeren en rapporteren aan de netbeheerder wanneer van toepassing.

Bovendien geldt dat er een proces dient te zijn gedefinieerd, vastgelegd en geïmplementeerd om in voorkomende gevallen contact op te nemen met de verzender van de opdrachten en om opheldering te vragen. Pas daarna kan, op basis van het vier-ogenprincipe, de blokkering worden opgeheven.

4.21 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4,B6 Klasse: 1 Borging: -

Netbeheerder dient processen ten aanzien van sleutel- en wachtwoordbeheer te hebben gedefinieerd, vastgelegd en geïmplementeerd.

Hierbij geldt dat bijvoorbeeld een aparte 'cryptoserver' wordt ingericht die de volgende processen en operaties ondersteunt:

- ontsleuteling en authenticatie van binnenkomende berichten van apparaten;
- versleuteling en authenticatie van uitgaande berichten aan apparaten;
- importeren van initiële fabriekssleutels van nieuwe meters
- beheer van beveiligingssleutels, waaronder die voor P2-encryptie, P3-encryptie ('end-to-end')
- beheer van (overige) metersleutels, waaronder mogelijke 'masterkeys'
- beheer van wachtwoorden (waaronder P0-wachtwoorden); en
- beheer van logingegevens.

Het ontsleutelen en inladen van initiele fabriekssleutels in de cryptoserver dient enkel mogelijk te zijn via een geautomatiseerd en beveiligd proces zonder tussenkomst van personen, of met handelingen van meerdere personen.

Hierbij geldt dat bij uitbedrijfname of kwijtraken (door bijvoorbeeld diefstal) van een meter of dataconcentrator de voor communicatie noodzakelijke sleutels en wachtwoorden in het CS op non-actief worden gezet of worden verwijderd.

Toegangsrechten voor de mastersleutels van apparaten dienen maximaal ingeperkt te zijn, bij voorkeur beperkter dan voor andere sleutels en wachtwoorden.

4.22 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B4,B6 Klasse: 3 Borging: -

Netbeheerder dient voor sleutel- en wachtwoordwijzigingen procedures te hebben gedefinieerd, vastgelegd en geïmplementeerd welke robuust zijn tegen initieel mislukte sleutelwijzigingen. Oude sleutels en wachtwoorden dienen na geconstateerde succesvolle vervanging niet meer te worden geaccepteerd.

Als voorbeeld zou het CS oude sleutels niet direct na wijziging vernietigen of op non-actief kunnen zetten voordat tenminste eenmaal succesvol is gecommuniceerd op basis van de nieuwe sleutels.

Sleutels dienen de cryptoserver nooit onbeveiligd te verlaten.

4.23 ISO: 12 Verwerving, ontwikkeling en onderhoud … Doel: B10 Klasse: 2 Borging: -

Netbeheerder dient te borgen dat leveranciers van cryptofunctionaliteit de technische hulpmiddelen en procedures leveren om veilig te kunnen backuppen en, wanneer nodig, te kunnen herstellen.

In geval van gebruik van een cryptoserver geldt bovendien dat backups versleuteld moeten zijn alvorens deze de cryptoserver verlaten.

Alle handelingen ten aanzien van cryptografische functionaliteit dienen te worden gelogd waarbij toegang tot de logging afgeschermd is voor medewerkers met (directe) toegang tot deze functionaliteit.

7. Verklarende woordenlijst

7.1 Afkortingen

AES	Advanced Encryption Standard
APN	Access Point Name
BRS	Business Requirements Specification (BRS) van EDSN, eisen aan de P4-poort (zie ook DPM).
CBP	College Bescherming Persoonsgegevens
CS	Centraal Systeem
DC	Dataconcentrator
DoS	Denial of Service
DPM	Detail Proces Model (DPM) van EDSN, eisen aan de P4-poort (zie ook BRS)
DSMR	Dutch Smart Metering Requirements
EDGE	Enhanced Data Rates for GSM Evolution
EDSN	Energie Data Services Nederland, uitvoerend orgaan van de NEDU
GPRS	General Packet Radio Service
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
NEDU	Nederlandse Energie Data Uitwisseling, platform voor organiseren data-uitwisseling tussen energiebedrijven en meetverantwoordelijken
NTA	Nederlandse Technische Afspraak
ODA	Onafhankelijke Diensten Aanbieder
pgUSM	ProjectGroep Uitrol Slimme Meters
PLC	Power Line Communication
RNBG	Regionale NetBeheerder Gas
SIM	Subscriber Identity Module
SLA	Service Level Agreement
UMTS	Universal Mobile Telecommunications System
WBP	Wet Bescherming Persoonsgegevens

7.2 Definities

Anomaliedetectie	Het gebruik van bekende of verwachte patronen om afwijkingen te detecteren (met name in communicatie over een netwerk) met als doel mogelijke beveiligingsaanvallen te herkennen.
Apparaten	Meters en dataconcentrators
Applicatieniveau	Het hoogste niveau in een stapeling van gelaagde netwerkprotocollen (zoals in het zogenaamde 'OSI referentiemodel'). Op dit niveau krijgt data betekenis, lagere niveaus hebben bijvoorbeeld betrekking op het voltage gebruikt om informatie over te dragen over een koperen draad.
Backdoor	Toegangsmogelijkheid tot een systeem of netwerk dat de formele beveiligingssystemen omzeilt.
Bericht	Data verstuurd over een communicatieverbinding.
Beveiligd	Authenticiteit, vertrouwelijkheid en versheid kunnen vaststellen
Commando	Een opdracht aan een apparaat of systeem. Een commando kan als (onderdeel van) een bericht worden verstuurd.
Datacommunicatie-leverancier	Partij anders dan de netbeheerder die een deel van de datacommunicatie in de slimme-meterinfrastructuur verzorgt.
Denial-of-Service-aanval	Poging om een systeem onbereikbaar te maken, bijvoorbeeld door het sturen van een overvloed aan (foutieve) instructies.
Dienst	Een samenhangend gedeelte van de functionaliteit van een apparaat of toepassing die via een interface ter beschikking wordt gesteld. Voorbeelden van diensten zijn het updaten van firmware op een apparaat of het voeren van een spraakgesprek op een GSM netwerk.
Doorlaatwaarde	Maximaal toegestaan vermogen dat (door een meter) wordt doorgelaten aan een huishouden of bedrijf
End-to-end beveiliging op applicatieniveau	Beveiliging van communicatie tussen twee applicaties, waarbij de beveiliging pas vervalt vanaf een punt binnen de applicatie. De beveiliging zelf is weer een combinatie van maatregelen zoals encryptie en authenticatie
Energiebedrijven	Netbeheerders en energieleveranciers
Fabriekssleutel	Beveiligingssleutel die door de fabrikant in de meter wordt gezet voordat deze aan de netbeheerder wordt geleverd.
Gebruikersnaam	Unieke tekenreeks gebruikt ter identificatie van een gebruiker (of apparaat).
Informatie voorziening	Alle processen, gegevens en informatiesystemen, inclusief de technische infrastructuur die verbonden is met het automatisch verwerken van bedrijfsgegevens.
Inloggegevens	Combinatie van bijvoorbeeld een gebruikersnaam en wachtwoord, ter authenticatie van (meestal natuurlijke) personen

Klant	Persoon met een (slimme) meter.
Knijpen	Het beperken van de doorlaatwaarde van de elektriciteitsaansluiting.
Meshed RF	Draadloos netwerk tussen meters waarbij berichten langs verschillende routes over meerdere naburige meters worden uitgewisseld met een centraal verzamelpunt (dataconcentrator)
Masterkey	Niet-wijzigbare, door leverancier geïnstalleerde sleutel, welke nodig is voor wijzigen van andere sleutels of wachtwoorden.
Metersleutel	Een door de netbeheerder bepaalde sleutel die uniek is per meter.
Netbeheerder	Onafhankelijk (nuts)bedrijf dat een energietransportnetwerk beheert. In deze documenten wordt met 'netbeheerder' altijd een 'regionale netbeheerder' bedoeld, en dus niet de (landelijke) netbeheerder van het hoogspanningsnet.
Schakelen	Het af- en aanschakelen van de energievoorziening van een of meer klanten. Dit kan zowel de elektriciteits-, als gasaansluiting betreffen, of eventueel andere via P2 gekoppelde aansluitingen waaronder water.
Sessiesleutel	Beveiligingssleutel met een unieke waarde die aan het begin van een sessie wordt bepaald en slechts tijdens de duur van die sessie wordt gebruikt.
Sleutel	Tekenreeks welke gebruikt wordt voor encryptie (versleuteling) van berichten. Afhankelijk van de gebruikte encryptie is deze enkel bekend bij de verzendende en ontvangende partij (symmetrische encryptie) of deels bekend aan de ontvangende partij en deels bij alle verzendende partijen (asymmetrische encryptie)
Vier-ogenprincipe	Voor kritieke handelingen is de instemming en actieve inbreng van ten minste 2 personen nodig. Voorbeeld: één iemand maakt opdracht aan, één iemand keurt deze vervolgens goed.
Wachtwoord	Geheime tekenreeks welke gebruikt wordt om een geclaimde identiteit (in de vorm van een gebruikersnaam) te verifiëren (ook wel: authenticatie). Het wachtwoord dient uitsluitend bekend te zijn bij de houder van de identiteit en bij de controleur van de identiteit.