Adviesrapport ICT-beveiliging in de Zorg

Ministerie van VWS

Interpay

16 oktober 2006

Adviesrapport ICT-Beveiliging in de Zorg

Ministerie van VWS

Interpay

Datum	16 oktober 2006
Auteur(s)	R.A. van Erk, J.G. van Dongen
Project Manager	Drs. H.J.W.M. Luijks

Inhoud

1 Introductie

Onder regie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is begin 2006 het Landelijk Schakelpunt voor de zorgsector opgericht. Het schakelpunt regelt onder meer de veilige, actuele elektronische uitwisseling van patiënteninformatie tussen alle partijen in de zorg.

Een geruisloos functionerend Landelijk Schakelpunt is een noodzakelijke voorwaarde voor de landelijke invoering van het Elektronisch Medicatie Dossier (EMD) en het elektronische Waarneem Dossier Huisartsen (WDH), de eerste hoofdstukken van een landelijk Elektronisch Patiënten Dossier (EPD).

De minister van VWS heeft besloten om in 2005 de eerste stappen te zetten voor de realisatie van het landelijke Elektronische Patiënten Dossier. In samenwerking met het agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), het Nationaal ICT Instituut in de Zorg (NICTIZ) en de betrokken branche- en koepelorganisaties in de zorgsector is het ministerie gestart met de invulling van het EPD.

Het belang van beveiligingsbewustzijn en beveiligingsniveau op bestuurlijk en technisch niveau vormt voor het ministerie aanleiding om in gesprek te komen met partijen die over de expertise beschikken om hen hierin te adviseren. In dit kader vond op 9 februari 2006 een gesprek plaats tussen de heer M. van Rijn (Directeur-Generaal Gezondheidszorg), mevrouw E. Maat (Hoofd Programma ICT in de zorg), de heer A. Kuijpers (Directeur Interpay) en de heer W. Machielse (Directieadviseur Interpay). Het hoge beveiligingsniveau van het Nederlandse betalingsverkeer, de in bijna veertig jaar opgebouwde ervaring in het betalingsverkeer en de expertise op het gebied van risk en security management van Interpay Nederland liggen hieraan ten grondslag. Centraal in dit gesprek stond de vraag in hoeverre Interpay het ministerie van VWS kan adviseren en of een vorm van samenwerking tussen beide partijen tot stand kan worden gebracht.

2 Doel, reikwijdte en resultaten adviesrapport

In de discussie over de beveiliging en privacy in de zorgsector wordt vaak verwezen naar het bankwezen en de wijze waarop daar het beveiligingsniveau en beveiligingsgedrag wordt gewaarborgd. Aan de Tweede Kamer is in november 2005 de toezegging gedaan om het bankwezen te benaderen. De aanwezige expertise wordt aangewend om de informatiebeveiliging in de zorgsector door te lichten en adviezen en/of aanbevelingen op te stellen waarmee een mogelijke achterstand van de beveiliging van de ICT in de zorgsector kan worden opgelost.

2.1 Doel

Op 15 februari 2006 heeft Interpay van mevrouw E.M. Maat de opdrachtomschrijving ontvangen.
De opdracht luidt als volgt: "het verkrijgen van gemeenschappelijk inzicht in de huidige mate van beveiliging van ICT in de zorgsector in relatie tot de invoering van het Elektronisch Patiënten Dossier (EPD) en maatregelen waarmee een mogelijke achterstand kan worden ingehaald, geborgd en gecontroleerd". Dit stelt het ministerie vervolgens in staat om het niveau van beveiliging van ICT in de zorgsector te bevorderen en de handhaving en bewaking te stimuleren.

De opdrachtomschrijving is op 19 juli aangescherpt. Het op te stellen adviesrapport dient voor een belangrijk deel te bestaan uit een beschrijving van de wijze waarop het bankwezen de beveiliging van het betalingsverkeer heeft ingericht en in hoeverre de beveiliging of maatregelen toepasbaar zijn in de zorgsector. Namens het ministerie waren mevrouw E.M. Maat en mevrouw E. Castelijns aanwezig, Interpay werd op 19 juli vertegenwoordigd door de heer H.J.W.M. Luijks, de heer R.A. van Erk en mevrouw K.T.J. Cardinaal – van de Laarschot.

2.2 Reikwijdte

Het ministerie van VWS heeft een zestal vragen voorgelegd aan Interpay:

- Kunt u een overzicht opstellen van relevante overeenkomstige ervaringen met de invoering van informatiebeveiliging vanuit Interpay?
- Kunt u een oordeel geven over het huidige beveiligingsniveau in de zorgsector?
- Kunt u een overzicht geven van de knelpunten van bestuurlijke, organisatorische, technische of juridische aard?
- Kunt u aanbevelingen doen om de mogelijke achterstand van beveiliging van ICT in de zorg op korte termijn in te halen?
- Kunt u aangeven welke wijzigingen noodzakelijk zijn op het gebied van organisatorische en bedrijfseconomische aard op het niveau van ziekenhuizen, huisartsenpraktijken en individuele zorgaanbieders?
- Kunt u aanbevelingen doen voor een moderne en efficiënte manier van toezicht op de naleving van beveiliging van ICT in de zorg?

Naar aanleiding van deze vragen heeft Interpay zich een beeld gevormd van het huidige beveiligingsniveau in de zorgsector. Zij heeft daartoe een beperkt aantal direct betrokkenen in de zorgsector geïnterviewd. Vervolgens beschrijft Interpay in dit adviesrapport de beveiligingsmaatregelen van het betalingsverkeer in de bancaire sector en een analyse van de bruikbaarheid ervan in de zorgsector.

2.3 Resultaten

Bij het hoofdstuk "Beleid, Naleving en Sancties" wordt ingegaan op welke wijze Interpay verplicht is om zich te houden aan bestaande regelgeving en op welke wijze hieraan een

invulling wordt gegeven.

Het hoofdstuk "Escalatie en Communicatie" gaat in op de werkwijze die Interpay hanteert bij grootschalige interbancaire problemen voor wat betreft de continuïteit van de bedrijfsvoering, de integriteit van het betalingsverkeer en de afstemming daarvan.

Het hoofdstuk "Certificeren en toezicht" geeft het model weer dat wordt gebruikt om te komen tot certificatie van betaalapparatuur. Daarnaast geeft dit hoofdstuk weer welke acceptatiecriteria kunnen worden gesteld, hoe hieraan door middel van deelcertificatie op een veilige en betrouwbare manier invulling wordt gegeven en op welke manier het toezicht wordt ingevuld.

Het hoofdstuk "Keymanagement, organisatie en apparatuur" beschrijft hoe Interpay omgaat met het sleutelbeheer van betalingsapparatuur en op welke wijze deze organisatorisch zijn ingebed.

Het hoofdstuk "Preventie, detectie en repressie" is gebaseerd op het naleven van regels en het voorkomen en bestrijden van fraude in de breedste zin van het woord.

3 Management summary

Interpay is als financieel dienstverlener binnen het Nederlandse betalingsverkeer gevraagd om ervaringen en mogelijke parallellen met de zorgsector op het gebied van informatiebeveiliging te delen met het ministerie van VWS. Dit heeft geresulteerd in een onderzoek dat van 1 juni 2006 tot 15 september 2006 is uitgevoerd. Gedurende dit onderzoek zijn gesprekken gevoerd met een representatieve afspiegeling vanuit de zorgsector, zoals vertegenwoordigers van zorginstellingen en zorgverleners en architecten welke oplossingen aandragen voor de invoering van een EPD binnen de zorgsector.

De methode die is gebruikt om tot de conclusies van dit rapport te komen is gebaseerd op interviews en desk research, gevoed met de praktische ervaringen die Interpay heeft opgedaan met informatiebeveiliging.

Gelet op bovenstaande is het rapport dan ook geschreven vanuit het perspectief informatiebeveiliging. Onderwerpen die in dit rapport aan de orde komen zijn enerzijds geselecteerd op basis van enige overeenkomst met de zorgsector en anderzijds omdat zij stof tot nadenken geven die kunnen leiden tot implementatie ervan.

Het hoofdstuk "Certificeren en Toezicht" vormt naar de mening van Interpay de kern van het adviesrapport omdat hier de basiselementen en bouwstenen liggen voor een goed en gedegen landelijk werkend EPD. Indien aan deze basis afbreuk wordt gedaan kan dit ondanks andere technische toepassingen nooit leiden tot een EPD dat door het veld als veilig en betrouwbaar wordt beschouwd. Dit punt is cruciaal, vooral omdat patiënten exact willen weten hoe wordt omgesprongen met deze privacy gevoelige informatie en de elektronische opslag en uitwisseling ervan.

3.1 Algemeen beeld

Gedurende het onderzoek is gebleken dat bij de invoering van de hoofdstukken voor een landelijk EPD de beleving omtrent informatiebeveiliging zeer divers is. Bij de zorgverleners die enkelvoudig werken zoals de huisartsen is de verwachting dat zij te maken krijgen met ingrijpende wijzigingen om medische gegevens op een veilige manier te verwerken en uit te wisselen. De huidige eisen die worden gesteld zijn van dien aard dat deze groep er niet aan ontkomt aansluiting te zoeken bij een ASP, om te voldoen aan bijvoorbeeld de beschikbaarheidseis.

De apothekers, al dan niet geclusterd en ontsloten via overkoepelende instanties, staan voor wat betreft de invoering van het EMD voor de uitdaging om hun thans werkende (apotheek)applicaties gecertificeerd en opgenomen te krijgen in de landelijk beschikbare en toegankelijke applicaties via het LSP.

De groep van grote zorginstellingen (de ziekenhuizen) geven voor een deel de indruk nog onvoldoende budget ter beschikking te stellen om een en ander te kunnen regelen. De meest essentiële technische beveiligingsmaatregelen als virusscanners en firewalls zijn doorgaans aanwezig. Met name wordt thans nog onvoldoende aandacht besteed aan het belang van cultuur- en gedragsverandering en de noodzakelijke organisatorische maatregelen en procedurele aspecten om te kunnen voldoen aan de gewenste normen en standaards. Naast het stimuleren van investeren in informatiebeveiliging is ook een andere beveiligingsattitude noodzakelijk om een invoering van delen van het EPD succesvol te laten verlopen.

3.1.1 EPD beleving

De beleving van het onderwerp EPD is divers, dit wordt gevoed door een eilandgevoel bij de

diverse belanghebbende partijen. Iedere partij interpreteert het begrip EPD verschillend. Voor de bedrijfsvoering wordt vooral gekeken naar de ontwikkelingen richting 3e generaties EPD's die klinische paden ondersteunen. Dit in tegenstelling tot de huidige lokale EDP's die vooral als kijkdozen worden gezien. In de huidige situatie ontbreken duidelijke standaards voor de codering binnen de applicaties. Gegevens van de huidige lokale EPD's zijn veelal niet gestandaardiseerd en niet landelijk uitwisselbaar.
Een ander probleem voor zover het de medische gegevens betreft is de presentatie naar de patiënt die momenteel onbegrijpelijk is.

Een echt landelijk EPD wordt door de zorginstellingen niet binnen vijf jaar verwacht. Kenmerkend is de verwachting dat softwarefabrikanten gezien de beperkte Nederlandse markt niet in staat zullen zijn om volgende generaties EPD's te ontwikkelen.

Het toezicht op de invoering van een EPD, waarbij de diverse voorschriften en wettelijke kaders dienen te worden gevolgd, geeft voor de huidige toezichthouder in de gezondheidszorg een extra taak doordat nu ook specifiek gelet moet worden op ICT-onderwerpen. Dit is voor de Inspectie voor de Gezondheidszorg in haar rol als toezichthouder een zware taak aangezien zij daar thans niet voor is geëquipeerd.

3.2 Cultuur

Binnen de zorgsector wordt ICT veelal gezien als een ondersteunend proces. Binnen de bancaire wereld is ICT van begin af aan het uitgangspunt geweest en kan men spreken van primaire processen waarvan de bedrijfsvoering volledig afhankelijk is. De zorgsector dient op zorgvuldige wijze een cultuuromslag te maken waarbij ook wordt ingezien dat ICT een onderdeel is van het primaire proces voor de bedrijfsvoering.

Ondanks het feit dat de cultuurverschillen tussen de bancaire wereld en de zorgsector groot zijn, vallen er voldoende parallellen te onderkennen die een advies rechtvaardigen.

3.3 Conclusies en adviezen

In deze paragraaf zijn de belangrijkste aanbevelingen opgenomen. In het bijzonder binnen het hoofdstuk "Certificeren en Toezicht" worden ook andere aanbevelingen gedaan.

3.3.1 Normering

Het gebruik van instrumenten voor de informatiebeveiliging - specifiek de NEN-7510 norm, zijnde de voor de zorgsector toegespitste en afgeleide richtlijnen van de algemeen in gebruik zijnde Code van Informatiebeveiliging - is een kwaliteitsaspect die door het veld is gemaakt en geaccepteerd. Ondanks het draagvlak bij de theoretische totstandkoming van deze richtlijnen blijft de naleving in de praktijk achter. Hier dient een behoorlijke inhaalslag te worden gemaakt.

Interpay beveelt aan:

a) het gebruik van de NEN-7510 monitor binnen de zorgsector meer te propageren. Met behulp van deze zelfanalyse zal binnen het veld een realistischer beeld worden gecreëerd van de (on)volkomenheden van de eigen organisatie;

b) de normerende instantie NEN voor het veld controleerbare en toetsbare checklijsten te laten ontwikkelen die op dezelfde wijze gebruikt kunnen worden voor zorgverleners waar de NEN7510 monitor te grootschalig is voor gebruik.

3.3.2 Eisen

Vanuit het NICTIZ zijn de eisen aan te koppelen systemen en netwerken door middel van GBZ

en ZSP duidelijk geconcretiseerd. In dit kader moeten zij gezien worden als lokale eisen. Deze eisen zijn een verder uitgewerkte vertaling van de geaccepteerde NEN-normering, specifiek aangevuld om te kunnen werken met het Landelijk Schakel Punt. Specifieke eisen voor systemen en netwerken zijn noodzakelijk om eenduidigheid in onderlinge communicatie, transport van gegevens en de mate van beveiliging te bewerkstelligen. Indien deze acceptatiecriteria volledig worden nageleefd lijkt niets een verdere succesvolle implementatie van de diverse EPD hoofdstukken meer in de weg te staan. Onduidelijker is het beeld dat naar boven komt in het licht van landelijke eisen die gesteld moeten worden aan de volledige landelijke infrastructuur voor wat betreft dezelfde criteria.

Interpay beveelt aan:

c) een onafhankelijk partij een risicoanalyse te laten verrichten naar de kwetsbaarheden bij de implementatie van criteria, zoals die genomen zijn bij de werking van een landelijke infrastructuur voor het EPD.

3.3.3 Certificering

Het certificeren volgens de GBZ- en ZSP-eisen is een complex geheel omdat er een grote diversiteit aan GBZ systemen is met daarop draaiende zorgondersteunende applicaties. Ook zijn veel GBZ-systemen op de een of andere manier gekoppeld aan andere systemen. Hiermee is het volledig voldoen aan de GBZ eisen een langdurig en moeizaam proces.

Interpay beveelt aan:

d) een scheiding aan te brengen in het certificeringmodel waarbij een onderscheid wordt gemaakt tussen een beveiligingsdeel(verplicht) en een functioneel deel(deels verplicht).

3.3.4 Organisatorische aspecten

In het kader van de zware taak voor de Inspectie voor de Gezondheidszorg (mede gelet op de 'roep' voor een loketfunctie vanuit de patiënt en de noodzaak van een certificerende instantie) is het van belang om deze rollen te onderkennen en gescheiden in het leven te roepen, waarbij ieder orgaan verantwoording dient af te leggen aan het hoogste orgaan namelijk de Inspectie voor de Gezondheidszorg. Het is de ervaring van Interpay dat alleen door een duidelijke functiescheiding de kwaliteit van de zorgondersteunende systemen, het communicatiekanaal naar de patiënt en een onafhankelijke monitor binnen de zorgsector gewaarborgd kunnen worden.

Interpay beveelt aan:

e) het hoofdtoezicht op de invoering en naleving van de EPD voor wat betreft de ICT bij de Inspectie voor de Gezondheidszorg te leggen;

f) een onafhankelijke instantie te benoemen die rapporteert aan de Inspectie voor de Gezondheidszorg en als taakstelling krijgt om een loketfunctie op te zetten als spreekbuis voor publieke zaken omtrent het EPD;

g) beleg het toezicht en het certificeren van de diverse GBZ en ZSP systemen bij een onafhankelijke instantie, die rapporteert aan de Inspectie voor de Gezondheidszorg.

3.3.5 Regio versus landelijk

Wanneer legacy systemen al zijn opgenomen in regio's ontstaan hieruit diverse functioneel goed werkende processen. Hoewel deze systemen thans nog niet voldoen aan de gestelde GBZ-eisen lijkt het niet raadzaam om aan de al opgebouwde functionaliteit voorbij te gaan. Hoewel er beveiligingsomissies zitten in de regionale versus landelijke functionaliteit verdient

het aanbeveling om de regio's het voortouw te laten nemen om uiteindelijk te groeien naar de landelijk afgesproken en geaccepteerde standaard. Een van de voornaamste beveiligingsomissies kan met een UZI-pas oplossing teniet worden gedaan.

Interpay beveelt aan:

h) de ingebruikname van de UZI-pas te versnellen door deze ook toe te passen binnen de regionale systemen.

De invoering van de diverse hoofdstukken van het EPD lijkt voor regionaal niveau eerder haalbaar dan voor landelijk niveau. Vooral omdat de diverse zorgverleners binnen de regio al hun systemen en/of processen op elkaar hebben afgestemd. De combinatie van regio en de daarin nu al geboden functionaliteit is een belangrijke motor voor een gefaseerde opbouw en betrokkenheid van alle deelnemers. Gelet op deze bevinding is een hybride oplossing die gefaseerd migreert naar een landelijke uniforme en gewenste situatie te prefereren.

Interpay beveelt aan:

i) NICTIZ het conceptuele idee van hybride systemen binnen de regio's te laten omarmen.

3.3.6 Privacy versus betrouwbaarheid

Het algemeen belang, invoering van een landelijk EPD, waarbij medische gegevens op een betrouwbare wijze, via een landelijk netwerk veilig worden getransporteerd en uitgewisseld kent bij de beleving van velen een onderbelicht privacyaspect.
Naar de mening van Interpay wordt op dit privacyaspect teveel de nadruk gelegd en is de betrouwbaarheid van de opgeslagen medische gegevens evenals het transmuraal muteren een nadrukkelijker aspect waar aandacht aan dient te worden geschonken.

Interpay beveelt aan:

j) de opslag en het transport van medische patiëntengegevens zoals bedoeld bij het EPD voor de vertrouwelijkheid van de gegevens te vercijferen;

k) voor de betrouwbaarheid van de gegevens deze te voorzien van een uniek kenmerk(hash).

3.3.7 Loketfunctie

Het EPD-model kent voorzieningen waarbij patiënten de mogelijkheid krijgen om de eigen patiëntgegevens al dan niet toegankelijk te laten zijn voor hulpverleners. Met die gedachte is het voor het welslagen van de invoering van een landelijk EPD van groot belang dat zoveel mogelijk patiënten hieraan meewerken. Het risico van afhaken van een patiënt bij het EPD is evident aanwezig wanneer deze zich niet begrepen voelt of zich niet in voldoende mate kan uiten bij communicatie omtrent zijn elektronische dossier. Los van de wet op de EPD dient er een voorziening te worden gecreëerd die de patiënt de mogelijkheid biedt om zich te uiten en te laten informeren c.q. vertegenwoordigen in deze materie. Binnen de huidige regelingen is het buitengewoon lastig om precies te weten bij welke klacht of vraag welke weg bewandeld dient te worden. Het lijkt erop dat de toegankelijkheid voor de individuele patiënt/consument onvoldoende is belicht.

Interpay beveelt aan:

l) de publiciteit omtrent de invoering van de diverse hoofdstukken van het landelijke EPD te kanaliseren via een klankbordgroep die publiekelijk toegankelijk is en namens het publiek kan onderhandelen.

3.3.8 *Invoering informatiebeveiliging*

De diverse banken zijn gegroeid naar een volwassen cultuur waarbij er voor is gezorgd dat de functionaliteit van het betalingsverkeer goed werkt en waarna het toetsbaar maken van de beveiligingseisen onderdeel is geworden van de architectuur. Op deze manier maakt informatiebeveiliging integraal deel uit van de huidige business processen. Naarmate het belang, is beveiliging een steeds prominentere plaats gaan innemen.
De beveiligingseisen voor de authenticatie via de UZI pas, de wijze van autoriseren, de transportbeveiliging via het LSP en de logging op het LSP maken dienoverkomstig onderdeel uit van de architectuur.

3.3.9 *Beveiligingsbewustzijn*

Beveiligingsbewustzijn wordt nog steeds toegedicht aan ICT personeel. De ervaring leert dat bewustzijn niet alleen wordt gecreëerd door het stellen van regels maar ook met kennisoverdracht, cultuur en gedrag. Hierbij kan openheid en transparantie worden bereikt door 'open' te communiceren waarbij rapportages en trendanalyses instrumenten zijn om ervaringen te onderbouwen en daarnaast om op deze processen te sturen.

Momenteel wordt voor Zorginstellingen gebruik gemaakt van zogenoemde DBC's om de kwaliteit en de kosten van de zorgsector te meten. Interpay is van mening dat de visie gericht dient te zijn op het beheersbaar houden van de kosten in de gezondheidszorg zonder de kwaliteit te verliezen. Dit kan mede bereikt worden door naast binnen een zorginstelling te sturen op de DBC's ook aandacht te schenken aan het landelijk publiceren van de kwaliteit en prijs van DBC gegevens. Betrouwbaarheid van de DBC gegevens is een van de kwaliteitsaspecten. Deze betrouwbaarheid is een van de zaken die via technische informatiebeveiligingsmaatregelen kan worden afgedwongen. Naast het belang van de privacy/vertrouwelijkheid is juist dit aspect wezenlijk voor het gebruik in met name de primaire processen. De specialist/behandelaar is sterker dan voorheen afhankelijk van de juistheid, tijdigheid en volledigheid van de opgevraagde gegevens, juist omdat deze gegevens vanaf meerdere plekken in het land verkregen kunnen zijn. Vanuit deze visie kan een business case voor de zorgsector worden ontwikkeld door de zorginstellingen. Hierbij wordt informatiebeveiliging er onlosmakelijk mee verbonden en kan men zich met trots meten met de collega zorginstellingen.

Interpay beveelt aan:

m) onderlinge concurrentie door middel van het publiceren van DBC gerelateerde kerngegevens en de daarbij behorende kostprijs (die mede bepaald is door de betrouwbaarheid van patiënt- en daaraan gerelateerde medische gegevens), per zorginstelling te overwegen.

4 Beleid, Naleving en Sancties

Bij het hoofdstuk "Beleid, Naleving en Sancties" wordt ingegaan op welke wijze Interpay verplicht is om zich te houden aan bestaande regelgeving en op welke wijze hier een invulling aan wordt gegeven.

4.1 Toezichthouder

De Nederlandsche Bank (DNB) is verantwoordelijk voor het bewaken van de financiële stabiliteit. Zo stelt DNB normen en eisen op voor de financiële sector en houdt zij toezicht op de naleving ervan. De normen en eisen voor de financiële sector zijn benoemd in de Regeling Organisatie en Beheer (ROB) en het toetsingskader Business Continuïteit Planning (BCP). De ROB-eisen zijn door de verschillende financiële instellingen in het beleid opgenomen en vertaald naar concrete maatregelen. Binnen Interpay heeft zich dit voor wat betreft informatiebeveiliging vertaald naar een Handboek Beveiliging dat is afgeleid van de internationaal erkende Code voor Informatiebeveiliging.

Naast het stellen van normen en eisen toetst DNB de financiële instellingen op het naleven van de geformuleerde eisen door het uitvoeren van audits.

4.1.1 Toezichthoudende rol

In dit onderdeel wordt dieper ingegaan op de toezichthoudende rol op het Nederlandse betalingsverkeer. Onderdelen als doelstelling, kaders, reikwijdte en rollen van belanghebbenden worden hierin uiteengezet evenals een verwijzing naar diverse informatiebronnen.

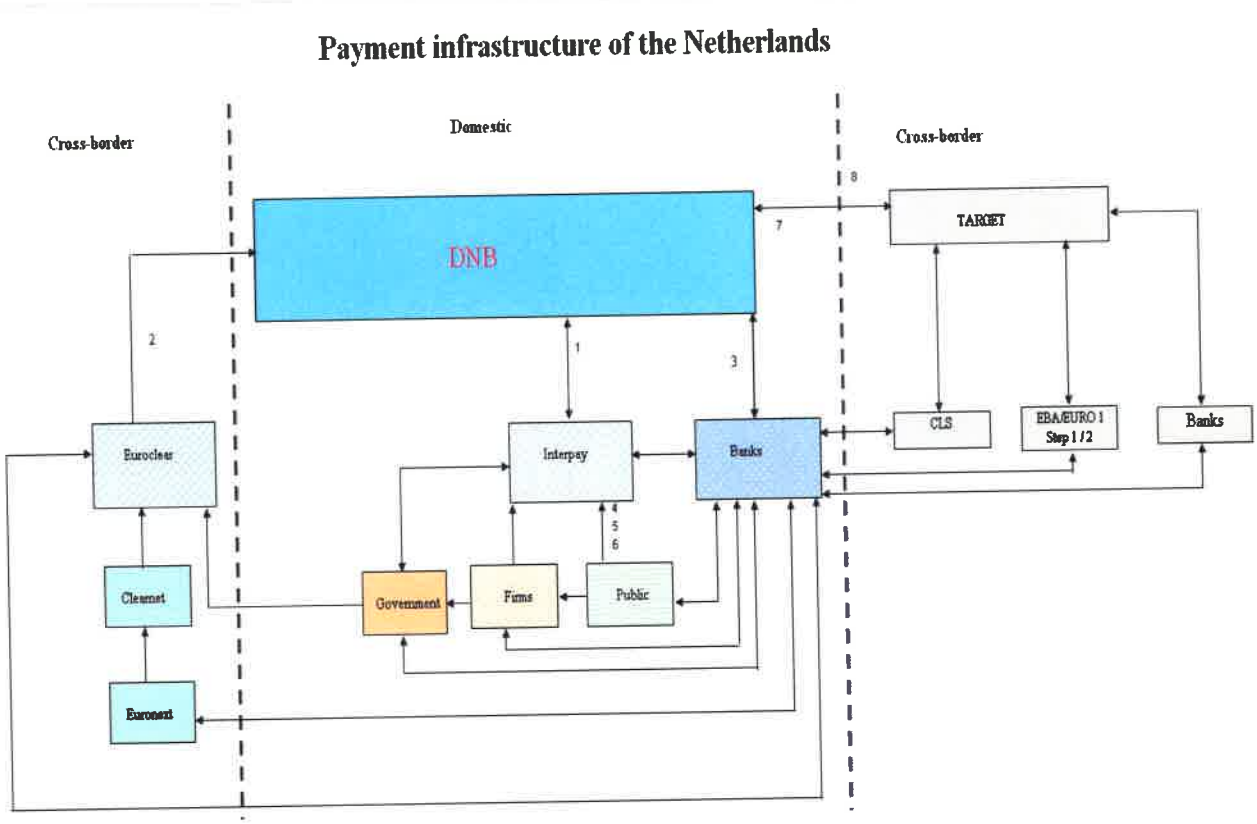
4.1.2 Doelstelling

Een stabiel financieel stelsel is sterk afhankelijk van een veilig en betrouwbaar betalingsverkeer. Iedereen moet probleemloos kunnen betalen met munten en bankbiljetten, maar ook met zijn chipknip, pinpas en creditcard, of via het internet.
De miljoenen transacties die banken dagelijks uitvoeren, moeten veilig en zonder storingen verlopen.
De doelstelling van een toezichthoudende rol is het bewaken van de veiligheid en betrouwbaarheid van het betalingsverkeer, zodat een stabiel financieel stelsel gegarandeerd is.
Om de doelstelling te kunnen behalen en behouden heeft de toezichthouder voor zichzelf een duidelijk gebied afgekaderd.

4.1.3 Kaders en reikwijdte

Om de rol als toezichthouder te kunnen vervullen, moet inzichtelijk zijn wat de grenzen zijn. Deze grenzen kunnen worden afgebakend door enerzijds de reikwijdte te bepalen en anderzijds de kaders op te stellen en te verankeren.

Onderstaand overzicht "Payment infrastructure of the Netherlands" geeft een beeld van het gebied waarin de toezichthouder een rol speelt.



Het bepalen van deze reikwijdte geeft onmiddellijk een goed beeld van de grenzen en mogelijke afhankelijkheden in binnen- en buitenland (crossborder).
Naast het feit dat de infrastructuur en koppelingen tussen de infrastructuren in beeld gebracht zijn, zijn ook op hoofdlijnen de belangrijkste partijen benoemd.
Vervolgens dienen partijen ook te beschikken over kaders waarmee ze kunnen werken en waarmee de toezichthouder zijn rol kan uitoefenen.
De kaders komen voort uit nationale en Europese wet- en regelgeving en na afstemming met betrokken partijen.

De Nederlandsche Bank (DNB) als toezichthouder kent de volgende taken:

- Het verlenen van toegang tot het financiële stelsel middels het afgeven van vergunningen;
- Het opstellen en bijhouden van toetsingskaders met normen en eisen;
- Het toetsen op de naleving van geformuleerde toetsingskaders.

4.1.4 Instrumenten

Om haar taak als toezichthouder te kunnen uitoefenen, heeft de DNB een aantal instrumenten ontwikkeld. De instrumenten zijn dusdanig van opzet, dat zij niet alleen het behoud en onderhoud van het betalingsverkeer dienen, maar ook de toetreding en uittreding.

Om toegang te verkrijgen tot het betalingsverkeer dient men een vergunning aan te vragen bij DNB. Bij het verkrijgen van een vergunning voldoet men in voldoende mate aan gestelde eisen/normen om aan het betalingsverkeer te kunnen deelnemen.

Niet alleen bij toetreding stelt men eisen/normen, maar ook tijdens deelname aan het betalingsverkeer. Deze eisen/normen zijn o.a. benoemd in de Regeling Organisatie en Beheersing (ROB) en het toetsingskader Business Continuïteit planning (BCP).

De ROB regeling betreft de beheersing van risico's die instellingen lopen, daarbij inbegrepen de risico's die voortvloeien uit het niet of onvoldoende naleven van regelgeving en inbreuken op de integriteit van de bedrijfsvoering. Het gaat hierbij om de materiële risico's, dat wil zeggen risico's die de financiële prestaties, financiële positie, continuïteit of reputatie van de instelling in belangrijke mate kunnen aantasten. Bij dit alles is het uitgangspunt dat de verantwoordelijkheid voor het opstellen van procedures, regels en normen, de inbedding hiervan in de bedrijfsprocessen en het toezicht op de werking en de naleving bij de instelling zelf ligt. Het bestuur van de instelling ziet er op toe dat dit in de praktijk gerealiseerd wordt. De regeling spitst zich toe op de elementen risicobeheersing, organisatorische maatregelen, informatie en communicatie en toetsing, beoordeling en bijstelling.

Het toetsingskader Business Continuïteit planning (BCP) gaat in op factoren die een bedreiging kunnen vormen voor het ongestoord functioneren van het betalingsverkeer. In het BCP zijn uitgangspunten geformuleerd en wordt aandacht besteed aan continuïteitsmaatregelen, crisisorganisatie, communicatie, het hebben van diverse continuïteitsplannen en het testen van deze plannen.

De financiële instellingen nemen de eisen/normen op in hun policies /beleid. Het beleid wordt in de financiële organisatie vertaald naar maatregelen.

Naast het (op)stellen van eisen/normen, toetst de DNB de financiële instellingen op het naleven ervan. Het toetsen gebeurt in veel gevallen in samenwerking met een interne audit afdeling van de instelling. Bij het toetsen zal men letten op of de genomen maatregelen voldoen aan gestelde eisen/normen.

4.1.5 Rollen van belanghebbende

Financiële instellingen

- De financiële instellingen dragen bij aan het formuleren van eisen/normen;
- De financiële instellingen dragen zorg voor het implementeren van voorgestelde maatregelen;
- De financiële instellingen zijn verantwoordelijk voor de werking van geïmplementeerde maatregelen.

Interne audit afdeling

Dit is de afdeling die belast is met de toetsing en beoordeling van de organisatie-inrichting en het beheersingsmechanisme. Deze functie is onafhankelijk van de lijn en staat los van de interne controlemaatregelen die in de diverse onderdelen van de onderscheiden bedrijfsprocessen zijn geïntegreerd. De interne auditfunctie ressorteert rechtstreeks onder de hoogste leiding van de instelling.

4.1.6 Toezichthoudende rol zoals deze is waargenomen in de zorgsector

Binnen de zorgsector is voor medische zaken een algemene rol weggelegd voor de Inspectie voor de Gezondheidszorg als bewaker van de kwaliteit van de volksgezondheid. Gedurende het onderzoek valt op dat er veel onduidelijkheden zijn wie de toezichthoudende rol voor wat betreft het EPD inneemt. Verwacht wordt dat de wet op de EPD hierin duidelijkheid verschaft. Wanneer gesproken wordt over toezichthouderschap wordt hieronder verstaan de controle op de juiste opzet, invoering en werking van de diverse onderdelen binnen een landelijk functionerende EPD.

4.2 Interbancair overlegorgaan geënt op informatiebeveiliging

De werkgroep Coördinatie Informatiebeveiliging (CIBEV) van de Nederlandse Vereniging van Banken (NVB) houdt zich bezig met de informatiebeveiliging van het Nederlandse betalingsverkeer. De CIBEV stelt "ledencirculaires" op. Hierin zijn technische afspraken

vastgelegd over de beveiliging van berichtenverkeer. De afspraken geven de banken implementatievrijheid, maar zijn nauwkeurig genoeg om een juist beveiligingsniveau voor de sector als geheel te waarborgen.

4.3 Sancties

Rules & Regulations spelen een belangrijke rol in het betalingsverkeer. Deze beschrijvingen geven duidelijk de rollen en verantwoordelijkheden weer. Credit card-maatschappijen als MasterCard Worldwide en Visa International maken er gebruik van. Zij hanteren uiteenlopende methodieken om te kunnen vaststellen of door betrokken partijen aan de Rules & Regulations wordt voldaan. Sanctionering kan tot stand komen nadat - via monitoring, self assessment of audits – is vastgesteld dat niet is voldaan aan één of meerdere regels. In veel gevallen bestaan sancties uit het opleggen van significante boetes en zelfs intrekken van de licentie.

5 Escalatie en Communicatie

Hoofdstuk "Escalatie en Communicatie" gaat in op de werkwijze die Interpay hanteert bij grootschalige interbancaire kwesties inzake de continuïteit van de bedrijfsvoering, de integriteit van het betalingsverkeer en de afstemming daarvan.

5.1 Continuïteit van de bedrijfsvoering

Interpay levert specifieke diensten ten behoeve van het bankwezen. Het wegvallen van of verstoring in de primaire dienstverlening van Interpay heeft niet alleen direct consequenties voor de banken, maar ook voor de Nederlandse economie. Daarmee heeft Interpay de directe verantwoordelijkheid om mogelijke dreigingen (intern en extern), verstoringen en incidenten te beheersen.

5.1.1 Crisis management Team en Escalatie

Doordat Interpay het grootste deel van het betalingsverkeer binnen Nederland regelt, heeft het niet functioneren van de primaire dienstverlening direct consequenties voor de klanten van Interpay maar ook voor de Nederlandse economie en samenleving. Het is dan ook de verantwoordelijkheid van Interpay om mogelijke dreigingen (intern en extern), verstoringen en incidenten te beheersen.

De spil in de beheersing is het Crisis Management Team (CMT) van de afzonderlijke instellingen, tezamen met voorbereide plannen en procedures. Het CMT komt, afhankelijk van de omvang en aard van een calamiteit, bijeen en beslist over het activeren van plannen en coördineert de activiteiten van betrokken teams. Daarnaast is het CMT verantwoordelijk voor juridische, personele, publicitaire en operationele aangelegenheden.

Een escalatie van het CMT kan op diverse manieren plaatsvinden. Extern vanuit de financiële sector middels de procedure beschreven in "het rode boekje". Vanuit het ministerie van "binnenlandse zaken" en "justitie" beschreven in de procedure van de NCTb (Nationaal Coördinator Terrorismebestrijding). Vanuit de lokale overheid beschreven in de gezamenlijke rampenplannen. Intern vanuit de diverse maatregelen die ingevoerd zijn.

5.2 Integriteit van het betalingsverkeer

5.2.1 Inleiding

Bestrijden van fraude is binnen de Nederlandse financiële wereld sinds jaar en dag geen issue waarop wordt geconcurreerd. De samenwerking op dit punt wordt altijd gezocht, maatregelen worden waar mogelijk gezamenlijk genomen en kennis wordt gedeeld. De afdeling Brand Services / Fraud Control van Interpay heeft op een aantal terreinen al jarenlang een centrale rol.
In 1997 hebben de Nederlandse banken besloten tot het opstellen van het 'Draaiboek Crisisbeheersing'. Uitgangspunt vormt het feit dat banken álle fraude- en continuïteitsincidenten - met een interbancair karakter én grote impact - melden aan het Centrale Meldpunt dat banken bij Interpay hebben belegd. Het draaiboek bevat een opzet voor escalatie door het bijeenroepen van het Pré-Crisisteam, het Crisisteam en/of het Kernteam Communicatie, afhankelijk van aard en omvang van de crisissituatie.
De respectievelijke teams treffen maatregelen om de crisis het hoofd te bieden en eenduidige communicatie te bewerkstelligen.

5.2.2 Aanbevelingen voor de zorgsector

Zorg voor de totstandkoming van een expertgroep die richtinggevend kan werken om informatiebeveiliging in de zorg te structureren.

Mogelijk kunnen de overkoepelende organisaties (zoals NFG, VNZ etc) al dan niet gezamenlijk zorgdragen voor een dergelijke expertgroep (zie ook de aanbevelingen voor het toezicht in het hoofdstuk Certificeren en Toezicht).
Er is geen overeenkomende gemeenschappelijke coördinerende organisatie, die zowel richtinggevend is voor de standaardisatie van informatiebeveiliging als voor het gezamenlijke beleid ten aanzien van informatiebeveiliging.
Wel besteden koepelorganisaties zoals b.v. KNMP, NFU, etc aandacht aan het beleid, maar niet structureel. Het NEN faciliteerde de totstandkoming van NEN7510, 7511 en 7512. De Inspectie voor de Gezondheidszorg is de toezichthoudende instantie, maar heeft niet de kwaliteiten ten aanzien van ICT en de capaciteit om een actieve rol te vervullen. NICTIZ stelt de normen op voor de landelijke uitwisseling, maar is niet structureel betrokken bij het informatiebeveiligingsbeleid in de zorgsector.
Interpay heeft niet gekeken hoe informatiebeveiliging is geregeld binnen de gehele Overheid, maar heeft dit beperkt tot de zorg. In analogie met het onderdeel in paragraaf 4.2 verdient het aanbeveling om een expertgroep op te zetten die richtinggevend kan werken om informatiebeveiliging in de zorg te structureren.

Formaliseer en centraliseer de afspraken over continuïteitsvoorzieningen
Volgens NEN7510 dienen zorginstellingen van het EPD continuïteitsvoorzieningen te treffen. Deze voorzieningen zijn echter niet gecentraliseerd verzameld en beschreven, zodat niet vaststaat wat deze voorzieningen zijn. Gelet op de invoering van een landelijk werkend EPD en elkaar ondersteunende onderdelen daarvan, is het noodzakelijk dat omwille van de continuïteit afspraken worden geformaliseerd. Hierbij valt te denken aan uitwijkscenario's die jaarlijks op effectiviteit worden getest en waar nodig bijgesteld.

Creëer een draaiboek crisisbeheersing
Gedurende het onderzoek is niet vast komen te staan of een landelijk werkend EPD ook voorziet in noodscenario's voor wat betreft crisissen. Een draaiboek crisisbeheersing voor de zorgsector kan uitkomst bieden bij een:

- aanval of inbraak op systemen of netwerken;
- compromittatie van patiënt gegevens;
- uitval LSP voor langdurige tijd;
- algemene verstoring voor langere tijd.

Om het draaiboek te kunnen activeren dient een aantal afspraken te worden gemaakt, onder andere over de randvoorwaarden voor het bijeenkomen van een crisisteam.

Het verdient aanbeveling om bij het opzetten van een crisisteam voor de zorg onderstaande aspecten mee te nemen in de voorbereidingen:

- Zorg voor één duidelijk en herkenbaar aanspreekpunt;
- Een goede 7x24 bereikbaarheid van dit aanspreekpunt is gewenst;
- Centraliseer alle beschikbare informatie bij dit aanspreekpunt;
- Beschrijf procedures in geval van een crisissituatie;
- In het draaiboek dienen tactische en operationele stappen te worden vastgelegd en geactualiseerd aangaande:
    - procedure met betrekking tot het in werking stellen;
    - naw-gegevens en telefoonnummers van betrokken functionarissen.

6 Certificeren en Toezicht

Het hoofdstuk aangaande "Certificeren en toezicht" geeft het model weer dat wordt gebruikt om te komen tot Certificatie van betaalapparatuur. Daarnaast geeft dit hoofdstuk weer welke acceptatiecriteria kunnen worden gesteld, hoe hieraan door middel van deelcertificatie op een veilige en betrouwbare manier invulling wordt gegeven en op welke manier het toezicht wordt ingevuld.

6.1.1 Inleiding

Naast een fysieke kaart maken winkels in Nederland gebruik van gecertificeerde betaalautomaten. Door certificering van betaalautomaten kunnen banken instaan voor de klant en het gebruik van de PINcode, een verplichting voor banken die deel uitmaakt van de Algemene Bankvoorwaarden. Het proces van certificering legt aan alle betrokken partijen uit de keten een inspanningsverplichting op.

Het certificeren van een betaalautomaat bestaat uit een aantal stappen:

- Indien een leverancier een nieuwe betaalautomaat op de markt wil brengen, dient hij voor het certificeren een verzoek in bij een interbancaire commissie (Klankbord Currence).
- De interbancaire commissie geeft de opdracht aan een gecertificeerd onderzoeksinstituut om de correcte werking van de hardware en software te onderzoeken.
- Indien de betaalautomaat aan de gestelde eisen voldoet, krijgt de leverancier toestemming om voor bepaalde tijd betaalautomaten door Interpay te laten personaliseren (dat wil zeggen: hem voorzien van cryptografische sleutels).
- Tijdens het proces van personaliseren van betaalautomaten wordt de software getoetst aan de onderzochte software.

6.1.2 Proces van certificeren van betaalautomaten t.b.v. het merk 'PIN'

Voor het gebruik van betaalautomaten zijn regels uitgevaardigd ten aanzien van de kwaliteit van hard- en software. Deze aspecten worden onderzocht bij de certificering van betaalautomaten. Een betaalautomaat wordt niet eerder ingezet voor bijvoorbeeld het product PIN, voordat het betreffende type is gecertificeerd conform de Certificeringsprocedure PIN & Chipknip. Voor het deel van de software dat de securityaspecten voor zijn rekening neemt, wordt geëist dat technisch vastgesteld kan worden dat de gecertificeerde securitysoftware volledig overeenkomt met de software zoals die daadwerkelijk in de daarvoor bedoelde gecertificeerde hardware (de fysieke betaalautomaat) wordt geladen. De te gebruiken cryptografische technieken staan voorgeschreven in de security requirements.

Op initiatief van acht Nederlandse banken (ABN Amro, Rabobank, ING, Fortis, SNS, BNG, Friesland Bank en Van Lanschot Bankiers), is op 1 januari 2005 Currence opgericht. Currence is verantwoordelijk voor nationale collectieve betaalproducten en het faciliteren van marktwerking en transparantie, met behoud van de kwaliteit en veiligheid van het betalingsverkeer in Nederland.
Partijen die betaalproducten van Currence willen aanbieden, moeten voldoen aan de voorwaarden die Currence stelt aan onder meer de organisatie en de bedrijfsprocessen. Pas na certificering kunnen zij als licentiehouder tot de markt toetreden. Ook partijen die diensten, software of apparatuur aanbieden voor bijvoorbeeld het afwikkelen van transacties in het betalingsverkeer met Currence-producten moeten aan de voorwaarden voldoen om in aanmerking te komen voor een certificaat. Currence verschaft de licenties en certificaten op basis van onderzoek van onafhankelijke auditors en certificeringinstituten. Bij een geschil is arbitrage mogelijk via een onafhankelijk College van Beroep.