Afsprakenstelsel eHerkenning

Stelsel risicoanalyse

Versie 1.7

INHOUDSOPGAVE

COLOFON

Auteur	Status
Beheerorganisatie Afsprakenstelsel eHerkenning	Definitief
Project	**Datum**
Afsprakenstelsel eHerkenning	24 april 2013
Organisatie	**Classificatie**
Logius	Openbaar
Titel van het document	**Versie**
Afsprakenstelsel eHerkenning – Stelsel risicoanalyse	1.7

HISTORIE

Datum	Versie	Wijziging	Status	Verwerkt door
17/06/11	1.1	Nieuw	Definitief	Projectbureau
12/11/11	1.2	RFCs verwerkt conform besluit kernteam 11 oktober	Definitief	Projectbureau
23/12/11	1.3	Geen wijzigingen	Definitief	Projectbureau
28/04/12	1.4	Geen wijzigingen	Definitief	Beheerorganisatie
12/07/12	1.5	RFCs verwerkt conform besluit kernteam 26 juni	Definitief	Beheerorganisatie
01/04/13	1.6	RFC0192 verwerkt	Definitief	Beheerorganisatie
24/04/13	1.7	RFC0200 verwerkt	Definitief	Beheerorganisatie

DISTRIBUTIE

Datum	Distributie	Versie
	Tactisch overleg, Gebruikersraad en publicatie op eherkenning.nl	1.7

GOEDKEURING

Datum	Naam	Versie
24/04/13	Alle RFCs voor versie 1.7 goedgekeurd door Tactisch overleg	1.7

1 Toelichting op de stelselrisicoanalyse

Dit document maakt deel uit van het afsprakenstelsel eHerkenning. Het kan niet los worden gezien van de andere documenten van het afsprakenstelsel. Voor een algemene introductie op, en een overzicht van alle documenten binnen eHerkenning wordt de lezer van dit document aangeraden eerst het document [eHerkenning – Algemene introductie] te lezen.

1.1 Achtergrond

Voor het eerst is begin 2010 door een werkgroep van deelnemers een meer techniek georiënteerde risicoanalyse op het Netwerk voor eHerkenning uitgevoerd. De risicoanalyse uit 2010 is in maart en april 2011 in een werkgroep van deelnemers en stelselexperts herijkt. Het resultaat van de herijking is dat er stelselrisico's zijn weggenomen door nadere specificaties van het stelsel, risico's door praktijkervaring na de implementaties minder relevant blijken en een aantal risico's zijn toegevoegd.

1.2 Doel en uitgangspunten voor de risicoanalyse

- De stelselrisicoanalyse is als basis gebruikt voor het opstellen van het Gemeenschappelijke Normenkader Informatiebeveiliging eHerkenning ten behoeve van de stelselverantwoording en de ISO 27001 certificering van deelnemers.
- De deelnemers worden geacht deze risicoanalyse ook te gebruiken als input voor hun eigen risicoanalyses in het kader van de verplichte ISO 27001 certificering.
- De beheerorganisatie wordt geacht de stelselrisicoanalyse te gebruiken als input voor de risicoanalyses op haar beheerprocessen, dit in het kader van de stelselverantwoording.
- De risicoanalyse wordt tenminste jaarlijks herijkt.

1.3 Opbouw van de analyse

In de initiële risicoanalyse van 2010 is alleen de impact opgenomen van optreden van een dreiging en de inschatting van de kans weggelaten omdat er op dat moment nog nauwelijks praktijkervaring met het netwerk was. In het afgelopen jaar is er echter voldoende ervaring en kennis opgebouwd om daar een eerste inschatting van te doen. De hoogte van het risico is veelal sterk afhankelijk van de kwaliteit van genomen maatregelen door deelnemers en beheerorganisatie. Er is van uitgegaan dat de hoogte van het risico afhankelijk is van:

- het ontbreken van specificaties of afspraken op stelselniveau;
- het niet nemen van maatregelen door een enkele individuele deelnemer waardoor ernstige netwerkbrede effecten kunnen ontstaan.

De mate van impact van het optreden van een dreiging is als volgt ingeschaald:

Hoog = Gevolgen zijn zeer bedreigend voor het functioneren van het Netwerk voor eHerkenning en/of zijn gebruikers.

Midden = Gevolgen zijn zeer negatief voor het functioneren van het Netwerk voor eHerkenning en/of enkele individuele gebruikers.

Laag = Gevolgen zijn negatief voor het functioneren van het Netwerk voor eHerkenning.

1.4 Risicomatrix

In de onderstaande tabel is de referentie opgenomen voor de beoordeling van hoogte van het risico. De mate van risico is opgebouwd uit de impact door het optreden van een risico en de kans dat het risico zich manifesteert.

Kans Impact	Hoog	Midden	Laag
Hoog	**H**	**H**	**M**
Midden	**H**	**M**	**L**
Laag	**M**	**L**	**L**

43

1 Algemene Risico's

Nr	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Netwerkrollen worden verstoord door een Denial-of-Service attack *Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel van het netwerk voor eHerkenning. De impact op het stelsel hangt af van het aantal partijen dat er per rol beschikbaar is.* *Oorzaken kunnen zijn:* *a. extern: een aanval op een frontend-applicatie* *b. intern: een fout in de configuratie bij een deelnemer waardoor een niet beheerste berichtenstroom wordt gegenereerd.*	M	a. H b. L	H L	ad a. Periodieke penetratietest. Afgesproken is dat tweemaal per jaar een penetratietest zal worden uitgevoerd door een externe partij op de eHerkenning systemen van de deelnemers en van de BO. Inrichten van monitoring op pogingen van onbevoegden om binnen te dringen op de systemen (intrusion detection). Ad b: Testen door de BO bij entree van een kandidaat- deelnemer in het Netwerk. Inrichten van configuratiemanagement door de deelnemers.
2.	Verlies van berichten *Toelichting: het manifest worden van deze dreiging leidt tot het niet correct afhandelen van één of meerdere individuele herkenningsvragen. De impact is daarmee gering.*	L	L	L	Is gemitigeerd in de ontwerpspecificaties van het Netwerk. Een verloren bericht wordt opnieuw aangeboden.
3.	Afgifte van onvolledige antwoorden *Toelichting: het manifest worden van deze dreiging leidt tot het niet correct afhandelen van één of meerdere individuele herkenningsvragen. De impact is daarmee gering.*	L	L	L	Is gemitigeerd in de ontwerpspecificaties van het Netwerk. Onvolledige berichten worden niet geaccepteerd.
4.	Logging/tracing-gegevens zijn onvoldoende bruikbaar voor het nagaan van een volledige herkenningsvraag *Toelichting: in geval van een geschil of problem-solving zal mogelijk gebruik gemaakt moeten worden van logging/tracing-gegevens van een volledige herkenningsvraag. Indien een deel van de keten niet beschikbaar is of inhoudelijk onvoldoende betrouwbaar is,*	M	L	L	In het (technisch) ontwerp van het stelsel is deze dreiging gemitigeerd. Maatregelen: - Beheer en beveiliging van de integriteit van logging en tracing gegevens. - Test van de implementaties bij toetreding. Deelnemers zijn zelf verantwoordelijk voor het beheer

	kan dit leiden tot een beperkte tot zeer ernstige complicatie van een geschilafhandeling of een veel langer problem-solving proces.				van de logging/tracing van (transactie)gegevens die binnen hun eigen domein worden vastgelegd.
5.	Verkeerde vertaling van de berichten *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegevens dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zijn niet beperkt tot één deelnemer. waardoor dit tot een hoge imagoschade voor het gehele netwerk kan resulteren.*	H	L	M	Maatregel: - Uitvoeren van testen bij de entree van een kandidaat- deelnemer in het Netwerk. - Inrichten van configuratiemanagement door de deelnemers.
6.	Besmetting van het netwerk door gebruikers *Toelichting: een dienstverlener of dienstafnemer kan onvoldoende beveiligingsmaatregelen hebben getroffen om te voorkomen dat een besmetting met virussen, wormen etc. wordt overgedragen aan het netwerk. In theorie zou dit tot gevolg kunnen hebben dat het netwerk niet meer of niet meer volledig functioneert. Tevens kan hierdoor een imagoprobleem ontstaan.*	H	M	H	In de aansluitvoorwaarden wordt van gebruikers verwacht (niet afgedwongen) dat zij hun informatiebeveiliging in voldoende mate op orde hebben. Deelnemers zijn zelf verantwoordelijk voor hun eigen informatiebeveiliging en hebben anti-virus software geïnstalleerd. Er zijn afspraken omtrent incidentmanagement, waardoor relevante partijen adequaat geïnformeerd worden over een mogelijke besmetting met malware.
7.	Repeterende incidenten of beschikbaarheidproblemen bij een of meerdere partijen of rollen *Toelichting: Het vertrouwen van gebruikers in het gehele netwerk voor eHerkenning komt in het geding als een en meerdere deelnemers frequent beveiligings- of beschikbaarheidproblemen hebben. Doorgaans wordt een ervaring van niet beschikbaarheid binnen een half jaar 'vergeten'; herhaling binnen die periode leidt doorgaans tot verlies aan*	M	M	M	Er zijn (status medium 2012) voldoende redundant ingevulde rollen om de continuïteit van het Netwerk te borgen. Er zijn echter (nog) geen afspraken gemaakt over het (tijdelijk) overnemen van activiteiten indien een rol bij een deelnemer, bijvoorbeeld een HM, niet meer beschikbaar is. Er is een incidentmanagement procedure afgesproken waardoor monitoring van incidenten in het stelsel plaatsvindt.

	vertrouwen.				
8.	Niet of niet tijdig melden van beveiligingsincidenten of kwetsbaarheden en oplossingen door deelnemers *Toelichting: Indien deelnemers niet tijdig incidenten melden wordt een mogelijk door de beheerorganisatie te coördineren actie steeds omvangrijker. Wanneer niet op basis van onderling vertrouwen binnen het netwerk incidenten en oplossingen worden gedeeld is dit negatief voor de performance op netwerkniveau.*	H	H	H	Er is een incidentmanagement procedure afgesproken. Hierbinnen is ruimte om bepaalde gevoelige incidenten discreet te behandelen. Incidenten en incidentmanagement worden periodiek besproken in het security officers overleg.
9.	Niet of niet tijdig melden van beveiligingsincidenten door dienstverleners of dienstafnemers *Toelichting: Diensverleners en dienstafnemers kunnen het netwerk onbedoeld besmetten met malware. Het niet tijdig melden van besmettingen leidt tot een verhoogde kans dat de besmetting door het netwerk heen verspreidt .*	H	L	M	De systemen in het Netwerk zijn gescheiden van de systemen van de dienstverleners en dienstafnemers. Alleen berichten die voldoen aan de specificaties worden geaccepteerd. Het Netwerk is niet aansprakelijk indien de besmetting door systemen van dienstverleners en dienstafnemers het gebruik van eHerkenning onmogelijk maken. *Op stelselniveau worden geen gegevens bijgehouden omtrent incidenten in relatie tot eHerkenning bij dienstafnemers of dienstverleners.* Meer in de “awareness”-zin wordt er in de gebruikersvoorwaarden c.q. aansluitvoorwaarden aandacht gevraagd voor informatiebeveiliging. Voor gemeenten, als gebruiker van Digid, is de verplichting vanuit het Rijk opgelegd om periodiek een audit op de informatiebeveiliging te laten uitvoeren.
10.	Een middel of machtiging wordt op een te hoog betrouwbaarheidsniveau geclassificeerd. *Toelichting: te hoog geclassificeerde middelen of machtigingen kunnen*	H	L	M	Het afsprakenstelsel bevat afspraken en procedures voor het classificeren van middelen en machtigingen.

	leiden tot misbruik van diensten van dienstverleners of ongeldigheid van informatietransacties tussen dienstverleners en dienstafnemers. Op die manier zouden diensten afgenomen kunnen worden waarvoor de dienstafnemer zich onvoldoende geauthenticeerd heeft.				
11.	Webapplicaties van beheerorganisatie en deelnemers zijn kwetsbaar. *Toelichting: Bij de bouw van webapplicaties is het vanzelfsprekend dat de bouwer zonder expliciete opdracht de applicatie standaard test op kwetsbaarheden. Niet testen kan leiden tot kwetsbaarheden die kunnen worden misbruikt. Misbruik ondermijnt het vertrouwen in het Netwerk voor eHerkenning.*	H	M	H	Applicaties van deelnemers worden verplicht voor opname in het Netwerk getest. Periodiek worden door de beheerorganisatie penetratietesten in het Netwerk georganiseerd. Afgesproken is om tweemaal per jaar penetratietesten uit te laten voeren bij deelnemers en BO. Wellicht ten overvloede: uitgesloten hiervan zijn de 'browser-lekken' die bij gebruikers (dienstverleners en dienstafnemers) kunnen voorkomen.

44

2 Risico's van de beheerorganisatie

De BO heeft een eigen risicoanalyse uitgevoerd op de processen en onderdelen (assets) waar zij direct verantwoordelijk voor is. Voor enkele specifieke assets werken de processen uitsluitend indien zowel deelnemers als de BO hun deel op orde hebben. In deze risicoanalyse worden de risico's geanalyseerd en maatregelen geformuleerd ten aanzien van:

- metadata
- dienstencatalogi
- testfaciliteiten
- incidentmanagement
- documentatie m.b.t. het Afsprakenstelsel.

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	De meta-data is onjuist, onvolledig of niet aktueel. *Toelichting: Onjuiste of niet tijdige wijzigingen kunnen leiden tot het schaden van de werking van eHerkenning of evt. het toelaten van een ongewenste berichten tot het netwerk.*	H	M	H	De (gezamenlijke) procedure voor het komen tot een aktueel en integer metadatabestand is beschreven in het Operationeel Handboek. De BO heeft tevens een werkbeschrijving gemaakt om te komen tot een geaggregeerd metadatabestand.
2.	De trusted party list van deelnemers op het netwerk van eHerkenning die opgenomen is in het metadatabestand, is onjuist, onvolledig of niet aktueel. *Toelichting: Onjuiste of niet tijdige wijzigingen kunnen leiden tot het schaden van de werking van eHerkenning of het toelaten van een ongewenste partij tot het netwerk.*	H	M	H	Door het opnemen van de certificaatnummers van de toegestane partijen (deelnemers) (ook wel genoemd "whitelist") is het in principe uitgesloten dat onbevoegde partijen zich op het eHerkenningsnetwerk begeven. In de werkbeschrijving bij de BO is aangegeven op welke wijze de controles hierop moeten plaatsvinden.
3.	Proces voor melding en afhandeling van beveiligingsincidenten werkt niet adequaat. *Toelichting: Afhankelijk van het type incident kan het niet goed werken van*	M	M	M	Het incidentmanagement proces is beschreven en afgesproken. Dit omvat de afspraak over de verplichting tot het melden van beveiligingsincidenten door deelnemers. Het incidentmanagement proces is beschreven in het Operationeel

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
	het incidentmanagement proces het netwerk operationeel schaden.				Handboek. Periodiek wordt hierover gerapporteerd aan het Bestuur nadat de geaggregeerde rapportage is besproken in het security officers overleg.
4.	De door DV's aangeleverde gegevens omtrent dienstencatalogi wordt foutief verwerkt. *Toelichting:* *Foutief verwerken kan bewust en onbewust.* *Bij foutieve gegevens bestaat het risico dat niet geautoriseerde personen toegang krijgen tot door DV aangeboden diensten of dat geautoriseerde personen geen diensten kunnen afnemen.* *Nieuwe versie van dienstencatalogus wordt te laat gepubliceerd.* *Hierdoor bestaat het risico dat door DV aangeboden dienst(en) niet via eHerkenning kunnen worden geleverd.*	M	M	M	Bij de BO is een procedure opgesteld om fouten in de Dienstencatalogus te minimaliseren. Basis wordt gevormd door de deelnemers die de gegevens van dienstverleners krijgen aangereikt. Daar zal de eerste controle moeten plaatsvinden. Beschikbare procedure moet strikt gevolgd worden, in dit geval vooral met betrekking tot de afgesproken tijdlijn.
5.	De beheerorganisatie beschikt over onvoldoende kennis en ervaring met betrekking tot informatiebeveiliging en risicomanagement. *Toelichting: Onvoldoende kennis en ervaring kan leiden tot inschattingsfouten bij incidentbehandeling of onvoldoende kwaliteit van de beveiligingstesten. In beide gevallen kan het imago van eHerkenning geschaad worden.*	M	M	M	De (tijdelijke) beheerorganisatie beschikt overexpertise met betrekking tot informatiebeveiliging Door capaciteitsmanagement en gedocumenteerde bedieningsprocessen is kennis beschikbaar en overdraagbaar. Er zijn rollen gedefinieerd en ingevuld voor securitymanager, riskmanager, incidentmanager en changemanager.
6.	Testgereedschap wordt misbruikt. *Toelichting: Het testgereedschap is publiek beschikbaar.* *Beschikbaar wordt gesteld:*	M	L	L	Deze testtools zijn in feite publiek beschikbaar op de extranet website. De BO beheert de software. De

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
	- de simulatortool *- de testtool voor dienstverleners*				testtools zelf worden, na een change, getest door de BO. De software staat op een afgeschermde omgeving.
7.	Testomgeving is onvoldoende gedocumenteerd. *Toelichting: Zonder documentatie zijn testwerkzaamheden onvoldoende overdraagbaar en kan een gebrek aan kennis van testgereedschap en omgeving leiden tot verstoringen in het Netwerk.*	H	M	H	De BO heeft een bedieningsprocedure gemaakt voor het beheren van de simulatortool en de testtool voor dienstverleners.
8.	Documentatie van het Netwerk voor eHerkenning is niet integer of volledig. *Toelichting: Te weinig zekerheid over de juistheid en volledigheid van de gedocumenteerde afspraken in het stelsel voor eHerkenning kan leiden tot verstoringen (issues over technisch aspecten)of juridische discussie over o.a. aansprakelijkheden*	H	M	H	Er is een changemanagement procedure ingericht die moet borgen dat de documentatie van het Afsprakenstelsel juist en volledig beschikbaar wordt gesteld aan de deelnemers. Alle changes worden, binnen deze procedure, besproken met (vertegenwoordigers van) deelnemers.
9.	Documentatie van het Netwerk voor eHerkenning is niet toegankelijk. *Toelichting: Langdurige onbeschikbaarheid van het archief is belemmerend voor de processen van de beheerorganisatie en kan bijvoorbeeld leiden tot vertragingen bij kandiaten voor toetreding.*	M	M	M	De documenten uit het Afsprakenstelsel zijn in principe "openbaar". Ten behoeve van de deelnemers heeft de BO de geldende documentatie online beschikbaar gesteld aan hiertoe geautoriseerde (vertegenwoordigers van) deelnemers.
10.	Fouten bij DNS beheer cookieserver *Toelichting: De gemeenschappelijke cookieserver is nodig voor de SSO functionaliteit bij de Herkenningsmakelaar.*	L	M	L	Maatregel: proces beschrijven voor beheer van de cookieserver in [Operationeel handboek], vervolgens oplossingen testen en periodiek monitoren. Risico ligt ook bij de deelnemers.

57

3 Risico's van de Herkenningsmakelaar

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Er wordt een verkeerde combinatie van authenticatie en machtiging op een vraag van de dienstverlener samengesteld. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren. Het verspreidingsgebied van de fout zal echter beperkt zijn.*	H	L	M	De kans dat een verkeerde combinatie zich voordoet wordt als Laag geclassificeerd. De oorzaak kan liggen in het onjuist invoeren van gegevens in de authenticatie of machtigingstabellen. Maatregel ligt in de sfeer van inputvalidatie. Iedere deelnemer is verantwoordelijk voor het juist registreren van gegevens.
2.	Ten onrechte niet doorgeven van berichten. *Toelichting: in dit geval is er sprake van een denial of service voor één of meerdere dienstafnemers. De oorzaak kan liggen in een al of niet bewust veroorzaakte technische fout in de dienstverlening. Gevolg kan zijn dat een deel van de dienstverlening niet beschikbaar is.*	H	M	H	Diverse maatregelen: zoals inputvalidatie bij het opnemen van machtigings- en authenticatiegegevens alsmede het testen van het netwerkverkeer.
3.	Bewust zelfstandig genereren van berichten als antwoord op een vraag van de dienstverlener zonder dat de achterliggende authenticatie en machtiging zijn aangevraagd. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren.*	M	L	L	De technische specificaties van het berichtenverkeer maakt het optreden van de deze dreiging onwaarschijnlijk. De kans op een onbewust genereren van een bericht bijvoorbeeld als gevolg van een foutieve beheerhandeling is groter maar de impact zal dan in de meeste gevallen klein zijn.

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
4.	Teruggeven van een te hoog betrouwbaarheidsniveau. *Toelichting: betrouwbaarheidsniveaus zijn in hoge mate bepalend voor het gestelde vertrouwen in het netwerk. Fouten in het gebruik van betrouwbaarheidsniveaus, al of niet opzettelijk, zijn direct gerelateerd aan de kern van de dienstverlening in het afsprakenstelsel. Dit kan grote imagoschade opleveren voor het gehele netwerk en de deelnemers.*	H	M	H	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging. Maatregelen worden gevonden in configuratiemanagement, inputvalidatie en testen.
5.	Foutief gegenereerde berichten. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegevens dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zullen primair een klein verspreidingsgebied kennen, echter deze dreiging raakt wel de kern van de dienstverlening van het gehele netwerk en de deelnemers.*	H	M	H	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging. Maatregelen worden gevonden in configuratiemanagement en testen.
6.	*verwijderd igv RFC192*				
7.	Deelnemer wordt ten onrechte vertrouwd. *Toelichting: deze dreiging is van toepassing op het moment dat een deelnemer op niet-legitieme wijze toegang verkrijgt tot het netwerk of op legitieme wijze ten onrechte tot het netwerk wordt toegelaten. Het vertrouwen in het afsprakenstelsel is gebaseerd op het niet voorkomen van een dergelijke situatie. Deze dreiging betreft daarmee het fundament van het afsprakenstelsel.*	H	M na:L	H na: M	Een fout in de tabellen is de oorzaak van het optreden van deze dreiging. Testbatterij is ingericht om o.a. bij toetreding fouten in de tabellen te reduceren. NB De kans dat deze dreiging optreedt is gedurende het toetredingsproces Hoog omdat dit een wijzigingsmoment is. In het afsprakenstelsel is een toetredingsproces beschreven. Onderdeel hiervan is een toetsing door een externe auditor. Na toetreding is de kans dat deze dreiging optreedt Laag en vooral afhankelijk van een juist tabellenbeheer (inputvalidatie).
8.	*verwijderd igv RFC192*				

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
9.	*verwijderd igv RFC192*				
10.	*verwijderd igv RFC192*				
11.	Ongeautoriseerd ophalen van machtigingen *Toelichting: Het manifest worden van deze dreiging, door het opvragen van een machtigingsbewijs zonder voorafgaande authenticatie, geeft een onbevoegd persoon inzicht in een specifieke machtiging. Deze informatie zou als input gebruikt kunnen worden voor het opbouwen van een malafide handeling.*	L	L	L	Dreiging zou op kunnen treden indien een deelnemer ten onrechte is vertrouwd (zie 7).
12.	*verwijderd igv RFC192*				
13.	Denial-of-Service attack op de Herkenningsmakelaar via een gecompromitteerde dienstverlener *Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel of het geheel van het netwerk voor eHerkenning. De impact hangt af van het aantal partijen dat er voor de rol van herkenningsmakelaar beschikbaar is. De gevolgen zullen merkbaar zijn voor alle dienstverleners die bij de betreffende herkenningsmakelaar zijn aangesloten.*	M	L	L	De dienstverlener heeft geen belang bij het offline brengen van de HM en verplicht zich volgens contract zijn netwerk afdoende te beschermen. De inschatting van de lage kans van optreden is ingegeven door het uitgangspunt dat de HM zijn verkeer afdoende monitort om tijdig actie te kunnen ondernemen.

58

4 Risico's voor de Authenticatiedienst

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Er wordt een verkeerde combinatie van authenticatie en machtiging op een vraag van de dienstverlener samengesteld. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk en de deelnemers op kan leveren. Het verspreidingsgebied van de fout zal echter beperkt zijn.*	M	M	M	De oorzaak kan liggen in het onjuist invoeren van gegevens in de authenticatie of machtigingstabellen. Maatregel ligt in de sfeer van inputvalidatie.
2.	Ten onrechte niet doorgeven van berichten. *Toelichting: in dit geval is er sprake van een denial of service voor één of meerdere dienstafnemers. De oorzaak kan liggen in een al of niet bewust veroorzaakte technische fout in de dienstverlening.*	H	M	H	Diverse maatregelen: zoals inputvalidatie bij het opnemen van machtigings- en authenticatiegegevens alsmede het testen van het netwerkverkeer.
3.	Bewust zelfstandig genereren van berichten als antwoord op een vraag van de dienstverlener zonder dat de achterliggende authenticatie en machtiging zijn aangevraagd. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. Voor het afsprakenstelsel betekent dit dat de kern van de dienstverlening wordt aangetast, wat grote imagoschade voor het gehele netwerk*	H	L	M	De technische specificaties van het berichtenverkeer maakt het optreden van de deze dreiging onwaarschijnlijk. De kans op een onbewust genereren van een bericht bijvoorbeeld als gevolg van een foutieve beheerhandeling is groter maar de impact zal dan in de meeste gevallen klein zijn. Waardoor dit risico maximaal op laag tot midden zal scoren.

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
	en de deelnemers op kan leveren.				
4.	Teruggeven van een te hoog betrouwbaarheidsniveau. *Toelichting: betrouwbaarheidsniveaus zijn in hoge mate bepalend voor het gestelde vertrouwen in het netwerk. Fouten in het gebruik van betrouwbaarheidsniveaus, al of niet opzettelijk, zijn direct gerelateerd aan de kern van de dienstverlening in het afsprakenstelsel. Dit kan grote imagoschade opleveren voor het gehele netwerk en de deelnemers.*	H	L	M	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging.
5.	Foutief gegenereerde berichten. *Toelichting: in deze situatie kan een dienstafnemer toegang verleend worden tot de gegevens van een andere dienstafnemer of wordt een handeling namens een andere dienstafnemer uitgevoerd dan beoogd. Afhankelijk van het type gegeven dat het betreft kan dit gevolgen hebben voor de benadeelde dienstafnemer. De gevolgen zullen primair een klein verspreidingsgebied kennen, echter deze dreiging raakt wel de kern van de dienstverlening van het gehele netwerk en de deelnemers zal resulteren.*	H	L	M	Het meest waarschijnlijke scenario is dat er sprake is van een verkeerde implementatie die in de tests voor toetreding niet zijn herkend, of een configuratiefout bij een deelnemer als gevolg van het doorvoeren van een wijziging.
6.	*verwijderd igv RFC192*				
7.	Deelnemer wordt ten onrechte vertrouwd. *Toelichting: deze dreiging is van toepassing op het moment dat een deelnemer op niet-legitieme wijze toegang verkrijgt tot het netwerk of op legitieme wijze ten onrechte tot het netwerk wordt toegelaten. Het vertrouwen in het afsprakenstelsel is gebaseerd op het niet voorkomen van een dergelijke situatie. Deze dreiging betreft daarmee het fundament van het afsprakenstelsel.*	H	H na:L	H na:M	Een fout in de metadata is de oorzaak van het optreden van deze dreiging. Testbatterij is ingericht om o.a. bij toetreding fouten in de tabellen te reduceren. NB De kans dat deze dreiging optreedt is gedurende het toetredingsproces Hoog omdat dit een wijzigingsmoment is. In het afsprakenstelsel is een toetredingsproces beschreven. Onderdeel hiervan is een toetsing door een onafhankelijke auditor. Na toetreding is de kans dat deze dreiging optreedt Laag

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
					en vooral afhankelijk van een juist tabellenbeheer (inputvalidatie).
8.	Deelnemer wordt ten onrechte niet vertrouwd *Toelichting: deze dreiging is van toepassing op het moment dat een beoogde deelnemer ten onrechte niet tot het netwerk wordt toegelaten of uitgesloten wordt. Dit levert irritatie op bij de deelnemer en mogelijk bij de klant van de deelnemer, maar geeft uiting aan een groot belang van het toetredingsproces. De impact geldt dus voor een enkele partij.*	L	H na:L	M na:L	Idem
9.	*verwijderd igv RFC192*				
10.	*verwijderd igv RFC192*				
11.	Ongeautoriseerd ophalen van machtigingen *Toelichting: Het manifest worden van deze dreiging, door het opvragen van een machtigingsbewijs zonder voorafgaande authenticatie, geeft een onbevoegd persoon inzicht in een specifieke machtiging. Deze informatie zou als input gebruikt kunnen worden voor het opbouwen van een malafide handeling.*	L	L	L	Dreiging zou op kunnen treden indien een deelnemer ten onrechte is vertrouwd (zie 7).
12.	*verwijderd igv RFC192*				
13.	Denial-of-Service attack via een gecompromitteerde dienstverlener *Toelichting: het manifest worden van deze dreiging leidt tot het niet functioneren van een deel of het geheel van het netwerk voor eHerkenning. De impact hangt af van het aantal partijen dat er voor de rol van AD beschikbaar is. De gevolgen zullen merkbaar zijn voor alle dienstverleners die bij de betreffende herkenningsmakelaar zijn aangesloten.*	M	L	L	De dienstverlener heeft geen belang bij het offline brengen van de AD en verplicht zich volgens contract zijn netwerk afdoende te beschermen. De inschatting van de lage kans van optreden is ingegeven door het uitgangspunt dat de HM zijn verkeer afdoende monitort om tijdig actie te kunnen ondernemen.

59

60

5 Risico's voor het Machtigingenregister

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Onjuist invoeren van machtigingsgegevens *Toelichting: bij optreden van deze dreiging wordt ten onrechte structureel de toegang tot een dienst van een dienstverlener toegewezen of geweigerd. Bij onjuiste toewijzing kan sprake zijn van significante impact, indien het een hoog betrouwbaarheidsniveau betreft. Daarnaast heeft het manifest worden van deze dreiging een negatief effect op het imago van het netwerk voor eHerkenning gezien de relevantie van machtigingen voor het netwerk. Het effect zal betrekking hebben op individuele gevallen.*	M*)	L	L*)	*) impact en hoogte van het risico is afhankelijk van het van toepassing zijnde betrouwbaarheidsniveau. Maatregel: inputvalidatie
2.	Ten onrechte afgeven van berichten *Toelichting: bij optreden van deze dreiging wordt ten onrechte eenmalig of structureel de toegang tot een dienst van een dienstverlener toegewezen. Er kan sprake zijn van significante impact, indien het een hoog betrouwbaarheidsniveau betreft. Daarnaast heeft het manifest worden van deze dreiging een negatief effect op het imago van het netwerk voor eHerkenning gezien de relevantie van machtigingen voor het netwerk. De impact blijft beperkt tot individuele gevallen.*	H	M	H	Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie onder 1.
3.	Ten onrechte negatief beantwoorden van machtigingsvragen *Toelichting: bij optreden van deze dreiging wordt ten onrechte structureel de toegang tot een dienst van een dienstverlener geweigerd. Dit zal leiden tot irritatie in individuele*	L	L	L	Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie nr. 1

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
	gevallen.				
4.	Onjuiste koppeling van machtigingsvraag en bericht *Toelichting: bij optreden van deze dreiging wordt toegang tot een onbedoelde dienst van een mogelijk andere dienstverlener toegewezen. Het manifest worden van deze dreiging kan bij bekend worden een zeer negatief effect op het imago van het netwerk voor eHerkenning omdat dienstverleners er van op aan moeten kunnen dat alleen de juiste geauthenticeerden toegang tot de dienstverlening hebben. De impact blijft beperkt tot individuele gevallen.*	M	M	M	Deze dreiging is een variant op dreiging 2. Oorzaak kan liggen in foutieve gegevens in de machtigingentabel. Zie nr. 1
5.	*verwijderd igv RFC192*				
6.	*verwijderd igv RFC192*				
7.	*verwijderd igv RFC192*				
8.	Foutief importeren/exporteren van machtigingen (bij overgang naar ander MR) *Toelichting: het manifest worden van deze dreiging leidt tot een aantasting van het imago (betrouwbaarheid) van het betreffende (nieuwe) machtigingregister door machtigingsvragen die ten onrechte worden toegewezen of afgewezen. Dit geldt voor het gehele verzorgingsgebied van het machtigingregister. De impact kan afhankelijk zijn van het zekerheidsniveau. De uitstraling op het imago van het gehele netwerk is afhankelijk van de grootte van het verzorgingsgebied van het machtigingregister.*	L	L	L	Dienstafnemers zijn zelf verantwoordelijk voor de controle van de juistheid van machtigingen.
9.	Ongeautoriseerde toegang tot MR (opzettelijk) *Toelichting: deze dreiging betreft het*	M	M	M	Indien er sprake is van online toegang door een dienstafnemer tot zijn machtigingen zal een dienstafnemer

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
	ten onrechte toegang krijgen tot het MR waardoor de vastgelegde machtigingen gecorrumpeerd kunnen worden. Het manifest worden van deze dreiging leidt tot een aantasting van de betrouwbaarheid van het machtigingregister door machtigingsvragen die ten onrechte worden toegewezen (of evt. afgewezen). Dit geldt potentieel voor het gehele verzorgingsgebied van het machtigingregister. Daarnaast is de impact afhankelijk van het betrouwbaarheidsniveau. De uitstraling op het imago van het gehele netwerk is afhankelijk van de grootte van het verzorgingsgebied van het machtigingregister.				(juridisch) op zijn verantwoordelijkheid gewezen moeten worden op de noodzaak vertrouwelijk om te gaan met toegangsgegevens of middelen. Dit kan onderdeel zijn van het contract tussen dienstafnemer en deelnemer.
10.	Registratie bij een machtigingsregister is onvolledig of onjuist *Toelichting: registratie van een nieuwe dienstafnemer bij een machtigingenregister, inclusief de houder van de hoogste machtiging. Fouten in dit proces kunnen leiden tot het ten onrechte verkrijgen van diensten bij dienstverleners.*	M	M	M	Maatregel: inputvalidatie
11.	*verwijderd igv RFC192*				
12.	*verwijderd igv RFC192*				

61

6 Risico's in de relaties tussen de rollen

6.1 Relatie Dienstverlener – HM

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	Commerciële competitie kan leiden tot stellen van lage informatiebeveiligingseisen aan dienstverleners. *Toelichting: het stellen van lage informatiebeveiligingseisen aan dienstverleners vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning (zie de betreffende dreiging in de paragraaf over de herkenningsmakelaar). Vraag is of dit wel een dreiging is. De eisen aan het koppelvlak zijn uniform. De gebruikersvoorwaarden zijn ook uniform. Verder dan dat kun je in feite als deelnemer niet gaan.*	M	L	L	Eisen aan het koppelvlak tussen HM en Dienstverlener zijn beschreven evenals de vrijheidsgraden daarin. Aansluitingen worden getest.
2.	*verwijderd igv RFC192*				
3.	De dienstverlener heeft onvoldoende beveiligingsmaatregelen getroffen: *Toelichting: vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning (zie de betreffende dreiging in de paragraaf over de herkenningsmakelaar). De dienstverlener kan bijvoorbeeld een stroom aan berichten in het netwerk genereren.*	M	L	L	Eisen aan het koppelvlak tussen HM en Dienstverlener is beschreven evenals de vrijheidsgraden daarin. Aansluitingen worden getest.
4.	HM is niet in staat technische fouten van de dienstverlener te herkennen en te mitigeren: *Toelichting: vergroot de kans op aantasting van de betrouwbaarheid van het netwerk voor eHerkenning.*	M	M	M	Impact hang sterk af van de aard van de dienst en de dienstverlener en het bijbehorende betrouwbaarheidsniveau.
5.	*verwijderd igv RFC192*				

6.2 Relatie HM – AD

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	*verwijderd igv RFC192*				
2.	[LEEG]				Geen additionele dreigingen anders dan al genoemd onder Algemeen.

6.3 Relatie HM –MR

Nr.	Dreiging	Impact	Kans	Risico	Opmerkingen en maatregelen
1.	*verwijderd igv RFC192*				
2.	*verwijderd igv RFC192*				
3.	*verwijderd igv RFC192*				