

Standaardisatiemogelijkheden afsprakenstelsel eHerkenning

Ten behoeve van Forum Standaardisatie - april 2010

Auteur Projectbureau Afsprakenstelsel
Versie 04
Status Concept
Den Haag, 01-04-2010



Document informatie

Colofon

Auteur	Status
Projectbureau Afsprakenstelsel eHerkenning	Concept
Project	Datum
Afsprakenstelsel eHerkenning	01-04-2010
Organisatie	Classificatie
ICTU	Vertrouwelijk
Titel	Locatie
Standaardisatiemogelijkheden afsprakenstelsel eHerkenning	Den Haag
Versie	
04	

Historie

Datum	Versie	Wijziging	Status	Verwerkt door
29-03-10	0.1		Concept	MS
30-03-10	0.2	Na bespreking met Cor Franke	Concept	MS

Distributielijst

Datum	Distributie	Presentatie	Versie
29-03-10	Tom Visser	n.v.t.	0.1
30-03-10	Cor Franke	n.v.t.	0.2

Goedkeuring

Datum	Naam	Versie
-------	------	--------

1 Inleiding

Authenticatie en autorisatie vormen sinds het begin een belangrijk onderwerp op de agenda van Forum en College Standaardisatie. Het programma eHerkenning is een van de concrete ontwikkellijnen. In de vergadering van 16 december is vanuit het ministerie van Economische Zaken een inleiding gegeven over eHerkenning en de voortgang van daarvan. In deze notitie wordt de actuele stand van zaken toegelicht en worden de vragen gesteld die bij het begin van een standaardisatieproces via Forum en College Standaardisatie van het uit het programma voortkomende afsprakenstelsel eHerkenning beantwoord dienen te worden. Een besluit van College Standaardisatie in de najaarsvergadering van 2010 over eHerkenning wordt door het ministerie van Economische Zaken en door de bij eHerkenning betrokken marktpartijen als een belangrijke stap op naar overheidsbrede toepassing van het afsprakenstelsel eHerkenning gezien.

1.1 Achtergronden eHerkenning

In het programma eHerkenning werken overheidsdienstverleners en marktpartijen samen om te komen tot organisatorische, functionele en technische afspraken voor eHerkenningdiensten. Inmiddels is versie 0.8 van het afsprakenstelsel waarin een en ander is vastgelegd, geaccordeerd door het samenwerkingsverband. Op basis van deze versie zal eind april de eerste proefimplementatie starten met Agentschap NL (voorheen SenterNovem) ten behoeve van de WBSO subsidieaanvraag. In de loop van de komende maanden zullen andere partijen dan Agentschap NL eveneens (proef)implementaties uitvoeren. Parallel daaraan wordt de doorontwikkeling naar een 1.0 versie uitgevoerd, enkele andere proefimplementaties opgestart en toegewerkt naar een volwaardige beheerorganisatie voor het afsprakenstelsel. Tegen het eind van 2010 dient het afsprakenstelsel voldoende volwassen te zijn om zich “op eigen benen”, dat wil zeggen zonder de projectmatige impuls, verder te ontwikkelen als noodzakelijk onderdeel van de e-overheid. In de tweede helft van 2010 worden de huidige gebruikers van DigiD Bedrijven gemigreerd naar eHerkenning. Dat zal het volume van gebruik stevig doen groeien, evenals de diversiteit van de deelnemende overheidsdienstverleners.

De oplossing voor eHerkenning die in het afsprakenstelsel is vastgelegd heeft de vorm van een netwerk waarin onderscheiden verantwoordelijkheden nauwkeurig over meerdere rollen verdeeld zijn. Deze rollen worden ingevuld door marktpartijen. Deze deelnemers aan het netwerk voor eHerkenning concurreren met elkaar op basis van een marktmodel. In het kader van de proefimplementaties zijn voor ieder van deze rollen inmiddels meerdere marktpartijen gegadigd: er is daadwerkelijk sprake van een beginnende “markt”. De netwerkoplossing doet recht aan de intrinsieke diversiteit en complexiteit van authenticatie en autorisatie van bedrijven. De verantwoordelijkheden ten aanzien van authenticatiemiddelen (PKI-certificaten, smartcards, tokens, userid-password combinaties etc.) enerzijds en het registreren en benutten van machtigingen en bevoegdheden anderzijds zijn los van elkaar bepaald. Daarmee creëert het netwerk maximale keuzevrijheid voor bedrijven en overheidsdienstverleners en maakt het hergebruik van reeds in omloop zijnde authenticatiemiddelen waaronder ook bankpassen en mobiele telefoons in principe mogelijk. Ook legt het de basis voor het hergebruiken van binnen (grote) bedrijven bestaande authenticatie- en machtigingsvoorzieningen door deze na certificatie toe te laten tot het netwerk. Dit model is in grote lijnen een verdere uitwerking van het rapport Verkenning authenticatie dat in maart 2007 in opdracht van Forum Standaardisatie is opgesteld.

In het afsprakenstelsel zijn de uitgangspunten die het ministerie van Economische Zaken bij de start van het project heeft vastgesteld verwerkt (zie bijlage).

Het programma eHerkenning ligt daarmee goed op koers. Het gewenste eindresultaat is: de conform het NUP afgesproken overheidsbreed inzet te zetten oplossing voor authenticatie en autorisatie van bedrijven en van degenen die namens bedrijven daadwerkelijk transacties met overheidsdienstverleners verrichten. Om dit resultaat te bereiken is verdere standaardisatie een belangrijk instrument. Overheidsdienstverleners enerzijds en geïnteresseerde marktpartijen anderzijds wensen zoveel mogelijk zekerheden over de toekomstvastheid van de oplossing alvorens er in te investeren. Een besluit om (delen van) eHerkenning op te nemen op de pas-toe-of-leg-uit lijst door het College Standaardisatie in de najaarsvergadering van 2010 wordt door het ministerie van Economische Zaken en door de betrokken marktpartijen als een belangrijke stap naar deze continuïteit gezien. Voorafgaand aan de aanvang van dit proces dienen enkele vragen beantwoord te worden:

- In welke vorm leent het afsprakenstelsel zich voor deze standaardisatie.
- Hoe verhoudt het afsprakenstelsel zich tot belendende percelen en de standaardisatie in die percelen?
- Met welke verdere ontwikkelingen en tijdslijnen dient in het standaardisatieproces rekening gehouden te worden, in het bijzonder ten aanzien van Europese standaardisatie.

1.2 Doel document

Deze notitie geeft een korte samenvatting van het afsprakenstelsel eHerkenning, plaatst dit in de context van de e-overheid. Vervolgens wordt aangegeven welke elementen uit het afsprakenstelsel zich lenen voor standaardisatie en hoe deze elementen zich verhouden tot de drie vormen van interoperabiliteit, organisatorisch, semantisch en technisch, waarop de overheidsstandaardisatie zich in eerste instantie richt. Tenslotte worden enkele concrete vragen aan Forum en College voorgelegd op basis waarvan het standaardisatieproces van het afsprakenstelsel eHerkenning langs Forum en College kan starten. De doelstelling daarbij is in de College vergadering van najaar 2010 een besluit over de standaardisatie te kunnen nemen.



2 Het Afsprakenstelsel eHerkenning

2.1 Doel eHerkenning

Het doel van het programma eHerkenning is *“het tot stand brengen van een eenduidige oplossing voor eHerkenning voor Bedrijven om zo de kwaliteit en beschikbaarheid van elektronische dienstverlening door de overheid te vergroten.”*

Om dit doel te bereiken wordt een netwerk voor eHerkenning gerealiseerd waarin marktpartijen verschillende afgebakende rollen vervullen. Het afsprakenstelsel eHerkenning beschrijft dit netwerk en de afspraken en richtlijnen die benodigd zijn om deze oplossing te laten werken en het vertrouwen in de herkenningdiensten die ermee gerealiseerd worden te verankeren. Toepassing van eHerkenning in brede domein, business-to-business, wordt niet uitgesloten.

2.2 Opzet eHerkenning: netwerkmodel

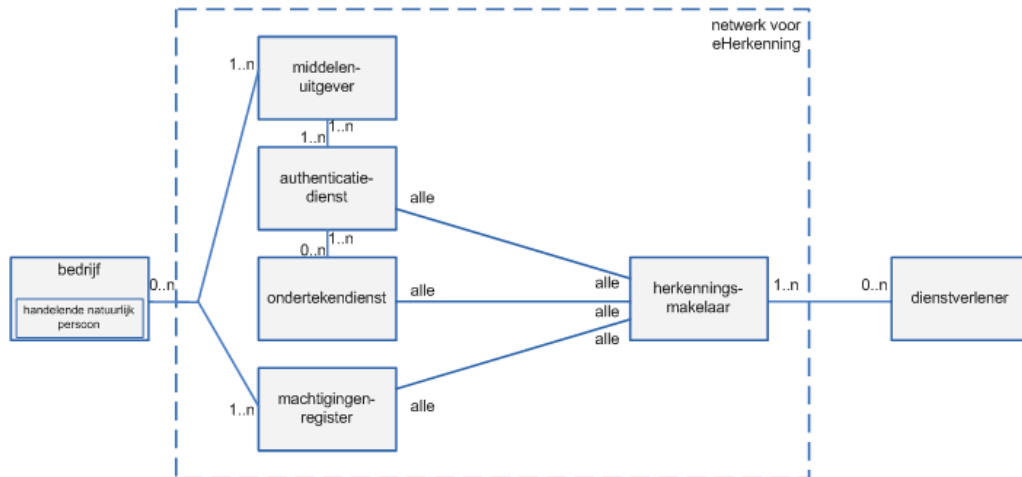
Om de elektronische herkenning van bedrijven door de overheid mogelijk te maken zal het afsprakenstelsel de afspraken regelen tussen primair de volgende vijf rollen¹:

1. Middelenuitgevers. Binnen eHerkenning zijn in principe allerlei middelen toegestaan, mits ze aan bepaalde technische en procedurele specificaties voldoen. De middelen zijn ingedeeld conform de STORK-betrouwbaarheidsniveaus. Deze middelen kunnen persoonsgebonden zijn (bijvoorbeeld telefoon, bankpas en gekwalificeerd certificaat) en/of bedrijfsgebonden (bijvoorbeeld tokens). Met een door een daartoe gerechtigde vertegenwoordiger van een bedrijf getekende verklaring kan iemand een middel aanschaffen bij een middelenuitgever;
2. Authenticatiediensten. Deze rol zorgt ervoor dat gebruikers worden geauthenticeerd. Daartoe onderhoudt de authenticatiedienst een of meer relaties met de uitgevers van herkenningmiddelen;
3. Machtigingenregisters. Een bedrijf kan een ander bedrijf of medewerkers van het eigen bedrijf machtigen om voor geïdentificeerde processen uit de dienstencatalogus namens dat bedrijf handelingen te verrichten. Deze machtiging wordt vastgelegd in een machtigingsregister, waarmee het bedrijf een contract dient te hebben. Eén partij mag zowel de rol van middelenuitgever als machtigingenregister spelen en de registratieprocessen voor uitgifte van middelen en registratie van machtigingen integreren. (Grote) bedrijven kunnen (op termijn) eigen machtigingenregisters aansluiten op het stelsel;
4. Herkenningmakelaars. Een herkenningmakelaar is het enige koppelvlak voor een overheidsdienstverlener met marktpartijen. Een overheidsdienstverlener dient een contract met een herkenningmakelaar te sluiten. Deze makelaar zoekt de benodigde eHerkenning-informatie op die nodig is voor de overheidsdienstverlener om de dienst te kunnen leveren. Het gaat daarbij om de informatie uit vanuit machtigingenregisters, authenticatiediensten en eventuele ondertekendiensten.

¹ Conform de beschrijving in notitie FS23-12-08 Voortgang eHerkenning voor Bedrijven van 16-12-2009

5. Ondertekendiensten. Deze rol maakt het mogelijk om documenten te voorzien van een elektronische handtekening. Nadat het te ondertekenen document aan de gebruiker wordt getoond, wordt ook hier het authenticatiemiddel gebruikt om te handtekening te zetten.

Schematisch ziet het afsprakenstelsel er als volgt uit:



2.3 Scope van de huidige versie 0.8 van het afsprakenstelsel

De versie 0.8 zoals deze op 29 maart door het kernteam van het samenwerkingsverband is geaccordeerd richt zich op eHerkenning in een webportaal. Daarbij zullen de functies authenticatie en eenvoudige machtigingen worden opgeleverd, waarmee het mogelijk wordt bedrijven te authenticeren via een handelende natuurlijk persoon die zich met een authenticatiemiddel authenticceert. In 2010 zal verder worden gewerkt aan ondertekenen, complexere machtigingen, dienstencatalogus en machine-to-machine communicatie.

In versie 0.8 van het afsprakenstelsel is de beheerorganisatie die eind 2010 ingericht moet zijn uitgewerkt. Dit beheer omvat alle facetten van het afsprakenstelsel: technisch, functioneel en ook de doorontwikkeling ervan. Daarnaast sluit de beheerorganisatie contracten met de deelnemers waarlangs het afsprakenstelsel van toepassing wordt verklaard. Voor de proefimplementaties is inmiddels een tijdelijke beheerorganisatie ingericht als onderdeel van de projectorganisatie.

De overheid zal toezicht houden op het stelsel en de marktwerking daarbinnen, gebaseerd op de eisen vanuit overheidsbeleid en regelgeving. Versie 0.8 van het afsprakenstelsel beschrijft de verhouding tussen het toepassen van al bestaande toezichtsarrangementen vanuit Nma, CBP en OPTA, de wijze waarop het publieke belang van het stelsel wordt verankerd door ministerie van Economische Zaken, de organisatie van de inbreng van overheidsdienstverleners in een Gebruikersraad en de wijze waarop de marktpartijen binnen deze kaders en binnen dat toezicht invloed hebben op het bestuur van het afsprakenstelsel en de beheerorganisatie daarvan.

Een verrekenmodel is onderdeel van het afsprakenstelsel. Dit bepaalt welk deel van de kosten op welke wijze door de overheidsdienstverleners bekostigd wordt via de contractuele relatie met de

herkenningsmakelaar en welk deel door bedrijven zelf bekostigd wordt via de aanschaf van middelen en de kosten voor registratie en beheer van machtigingen. De Staatssecretaris van Financiën heeft toegezegd de eerste jaren een tegemoetkoming aan bedrijven voor de kosten van een middel voor zijn rekening te willen nemen. Dezelfde vorm van stimulering wordt toegepast door de overheidsdienstverleners die proefimplementaties doen in 2010.

De op 29 maart 2010 door het kernteam aangenomen versie van het afsprakenstel zal op de bovenstaande onderdelen eisen stellen, standaarden voorschrijven en randvoorwaarden formuleren. Dit geheel geeft aan overheidsdienstverleners en marktpartijen voldoende richting om een aantal proefimplementaties uit te voeren en de daarbij behorende dienstverlening in te richten.

2.4 Afsprakenstelsel in breder perspectief

2.4.1 Samenhang eHerkenning en DigiD Machtiging

Het dossier authenticatie en autorisatie is breder dan eHerkenning. Eherkenning richt zich op het bedrijvendomein. In de onderstaande matrix staat beschreven hoe authenticatie zou moeten worden ingevuld en hoe autorisatie moet worden geregeld in het geval een burger of bedrijf een andere burger of bedrijf wil machtigen voor het afnemen van een dienst bij de overheid.

Daarbij gelden de volgende uitgangspunten:

		Belanghebbende (de machtigende persoon)	
		Burger	Bedrijf
Gemachtigde	Burger	A authenticceert via DigiD-burger machtigt via DigiD-Machtigen	C authenticceert via e-Herkenning machtigt via e-Herkenning
	Bedrijf	B authenticceert via e-Herkenning machtigt via DigiD-Machtigen	D authenticceert via e-Herkenning machtigt via e-Herkenning

Authenticatie:

- Voor authenticatie gebruikt een burger zijn DigiD burger
 - Voor authenticatie van een bedrijf gebruikt een medewerker van dat bedrijf eHerkenning
 -

Autorisatie:

- Als degene die zich laat vertegenwoordigen een burger is, dan dan vindt autorisatie via DigiD Machtigen plaats

– Als degene die zich laat vertegenwoordigen een bedrijf is, dan vindt autorisatie via eHerkenning plaats.

DigiD Machtigen zal als dienstverlener die eHerkenning toepast aangesloten moeten worden op eHerkenning om een burger zich te laten vertegenwoordigen door een bedrijf (kwadrant B in het schema). Kwadrant A wordt nu al door DigiD Machtiging ingevuld en kwadranten C en D vallen geheel binnen eHerkenning.

2.4.2 Samenhang eHerkenning – PKloverheid

Het programma van Eisen PKloverheid is in het proces van standaardisatie van Forum en College ingebracht. De samenhang met eHerkenning is dat authenticatiemiddelen die binnen de PKloverheid zijn uitgegeven voor eHerkenning zijn toegelaten als authenticatiemiddelen van betrouwbaarheidsniveau 4. Deze middelen kunnen gebruikt worden binnen eHerkenning zodra de betreffende middelenuitgever en bijbehorend authenticatiedienst als deelnemer tot eHerkenning toetreden. Aangezien de begrippenkaders van PKloverheid en eHerkenning gedeeltelijk overlappen dient zorgvuldig te worden gecontroleerd of deze op elkaar aansluiten.

2.4.3 DigiD Bedrijven wordt voor eind 2010 gemigreerd naar eHerkenning

De samenhang met het momenteel operationele DigiD Bedrijven is dat eHerkenning zal functioneren als een opvolger hiervan. De migratie hiervan zal mede vanuit het programma eHerkenning gefaciliteerd worden en voor eind 2010 worden afgerond.

2.4.4 Relatie met volgende generatie DigiD Burger: DigiD X

DigiD X is de volgende versie van DigiD Burger waaraan momenteel gewerkt wordt. Deze dient voorlopig backwards compatibel te zijn met de huidige DigiD koppelvlakken. DigiD X leidt niet tot wijziging van de positionering van DigiD Burger of DigiD Machtigingen ten opzichte van eHerkenning.

2.5 Vertrouwen en betrouwbaarheid eHerkenning

2.5.1 Betrouwbaarheidsniveaus zijn bepalend voor gehele keten

Vertrouwen is cruciaal voor de door eHerkenning te leveren herkenningdiensten. Maatregelen om dit vertrouwen te realiseren en te borgen kosten geld. Deze maatregelen dienen derhalve proportioneel te zijn. Dit leidt tot het bestaan van een breed spectrum en technische, procedurele- en toezichtsmaatregelen aangaande vertrouwen. Ondubbelzinnige afspraken over welke maatregelen noodzakelijk zijn voor welk type diensten zijn cruciaal voor het vertrouwen in authenticatie en autorisatieoplossingen.

Op dit gebied is momenteel Europese standaardisatie gaande die geleid heeft tot een indeling in vier betrouwbaarheidsniveaus genaamd STORK²: Een raamwerk voor “Quality Authentication Assurance”. Het is een doorontwikkeling van het Europese IDABC programma. Het afsprakenstelsel eHerkenning hanteert dit raamwerk voor de authenticatiemiddelen in het netwerk voor eHerkenning

² Het raamwerk is vastgelegd in STORK deliverable D2.3 - Quality authenticator scheme.

en past het raamwerk daarnaast, naar analogie, toe op de eisen die gesteld worden aan de registratie van machtigingen.

Betrouwbaarheidsniveau	Omschrijving
1	Geen of minimale betrouwbaarheid
2	Beperkte betrouwbaarheid
3	Redelijke betrouwbaarheid
4	Hoge betrouwbaarheid

Het hoogste niveau 4 komt overeen met de eisen die gesteld worden aan een gekwalificeerde elektronische handtekening.

2.5.2 Betrouwbaarheidsniveaus doen overheid de juiste vraag stellen

Een brede acceptatie van de STORK betrouwbaarheidsniveaus zal sterk bijdragen aan de adoptie van eHerkenning. Het netwerkmodel vereist immers dat de afspraken over betrouwbaarheid op een eenduidige manier door het hele netwerk heen worden vastgelegd: bij de bedrijven die diensten afnemen waarvoor eHerkenning vereist is, bij alle rollen binnen het netwerk voor eHerkenning en bij de overheidsdienstverleners die eHerkenning voor hun diensten toepassen. Immers, bij vertrouwen telt de zwakste schakel. Ondubbelzinnige vastlegging van de betrouwbaarheidsniveau is tevens cruciaal vanuit de scheiding tussen publiek en privaat domein bij eHerkenning. Het netwerk wordt ingevuld door private partijen en het afsprakenstelsel beschrijft aan welke eisen deze minimaal moeten voldoen. Deze eisen variëren per betrouwbaarheidsniveau. Door de wijze waarop betrouwbaarheidsniveaus geassocieerd worden van overheidswege vast te leggen worden overheidsdienstverleners in staat gesteld om een heldere vraag, “lever authenticatie op betrouwbaarheidsniveau x” te stellen. Daarnaast wordt daarmee controleerbaar of de marktpartijen een herkenningdienst leveren volgens de eisen van het gevraagde betrouwbaarheidsniveau. Het gevraagde betrouwbaarheidsniveau bepaalt tevens de kosten van de herkenningdiensten voor zowel deze overheidsdienstverlener als voor de bedrijven.

2.5.3 Standaardiseer normenkader inclusief classificatieproces

Daarbij gelden twee kanttekeningen:

- STORK biedt slechts een raamwerk en geen gedetailleerd normenkader. Dit maakt de afspraken over de wijze van classificatie en ontwikkeling van gedetailleerde normenkaders relevant.
- De vraag welk betrouwbaarheidsniveau “goed genoeg” is voor welke overheidsdienst vereist meer dan het STORK raamwerk. Het vereist in feite een operationalisering van zaken zoals de zorgvuldigheidsbeginselen in de Algemene Wet Bestuursrecht en de privacy classificaties vanuit de Wet Bescherming Persoonsgegevens naar de in STORK gedefinieerde betrouwbaarheidsniveaus.

Door niet het algemene STORK raamwerk als standaard in het proces op te nemen maar het daarvan in het kader van eHerkenning af te leiden normenkader inclusief het in het afsprakenstelsel

opgenomen proces dat bepaalt wie en hoe tegen dit normenkader classificeert, wordt aan deze kanttekeningen tegemoet gekomen.

Het uitwerken van een dergelijk normenkader en het verkrijgen van voldoende draagvlak voor de standaardisatie daarvan gaat een forse stap verder dan hetgeen daarover in de huidige versie 0.8 van het afsprakenstelsel is vastgelegd, hierbij dient in de planning en verwachtingen rekening te worden gehouden.

2.6 Koppelvlakken eHerkenning

2.6.1 Overheidskoppelvlak versus de koppelvlakken binnen het netwerk

Het netwerk voor eHerkenning leidt tot één koppelvlak dat essentieel is voor de overheid: het koppelvlak waarmee overheidssdienstverleners aansluiten op het netwerk (op de herkenningmakelaar om precies te zijn). De standaardisatie van dat koppelvlak is essentieel voor de ontwikkeling van de e-overheid.

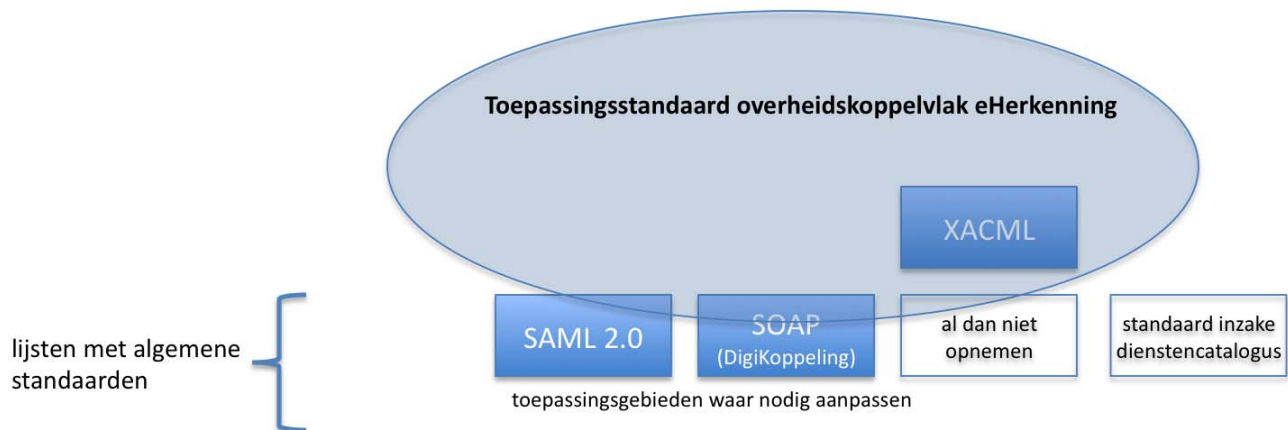
Daarnaast bestaan binnen het netwerk koppelvlakken tussen de verschillende rollen. Het afsprakenstelsel beschrijft eisen aan deze koppelvlakken. Waar mogelijk laat het afsprakenstelsel marktpartijen ruimte om hun diensten verder naar eigen inzicht in te richten. Afgezien van de boven uitgewerkte betrouwbaarheidsniveaus is verdere standaardisatie van deze interne koppelvlakken binnen het netwerk voor eHerkenning geen onderwerp voor het proces van Forum en College Standaardisatie, het betreft immers koppelvlakken tussen marktpartijen en het afsprakenstelsel is het mechanisme waarmee deze gezamenlijk (en met onafhankelijk toezicht) beslissen over de interne standaarden.

2.6.2 Te standaardiseren onderdelen van het overheidskoppelvlak

Het overheidskoppelvlak voor eHerkenning valt niet samen met één enkele technische koppelvlakstandaard. Het houdt een toepassing in waarbij meerdere technische koppelvlakstandaarden een rol spelen. Twee daarvan SAML 2.0 en SOAP komen reeds voor op de pas-toe-of-leg-uit lijst. Echter zonder dat het geformuleerde toepassingsgebied de toepassing voor eHerkenning omvat.

Naast de standaarden wordt gebruik gemaakt van de XACML standaard en wordt in de doorontwikkeling naar versie 1.0 van het afsprakenstelsel (voor september 2010) gekeken naar standaarden voor de definitie van diensten / dienstencatalogus.

Het voorstel is derhalve om voor eHerkenning de toepassingsstandaard waarin precies beschreven wordt hoe deze standaarden in hun samenhang het overheidskoppelvlak van eHerkenning invullen te standaardiseren in het proces van Forum en College.



De onderliggende technische koppelvlakstandaarden kunnen separaat daarvan voor algemenere toepassing op de pas-toe-of-leg-uit-lijst blijven staan of, indien daartoe besloten wordt, worden opgenomen. Zolang een voor het overheidskoppelvlak van eHerkenning toegepaste standaard niet op de pas-toe-of-leg-uit lijst staat blijft de standaardisatie ervan binnen de eHerkenningcontext onderdeel van de toepassingsstandaard. Voor de onderliggende standaarden die wel op de lijst zijn opgenomen geldt dat het toepassingsgebied moet worden uitgebreid tot de toepassing in het overheidskoppelvlak voor eHerkenning. Dit is vergelijkbaar met de wijze waarop bijvoorbeeld SOAP nu als technische standaard op de lijst van gangbare standaarden staat en daarnaast onderdeel is van de toepassingsstandaard DigiKoppeling WUS op de pas-toe-of-leg-uit lijst.

Om het geheel consistent te houden dient bewaakt te worden dat er geen standaarden op de pas-toe-of-leg-uit lijst komen waarvan het toepassingsgebied overlapt met het overheidskoppelvlak voor eHerkenning.

In de termen van het European Interoperability Framework is het overheidskoppelvlak voor eHerkenning een bijzonder type koppelvlak. Het betreft het koppelvlak van een generieke voorziening, eHerkenning, die door alle taakspecifieke diensten waarvoor B2G herkenningdiensten relevant zijn toegepast moet worden en niet een "business interoperability interface" tussen meerdere taakspecifieke diensten.

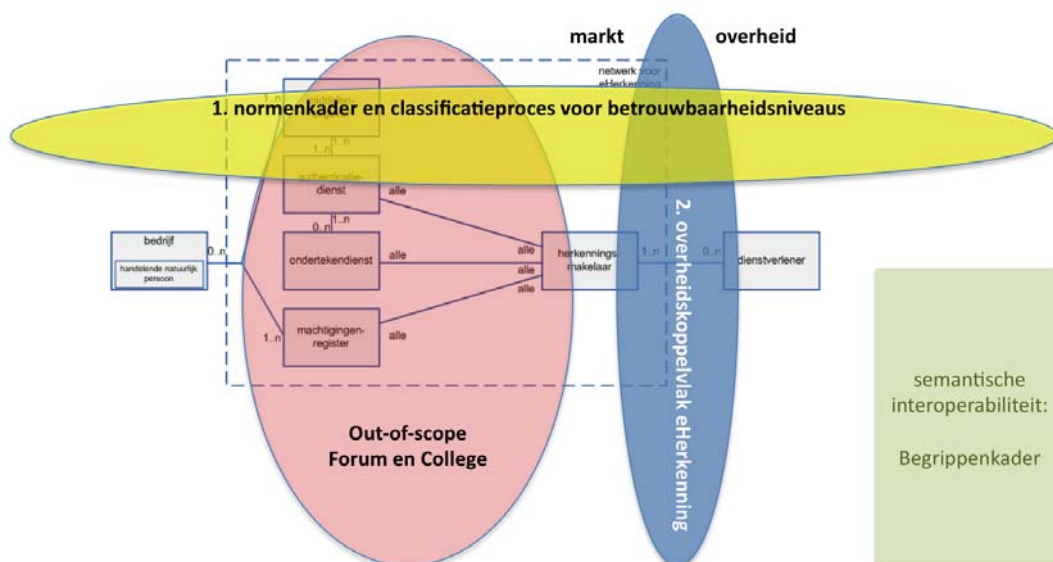
3 Analyse te standaardiseren onderdelen

Het rapport “Verkenning authenticatie” noemt drie zaken waarvan de standaardisatie tot verbetering leidt. Deze sluiten naadloos aan op het hierboven geschetste beeld. Het betreft:

- Kwaliteitsklassen voor authenticatiemiddelen (c.q. betrouwbaarheidsniveaus), waarmee de mate van zekerheid die aan het gebruik van een bepaald authenticatiemiddel mag worden ontleend voor alle betrokken partijen duidelijk is.
- De manier waarop berichten tussen de rollen en gebruikers zijn gestandaardiseerd om interoperabiliteit en concurrentie mogelijk te maken (c.q. de technische koppelvlakken).
- De gebruikte terminologie.

Dit leidt tot de volgende te standaardiseren onderdelen:

1. Een normenkader en classificatieproces voor betrouwbaarheidsniveaus dat past binnen het STORK raamwerk en dit voor eHerkenning operationaliseert.
2. Het overheidskoppelvlak voor eHerkenning dat als toepassingsstandaard exact specificeert hoe onderliggende koppelvlakstandaarden die al dan niet op de pas-toe-of-leg-uit lijst zijn geplaatst toegepast worden door overheidsdienstverleners die eHerkenning benutten.
3. Aanpassen van toepassingsgebied van reeds op pas-toe-of-leg-uit lijst opgenomen onderliggende technische koppelvlakstandaard SAML 2.0.
4. Gebruikte terminologie als onderwerp van semantische standaardisatie.
5. Overwegen om in het koppelvlak voor eHerkenning voorkomende onderliggende technische standaarden die nog niet in de pas-toe-of-leg-uit lijst staan afzonderlijk in procedure te nemen, dan wel te beoordelen of ze in aanmerking komen voor de lijst met gangbare standaarden.



De standaardisatie van onderdeel 1, de betrouwbaarheidsniveaus raakt de hele keten en vereist voldoende betrokkenheid en draagvlak. Bovendien is het gewenst de ervaringen uit meerdere (proef)implementaties verwerkt te hebben voordat er sprake kan zijn van formelere standaardisatie. De tijdslijn voor standaardiseren van onderdeel 1 dient derhalve langer te zijn en lijkt redelijkerwijs

op de tweede helft van 2011 uit te komen. Wel biedt dit dan een middel om te sturen op verdere adoptie van eHerkenning gedurende 2011.

De standaardisatie van onderdeel 2, het overheidskoppelvlak, is wel haalbaar in 2010, tenminste voor het toepassingsgebied van de nu voorziene (proef)implementaties. Dit dient dan ook de doelstelling voor een standaardisatiebesluit van het College in najaar 2010 te zijn. De semantische standaardisatie (4) is randvoorwaardelijk voor de andere twee. Het in procedure nemen van onderliggende technische standaarden kan later geschieden op basis van een onafhankelijke planning.

3.1 Consequenties van dit standaardisatie voorstel

3.1.1 Consequenties voor afsprakenstelsel eHerkenning

Het normenkader voor betrouwbaarheidsniveaus en het overheidskoppelvlak eHerkenning die gestandaardiseerd worden dienen losstaande zelfstandig leesbare delen van het afsprakenstelsel te zijn waarin de nu enigszins verspreid over versie 0.8 definitie verspreide aspecten zijn samengebracht. Hun afbakening met de rest van het afsprakenstelsel eHerkenning dient nauwkeurig vast te liggen. Met bovengenoemde tijdslijn zal het standaardisatieproces van de betrouwbaarheidsniveaus met name in 2011 inspanning vergen. De benodigde projectmatige aanpak en middelen daarvoor dienen belegd te worden.

3.1.2 Consequenties voor andere lopende standaardisaties

- De relatie tussen het standaardisatieproces voor het Programma van Eisen PKloverheid en dat voor de onderdelen van eHerkenning dient actief bestuurd te worden. De begrippenkaders dienen waar nodig op elkaar aangesloten te worden en er dient rekening mee gehouden te worden dat PKloverheid middelen naadloos binnen betrouwbaarheidsniveau 4 van eHerkenning kunnen worden toegepast.
- De relatie met relevante internationale standaardisaties is een punt van aandacht.

3.1.3 Consequenties voor de omgeving van eHerkenning

- Overheidsdienstverleners zullen het classificatieproces ten aanzien van het voor hun diensten vereiste betrouwbaarheidsniveau moeten accepteren en het overheidskoppelvlak van eHerkenning moet implementeren.
- Overheidsdienstverleners zullen het begrippenkader van eHerkenning moeten volgen conform hetgeen daarover wordt gestandaardiseerd.
- Om een Burger zich te kunnen laten vertegenwoordigen door een Bedrijf moet DigiD als overheidsdienstverlener worden aangesloten op eHerkenning, ook voor DigiD dient dan hetzelfde begrippenkader gehanteerd te worden.
- In het kader van afspraken over nummergebruik dient de verdere doorontwikkeling van het OIN als nummerformaat te worden vastgelegd en gevolgd.



4 Vraag aan Forum en College en proces

- a. Specifieke vragen:
1. Akkoord met de keuze om het afsprakenstelsel te standaardiseren in losse onderdelen met als belangrijkste twee
 - normenkader voor betrouwbaarheidsniveaus conform STORK
 - overheidskoppelvlak eHerkenningBespreken van de argumentatie om onderdelen te standaardiseren en niet het gehele afsprakenstelsel.
 2. Noodzaak om aanvullende acties te ondernemen ten aanzien van semantische interoperabiliteit van het begrippenkader. Gewenste focus en scope bespreken.
- b. Timing
- Planning is om het overheidskoppelvlak van versie 1.0 van het afsprakenstelsel in te brengen als standaard voor najaarsvergadering van 2010 en voor het standaardisatieproces van de betrouwbaarheidsniveaus een langere periode uit te trekken. Bespreken of een eerste stap ten aanzien van de betrouwbaarheidsniveau in najaar 2010 gewenst is. Deze zou niet meer kunnen zijn dan bevestiging van de keuze om het STORK raamwerk als referentiekader te hanteren.
- c. Wat stellen we voor aan het College