Forum Standaardisatie

Expertadvies Overheidskoppelvlak eHerkenning v1.4

Datum 6 augustus 2012

Colofon

Projectnaam	Expertadvies overheidskoppelvlak eHerkenning v1.4
Versienummer	1.0
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteurs	Jaap Kuipers Michael van Bekkum

Inhoud

Colofon 2

Inhoud 3

Managementsamenvatting 4

1 Doelstelling expertadvies 7

1.1 Achtergrond 7

1.2 Proces 7

1.3 Vervolg 8

1.4 Samenstelling expertgroep 8

1.5 Toelichting koppelvlak eHerkenning 9

1.6 Relatie met andere standaarden ..... ***Fout! Bladwijzer niet gedefinieerd.***

1.7 Leeswijzer 11

2 Toepassings– en werkingsgebied 12

2.1 Functioneel toepassingsgebied 12

2.2 Organisatorisch werkingsgebied 13

3 Toetsing van standaard aan criteria 14

3.1 Open standaardisatieproces 14

3.2 Toegevoegde waarde 19

3.3 Draagvlak 25

3.4 Opname bevordert adoptie 27

4 Advies aan Forum en College 31

4.1 Samenvatting van de toetsingscriteria 31

4.2 Advies aan Forum en College 32

4.3 Aanbevelingen ten aanzien van de adoptie van de standaard 33

5 Referenties 34

Managementsamenvatting

Wat is de conclusie van de expertgroep?
De expertgroep adviseert in meerderheid de standaard overheidskoppelvlak eHerkenning, versie 1.4, op te nemen op de lijst van 'pas toe of leg uit' indien aan de volgende voorwaarde is voldaan:

- Vermelden en publiceren van de bepalingen ten aanzien van intellectueel eigendomsrecht en merkrecht in aanvulling op de documentatie van de standaard.

Met als toepassingsgebied:
"Authenticatie voor webdiensten van overheidsdienstverleners aan bedrijven en organisaties en het vaststellen van de bevoegdheid voor de gevraagde dienst."

En als werkingsgebied:
"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector."

Op moment van schrijven spreken drie partijen, te weten de Belastingdienst, Logius en het Ministerie van BZK zich echter nog niet uit over opname op de lijst.

Aanvullend adviseert de expertgroep de beheerorganisatie van eHerkenning om te zorgen voor:

- Publicatie van het vastgestelde versiebeleid in aanvulling op de documentatie van de standaard.
- Inzichtelijk maken van de wijzigingen op de standaard in de verschillende versies in documentatie.
- Publiekelijk beschikbaar maken van de documentatie van de standaard zonder aanmeldingsproces.

De expertgroep heeft geen verdere risico's geïdentificeerd.

Waar gaat het inhoudelijk over?
De standaard overheidskoppelvlak eHerkenning beschrijft het koppelvlak tussen de (overheids)dienstverlener en de eHerkenningsmakelaar Via het koppelvlak ontvangen overheidsorganisaties identificatie en autorisatie informatie over vertegenwoordigers van bedrijven/organisaties ten behoeve van de toegang tot webdiensten die door dezelfde overheidsorganisaties worden geleverd.

Het eHerkenning overheidskoppelvlak is daarbij onderdeel van het afsprakenstelsel eHerkenning. Het afsprakenstelsel is een set bepalingen op basis waarvan partijen in een netwerk samenwerken om eHerkenningsdiensten te leveren. In dat netwerk nemen partijen deel die authenticatiemiddelen uitgeven, authenticatiediensten verlenen, als register voor bevoegdheden optreden en makelaarsdiensten verlenen voor eHerkenning.

Het eHerkenning overheidskoppelvlak beoogt het probleem van de diversiteit aan authenticatievoorzieningen voor losstaande overheidsdiensten op te lossen ("sleutelbos"), waardoor bedrijven als gebruiker geconfronteerd worden met vele keuzemogelijkheden en niet-

gestandaardiseerde samenhang tussen de technische koppelvlakken. In het verleden is daarbij door het Forum Standaardisatie de wens uitgesproken te komen tot betere kaders rondom identificatie, authenticatie en autorisatie[1]. eHerkenning kan een dergelijk kader bieden, conform het A3-advies van de Adviescommissie Authenticatie en Autorisatie Bedrijven[2].

Hoe is het proces verlopen?
Op 2 juli 2012 is een expertgroep met vertegenwoordigers uit bedrijfsleven en overheid bijeen gekomen. Vooraf zijn aanwezige experts en enkele anderen die niet aanwezig konden zijn, in de gelegenheid gesteld input aan te leveren. Op basis van deze input en de discussie tijdens de bijeenkomst is dit adviesrapport opgesteld.

Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces

De documentatie is na aanmelding beschikbaar, de besluitprocedure is voldoende toegankelijk, er is een bezwaarprocedure en de standaardisatieorganisatie is onafhankelijk en duurzaam. De standaard voldoet naar mening van de expertgroep echter pas aan de openheidscriteria als ook aan de volgende voorwaarde is voldaan:

- De bepalingen die gelden ten aanzien van het intellectueel eigendom (en merkrecht) moeten duidelijker worden gemaakt en moeten in aanvulling op de huidige documentatie van de standaard worden gepubliceerd.

Toegevoegde waarde

De expertgroep is van mening dat de voordelen van eHerkenning overheidskoppelvlak opwegen tegen de risico's en de nadelen: de overheidsbrede en maatschappelijke baten wegen op tegen de kosten, en privacy en beveiligingsrisico's zijn in de standaard in voldoende mate afgedekt. De standaard biedt ook meerwaarde ten opzichte van de standaard SAML v2.0. De voordelen van de standaard overheidskoppelvlak eHerkenning zijn met name terug te vinden in het terugdringen van de diversiteit in authenticatievoorzieningen en de bijdrage die dit levert aan de vermindering van interoperabiliteitsproblematiek op dit gebied. Het koppelvlak is bovendien als zelfstandig profiel bovenop SAML ook in te zetten buiten het stelsel eHerkenning om.

Er zijn alternatieven voor de standaard, maar deze zijn minder eenvoudig in gebruik, worden uitgefaseerd of kennen in veel beperktere mate inbedding in een uitwerking van afspraken en regels (zoals het afsprakenstelsel eHerkenning) om correct en interoperabel gebruik van de standaard te garanderen.

1 Forum Standaardisatie, http://www.forumstandaardisatie.nl/themas/authenticatie-en-autorisatie/
2 Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 Bedrijven) - Eindadvies, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/11/17/adviescommissie-authenticatie-en-autorisatie-bedrijven.html

Draagvlak

De expertgroep is van mening dat er voldoende draagvlak is voor de standaard: er is marktondersteuning voor de standaard door meerdere leveranciers en er is beleidsmatige ondersteuning voor eHerkenning in het iNUP en de Digitale Agenda.nl. Het aantal aangesloten aanbieders van overheidsdiensten is op moment van schrijven ongeveer 40 (met 44 overheidsdiensten) en neemt in aantal toe.

Opname bevordert de adoptie

Plaatsing op de 'pas toe of leg uit'-lijst bevestigt het door de overheid ontwikkelde en uitgevoerde beleid voor het realiseren van een landelijke herkennings-/authenticatiedienst. Een verplichting via 'pas toe of leg uit' ziet de expertgroep ook als middel om de in iNUP en Digitale Agenda gemaakte beleidsdoelen en bestuurlijke afspraken daadwerkelijk te bereiken en het gebruik van de eHerkenning standaard in de praktijk te bevorderen.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

Bij opname op de lijst is er enige overlap met de standaard SAML die al op de 'pas toe of leg uit'-lijst staat. Aanbeveling van de expertgroep aan het Forum is:

- Om aandacht te geven aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie en na te gaan hoe deze twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein.

Een aanbeveling die de expertgroep doet aan de beheerorganisatie voor eHerkenning is:

- na te gaan hoe de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd kunnen worden en waar nodig met een voorstel voor een alternatieve definitie te komen.

Een aanbeveling die de expertgroep doet aan Logius en eHerkenning gezamenlijk is:

- om de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart te brengen en waar mogelijk te verbeteren.

1 Doelstelling expertadvies

1.1 Achtergrond

In 2007 is door het kabinet besloten tot een actieplan Nederland Open in Verbinding [1]. Het doel van dit actieplan is om de informatievoorziening toegankelijker te maken, onafhankelijkheid van ICT-leveranciers te creëren en de weg vrij te maken voor innovatie.

Eén van de maatregelen van het actieplan is het gebruik van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain) [2]. Het College Standaardisatie, dat in 2006 door het kabinet is ingesteld, spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard [3]. Het College Standaardisatie wordt geadviseerd door het Forum Standaardisatie. Bureau Forum Standaardisatie ondersteunt beide instellingen.

Een veertiental experts is verzameld in een expertgroep, die de standaard heeft beoordeeld aan de hand van een aantal criteria. Deze criteria – vooraf vastgesteld door het College Standaardisatie [4] en uitgewerkt in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld.

Onderwerp van dit expertadvies is de standaard overheidskoppelvlak eHerkenning v1.4. Deze standaard is aangemeld door mevr. Paula de Winter namens ministerie EL&I voor opname op de lijst met open standaarden voor ‘pas toe of leg uit’. De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van deze standaard op de lijst, al dan niet onder bepaalde voorwaarden.

1.2 Proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- Door het Bureau Forum Standaardisatie is op 5 maart 2012 een intakegesprek gevoerd met de indiener. Hierin is de standaard getoetst op uitsluitingscriteria (‘criteria voor in behandelname’) en is een eerste inschatting gemaakt van de kansrijkheid voor opname.
- Op basis van de intake is besloten tot het instellen van een expertgroep. Op basis van dit besluit is door het Bureau Forum Standaardisatie een groep samengesteld en een voorzitter aangezocht. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor leden van de expertgroep.
- De expertgroep is begonnen met het individueel scoren van de standaard overheidskoppelvlak eHerkenning v1.4 aan de hand van een spreadsheet met vragen in het voorbereidingsdossier. Op basis van de verkregen antwoorden hebben voorzitter en begeleider van de expertgroep de verschillende knelpunten geïdentificeerd.
- Vervolgens is de expertgroep op 2 juli 2012 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit advies rapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om reactie. Na verwerking van de reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend voor de publieke consultatieronde.

1.3 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard de 'pas toe of leg uit'-lijst komt.

1.4 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden dhr. Jaap Kuipers. Hij heeft 10 jaar ervaring op het gebied van authenticatievoorzieningen, onder andere in relatie tot eHerkenning, DigiD en andere grootschalige voorzieningen. Hij is initiatiefnemer van het Platform Identity Management Nederland en onafhankelijk identity management adviseur voor onder andere ECP.nl en internationale projecten.

De expertgroep is in opdracht van het Forum Standaardisatie begeleid door dhr. Michael van Bekkum, adviseur standaarden en interoperabiliteit bij TNO.

Aan de expertgroep hebben deelgenomen:

- Dhr. Jeroen de Beer (Anoigo)
- Dhr. Siem de Bruijn (Digidentity)
- Mevr. Nicole Damen (Beheerorganisatie eHerkenning)
- Mevr. Welmoed Fokkema (Logius)
- Dhr. Peter Johan Groeneveld (CapGemini)
- Dhr. Indra Henneman (Beheerorganisatie eHerkenning)
- Dhr. Gershon Janssen (Aviation Industry)
- Dhr. Martijn Kaag (Connectis)
- Dhr. Wim Kegel (Logius)
- Dhr. Saam de Mooij (Min. BZK)
- Dhr. Hans Rob de Reus (Belastingdienst)
- Dhr. Ronald Siemonsma (CJIB)
- Dhr. Michael Stoelinga (Beheerorganisatie eHerkenning)
- Dhr. Kick Willemse (Evidos)

Als toehoorders waren aanwezig:
- Dhr. Nico van Baarsen (HEC)
- Mevr. Marjolein Minderhoud (HEC)
- Dhr. Mano Radema (HEC)
- Maarten van der Veen (Logius, Bureau Forum Standaardisatie)

Daarnaast is door een aantal mensen een inhoudelijke bijdrage geleverd door het individueel scoren van de standaard of door het geven van een schriftelijke reactie in algemene zin:
- Dhr. Maurice van Erven (KING)
- Dhr. Bob Hulsebosch (Novay)
- Dhr. Hans Zandbelt (Ping Identity)

Hun bijdrage is meegenomen in de discussie in de expertgroep.

1.5 Toelichting koppelvlak eHerkenning

De standaard overheidskoppelvlak eHerkenning v1.4 beschrijft het koppelvlak tussen een (overheids)dienstverlener en de eHerkenningsmakelaar. Via het koppelvlak ontvangen overheidsorganisaties identificatie-, authenticatie- en autorisatieinformatie'over bedrijven en organisaties en hun vertegenwoordigers, ten behoeve van de toegang tot webdiensten die door dezelfde overheidsorganisaties worden geleverd.

Het eHerkenning overheidskoppelvlak v1.4 is een onderdeel van het afsprakenstelsel eHerkenning. Het afsprakenstelsel eHerkenning is het geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek. procedures en regels voor een netwerk van samenwerkende partijen. In dat netwerk nemen partijen deel die authenticatiemiddelen uitgeven, authenticatiediensten verlenen, als register voor bevoegdheden optreden en makelaarsdiensten verlenen voor eHerkenning.

eHerkenning is een gestandaardiseerd, elektronisch middel voor de authenticatie van bedrijven en organisaties, wanneer zij digitaal diensten afnemen van (overheids)dienstverleners (zoals DigiD dat authenticatiemiddel nu al is voor burgers). eHerkenning maakt het bij de uitwisseling van deze gegevens mogelijk om de betrokken partijen te authenticeren, identificeren en autoriseren.

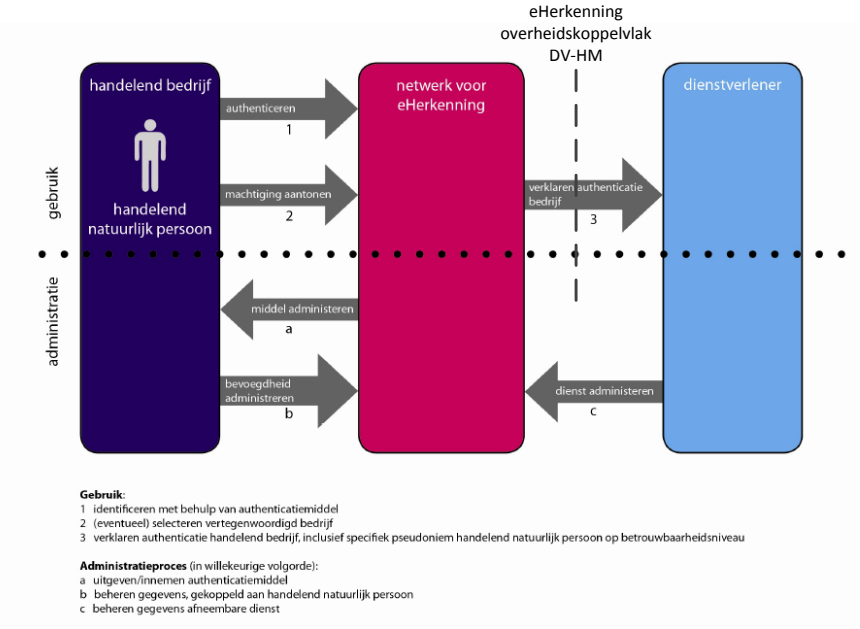
Iedere dienstverlener die aan de eisen voldoet, kan op eHerkenning aansluiten. Omdat de huidige (eerste) dienstverleners overheidsdienstverleners zijn, verstaan we binnen de scope van dit rapport onder de term dienstverlener tevens overheidsdienstverlener.

Het eHerkenning stelsel beoogt het probleem van de diversiteit aan authenticatievoorzieningen voor losstaande overheidsdiensten op te lossen ("sleutelbos"). Hierbij worden bedrijven als gebruiker geconfronteerd met vele keuzemogelijkheden en niet-gestandaardiseerde samenhang tussen de technische koppelvlakken. Bedrijven en andere organisaties kunnen met eHerkenning bij meerdere dienstverleners terecht en hebben daarbij niet meer voor iedere taak een ander authenticatiemiddel nodig. De dienstverlener op zijn beurt weet door eHerkenning met welke dienstafnemer (bedrijf) zij zaken doet en of de betreffende persoon

bevoegd is om namens die dienstafnemer zaken te doen met de dienstverlener. Zelf hoeft de dienstverlener daarvoor geen eigen authenticatiemiddel uit te geven en te beheren.

Het afsprakenstelsel eHerkenning bevat bepalingen over de te leveren dienstverlening, de soorten rollen in het netwerk en de relaties tussen die rollen. Verder bevat het afspraken over de precieze werking van het netwerk: technische relaties, ondersteunde functionaliteit, kwaliteit van gegevens en dienstverlening. Ook zijn afspraken opgenomen over de onderliggende infrastructuur: welke standaarden worden gehanteerd, en welke berichten en koppelvlakken worden ondersteund.

De standaard overheidskoppelvlak eHerkenning v1.4 beschrijft het koppelvlak tussen de (overheids)dienstverlener en de eHerkenningsmakelaar binnen het stelsel. De eHerkenningsmakelaar levert eHerkenningsdiensten op basis van het netwerk voor eHerkenning aan de overheidsdienstverlener. Het koppelvlak wordt daarbij door elke eHerkenningsmakelaar geïmplementeerd en aangeboden aan haar gebruikers, de dienstverleners. Het koppelvlak implementeert de use case "Authenticatie handelende dienstafnemer"[3]. In deze use case worden de identiteit van de handelende dienstafnemer, de (pseudo-)identiteit van de handelende natuurlijk persoon en de vertegenwoordigingsbevoegdheid van de handelende natuurlijk persoon namens de handelend dienstafnemer vastgesteld[4]. De eHerkenningsmakelaar geeft hierover een verklaring af aan de dienstverlener. De plaats van het koppelvlak in het stelsel eHerkenning is weergegeven in onderstaande figuur.



Figuur 1 Plaats van eHerkenning overheidskoppelvlak in stelsel eHerkenning[5]

3 "Afsprakenstelsel eHerkenning v1.4, Use cases", op te vragen via www.eherkenning.nlof info@eherkenning.nl

4 Deze begrippen worden toegelicht in het begrippenkader in "Afsprakenstelsel eHerkenning v1.4, Algemene Introductie", www.eherkenning.nl

5 Op basis van "Afsprakenstelsel eHerkenning v1.4, Algemene Introductie", p15, www.eherkenning.nl

1.6 Relatie met andere standaarden

Er bestaat een relatie met een aantal andere standaarden[6]:

die voorkomen op de lijst met open standaarden voor 'pas toe of leg uit':
- *SAML*
  Het eHerkenning koppelvlak is een specifiek profiel op SAML v2.0, een op XML gebaseerde standaard voor het uitwisselen van identiteitsinformatie zoals authenticatie, bevoegdheden en attributen tussen verschillende domeinen.
- *ISO27001 / 27002*
  Het eHerkenning koppelvlak heeft geen directe relatie met ISO27001/27002, dat eisen specificeert voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. In het ontwerp van het stelsel is wel rekening gehouden met de doelstelling om certificering realiseerbaar te maken in systemen die het afsprakenstelsel implementeren.

die voorkomen op de lijst met gangbare open standaarden:
- *HTTP*
  in eHerkenning wordt gespecificeerd welke bindings van SAML 2.0 worden verplicht (HTTP POST verplicht, anderen optioneel).
- *SHA-2*
  In eHerkenning wordt (minimaal) gebruik gemaakt van het SHA-256 hashing algoritme (onderdeel van de SHA-2 familie).
- *TLS*
  Alle verbindingen voor het eHerkenning koppelvlak moeten gebruik maken van SSL 3.0 of TLS.
- *XML*
  eHerkenning maakt gebruik van XML voor de specificatie van de berichten die via de koppelvlakken worden uitgewisseld.
- *UTF-8*
  Voor alle berichten die via het eHerkenning koppelvlak worden uitgewisseld, moet gebruik worden gemaakt van de Unicode character set UTF-8 encodering.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor 'pas toe of leg uit', is deze getoetst aan een viertal door het College Standaardisatie vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing. Hoofdstuk 4 bevat een samenvatting van de toets resultaten en het advies van de expertgroep aan het Forum Standaardisatie.

6 Overzicht gebruikte standaarden, "Afsprakenstelsel eHerkenning v1.4, Algemene Introductie", p49

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het "pas toe of leg uit"-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruikt moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

De expertgroep heeft voor het toepassingsgebied van het eHerkenning overheidskoppelvlak een aantal kenmerken en uitgangspunten vastgesteld:

- De standaard richt zich voor de overheid op de authenticatie ten behoeve van elektronische dienstverlening.
- De standaard is van toepassing op ontsluiting van elektronische dienstverlening via webtechnologie.
- Dienstverlening betreft zowel informatiediensten, interactiediensten als transactiediensten7 waarbij authenticatie is vereist.
- Het eHerkenning overheidskoppelvlak moet worden toegepast Op het koppelvlak tussen (overheids)dienstverlener en herkenningsmakelaar.
- Voor uitwisseling van authenticatiegegevens namens bedrijven, met een daarbij behorende machtigingsverklaring.

Als functioneel toepassingsgebied wordt daarom voorgesteld:

"Authenticatie voor webdiensten van overheidsdienstverleners aan organisaties en het vaststellen van de bevoegdheid voor de gevraagde dienst."

Toelichting op de definitie:

- Onder organisaties verstaan wordt hier verstaan: natuurlijke en niet-natuurlijke personen die zijn ingeschreven in een handelsregister. Dat wil zeggen dat het naast ondernemingen ook bijvoorbeeld verenigingen, stichtingen en (onderdelen van) overheidsorganisaties kan betreffen. De toepassing beperkt zich tot het koppelvlak tussen de aanbieders van herkenningsdiensten en de bovengenoemde overheidsdienstverleners.
- De bevoegdheid wordt vastgesteld aan de hand van de via het koppelvlak uitgewisselde machtigingsgegevens, inclusief een verklaring over de bevoegdheid van de handelende, natuurlijke persoon.

7 Er zijn verschillende manieren om elektronische overheidsdiensten te classificeren, deze manier van classificeren is voor de Nederlandse overheid een gangbare, en omvat bijvoorbeeld voorlichting en instructies (informatiediensten), betalingen en registraties (transactiediensten) en communicatie via e-mail of chat(interactiediensten). In voorkomende gevallen definiëren sommige overheden registraties via bijvoorbeeld formulieren ook wel als informatiedienst in plaats van transactiedienst.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is, te weten:

"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector."

Bovenstaande omschrijving van het werkingsgebied bevat naar de mening van de expertgroep direct of indirect alle relevante partijen op wie de standaard van toepassing is. De expertgroep zag geen reden om bovenstaand werkingsgebied verder in te perken.

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden zijn deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Open standaardisatieproces
2. Toegevoegde waarde
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingsprocedure en criteria voor lijsten met open standaarden"* [2] en staan op de website www.open-standaarden.nl. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen.

3.1 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.1.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.1.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?

3.1.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?

Zowel het specifcatiedocument als de overige documentatie zijn na aanmelding zonder kosten te downloaden via de website www.eherkenning.nl. Voor verkrijgen van de documentatie is geen lidmaatschap vereist.

De expertgroep constateert dat het wenselijk is dat de documentatie publiekelijk beschikbaar wordt gemaakt zonder aanmeldingsproces, omdat de aanmeldingsprocedure en de gegevens die nu bij aanmelding worden verzameld geen evidente bijdrage leveren aan adoptie van de standaard.

3.1.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is

3.1.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-

free voor eenieder beschikbaar?

Onderdeel van de privaatrechtelijke bepalingen in het Juridisch kader van het afsprakenstelsel eHerkenning[8], is dat alle intellectuele eigendomsrechten van zaken die door de beheerorganisatie zijn ontwikkeld, toekomen aan de beheerorganisatie dan wel diens licentiegevers. Als non-profit organisatie die het volledige afsprakenstelsel openbaar maakt staat de beheerorganisatie in voor de beschikbaarheid.

Er zijn geen beperkingen op het gebruik van de standaard in andere domeinen. Aan het gebruik van de merknaam eHerkenning zijn wel beperkingen opgelegd. Het recht op gebruik van het merk eHerkenning is gebonden aan de voorwaarden dat een Deelnemer aan alle verplichtingen, inclusief die van het koppelvlak, van het afsprakenstelsel voldoet en de Deelnemersovereenkomst heeft ondertekend. Als nu alleen het koppelvlak DV-HM wordt gebruikt buiten het afsprakenstelsel en er worden aanpassingen in doorgevoerd is dit geen probleem, mits dit maar niet onder de noemer van eHerkenning wordt gebruikt.

Ten aanzien van het gebruik van SAML binnen de standaard overheidskoppelvlak eHerkenning, gelden verder de bepalingen zoals die in de Intellectual Property Rights (IPR) policy van OASIS zijn vermeld[9]. Verder heeft de toenmalige expertgroep in het expertadvies voor SAML 2.0[10], ten aanzien van het intellectuele eigendomsrecht ook al opgemerkt dat *"in voldoende mate aan dit criterium wordt voldaan, hoewel strikt genomen patenten niet onherroepelijk ter beschikking worden gesteld."*

Voordat naar de mening van de expertgroep aan dit criterium is voldaan, dient één punt met betrekking tot beheer te worden opgelost:

- De bepalingen die gelden ten aanzien van het intellectueel eigendom (en merkrecht) moeten duidelijker worden gemaakt en moeten in aanvulling op de huidige documentatie van de standaard worden gepubliceerd.

3.1.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Er gelden ten aanzien van bijdragen door partijen die betrokken zijn bij de ontwikkeling van de standaard, geen andere bepalingen dan hierboven vermeld. Dat wil zeggen, dat deze bijdragen beschikbaar worden gesteld, met eerdergenoemd voorbehoud ten aanzien van de merknaam eHerkenning.

3.1.3 Is de inspraak van eenieder in voldoende mate geborgd?

8 eHerkenning - Juridisch Kader versie 1.4, http://www.eherkenning.nl
9 IPR policy OASIS Security Services (SAML) TC, https://www.oasis-open.org/committees/security/ipr.php
10 Expertadvies en consultatiedocument SAML 2.0, http://forumstandaardisatie.nl/fileadmin/os/documenten/OS_Consultatiedocument_SAML.pdf

3.1.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

De deelnemende partijen in eHerkenning hebben zeggenschap over de inhoud en ontwikkeling van alle onderdelen van het afsprakenstelsel eHerkenning, waaronder het overheidskoppelvlak. Deze zeggenschap door partijen binnen het Afsprakenstelsel eHerkenning vindt plaats op strategisch, tactisch en operationeel niveau, zoals vastgelegd in het "Instellingsbesluit besturing eHerkenning" [11] Op deze drie niveaus zijn drie overlegorganen ingesteld: de Stelselraad, het Tactisch Overleg en het Operationeel Overleg. In deze gremia zitten de betrokken partijen bij eHerkenning aan tafel, via een afvaardiging van deelnemers (partij die één of meer rollen vervult binnen het netwerk voor eHerkenning), dienstverleners (partij die conform het Afsprakenstelsel eHerkenning elektronische diensten aanbiedt) en gebruikers (partij die die conform het Afsprakenstelsel eHerkenning elektronische diensten afneemt). Deze gremia adviseren over de inhoud en ontwikkeling van het Afsprakenstelsel eHerkenning.

Toetreding tot deze gremia is vastgelegd in het Juridisch kader eHerkenning v1.4. Daarbij kunnen belanghebbenden toetreden tot gebruiksgroepen. Deze hebben formeel geen zeggenschap, maar krijgen deze zeggenschap via vertegenwoordiging (benoeming) in de bovengenoemde groep van gebruikers in de drie gremia.

Daarnaast kunnen Stelselraad en Tactisch Overleg werkgroepen inrichten, die hen kunnen adviseren ten aanzien van strategische, operationele en tactische onderwerpen. Tenslotte kunnen belanghebbenden die geen partij zijn in eHerkenning, via een deelnemer dan wel de voorzitter van de Stelselraad, inbreng leveren op basis van vooraf gepubliceerde agenda en stukken.

3.1.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

De besluitvorming in de drie overlegorganen vindt op de volgende manier plaats, zoals vastgelegd in het instellingsbesluit:

1. Zowel de Stelselraad, als het Tactisch Overleg als het Operationeel Overleg beslist over zaken bij meerderheid van het aantal uitgebrachte stemmen.
2. De voorzitter van het betreffend overlegorgaan heeft geen stem. De mogelijk aanwezige waarnemer in de Stelselraad heeft eveneens geen stem. De andere leden kunnen ieder één stem uitbrengen.
3. Bij staking van de stemmen is het voorstel verworpen.

3.1.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

11 Instellingsbesluit besturing eHerkenning, https://zoek.officielebekendmakingen.nl/stcrt-2012-13382.html

Er is momenteel een formele bezwaarprocedure voor belanghebbenden, vastgelegd als onderdeel van het juridisch kader in het stelsel eHerkenning. Bezwaren tegen het standaardisatieproces kunnen verder worden ingebracht via een deelnemer, dan wel de voorzitter van de Stelselraad. Omdat eHerkenning een privaatrechtelijke organisatie betreft, is uiteindelijk een gang naar de rechter ook mogelijk.

3.1.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? (geen harde voorwaarde)

De verschillende overlegorganen hebben elk een eigen cyclus voor bijeenkomsten, zoals vastgelegd in het instellingsbesluit:

- De Stelselraad komt ten minste vier keer per jaar bijeen (Artikel 6).
- Het Tactisch Overleg komt maandelijks bijeen (Artikel 17).
- Het Operationeel Overleg komt bijeen wanneer de voorzitter dit nodig acht om te adviseren over de implementatie van wijzigingen en releases in het Afsprakenstelsel eHerkenning (Artikel 25).

3.1.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? (geen harde voorwaarde)

De agenda en bijhorende de schriftelijke stukken van zowel Stelselraad, Tactisch Overleg als operationeel Overleg worden voorafgaand aan bijeenkomsten beschikbaar gesteld aan alle deelnemers, dienstverleners en gebruikers voor consultatie. De standaardisatieorganisatie organiseert echter geen brede publieke consultatie voordat een nieuwe versie van de standaard wordt vastgesteld.

3.1.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.1.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

De standaard wordt onderhouden door een beheerorganisatie, waarvan het ministerie van Economische Zaken, Landbouw en Innovatie initiatiefnemer is. De organisatie die de standaard eHerkenning per 1 september 2012 in beheer krijgt, Logius, is een organisatie die in 2006 is opgericht onder de naam GBO.Overheid[12].

3.1.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Voor Logius is er tot en met 2014 budget gereserveerd voor de ontwikkeling en het onderhoud van de standaard. Het ministerie van EL&I heeft zich garant gesteld voor de financiering. Financiering wordt per jaar nader bepaald op basis van plannen van de beheerorganisatie.

12 Zoals vastgesteld in het instellingsbesluit besturing eHerkenning, https://zoek.officielebekendmakingen.nl/stcrt-2012-13382.html

De expertgroep is van mening, dat onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie in voldoende mate zijn verzekerd.

3.1.5 Is het (versie) beheer van de standaard goed geregeld?

3.1.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)

Het versiebeheer voor de standaard is vastgelegd in het Operationeel Handboek Afsprakenstelsel eHerkenning. Er is een halfjaarlijkse releasecyclus voorgesteld voor zowel de standaard als het hele stelsel. Met een RFC zal vanaf versie v1.5 van de standaard de halfjaarlijkse releasecyclus opgenomen zijn in de procedure met een verwijzing naar een eventuele spoedprocedure.

De expertgroep stelt voor om dit vastgestelde versiebeleid in aanvulling op de huidige documentatie ook voor versie 1.4 van de standaard te publiceren; dit schept verdere duidelijkheid richting gebruikers van de standaard.

3.1.5.2 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard? (Dit is het geval als de standaardisatieorganisatie uitstekend scoort op de voorgaande deelvragen)

Voordat het standaardisatieproces voldoende goed is geregeld, moet naar mening van de experts aan drie voorwaarden worden voldaan:

- De bepalingen die gelden ten aanzien van het intellectueel eigendom (en merkrecht) moeten duidelijker worden gemaakt en moeten in aanvulling op de huidige documentatie van de standaard worden gepubliceerd.

3.1.6 Conclusie

De documentatie is na aanmelding beschikbaar, de besluitprocedure is voldoende toegankelijk, er is een bezwaarprocedure en de standaardisatieorganisatie is onafhankelijk en duurzaam. De standaard voldoet naar mening van de expertgroep echter pas aan de openheidscriteria als ook aan de volgende voorwaarde is voldaan:

- De bepalingen die gelden ten aanzien van het intellectueel eigendom (en merkrecht) moeten duidelijker worden gemaakt en moeten in aanvulling op de huidige documentatie van de standaard worden gepubliceerd.

De expertgroep adviseert de beheerorganisatie eHerkenning aanvullend te zorgen voor:

- Publicatie van het vastgestelde versiebeleid in aanvulling op de documentatie van de standaard.

- Inzichtelijk maken van de wijzigingen op de standaard in de verschillende versies in documentatie.
- Publiekelijk beschikbaar maken van de documentatie van de standaard zonder aanmeldingsproces.

3.2 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.2.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.2.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Binnen het in hoofdstuk 2 voorgestelde toepassingsgebied van eHerkenning is functionaliteit geselecteerd die in de praktijk van de standaard volledig ondersteund en al toegepast wordt. Naar de mening van de expertgroep zijn er geen functies in dit toepassingsgebied benoemd die de standaard niet ondersteunt.

3.2.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het in hoofdstuk 2 voorgestelde organisatorische werkingsgebied bevat naar mening van de expertgroep alle relevante partijen op wie de standaard van toepassing kan worden verklaard binnen de scope van de lijst met open standaarden voor "pas toe of leg uit".

3.2.1.3 Is de standaard generiek toepasbaar en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke voorzieningen?

De standaard eHerkenning overheidskoppelvlak is generiek toepasbaar voor alle overheidswebdiensten. De standaard heeft grote waarde voor realisatie van interoperabiliteit binnen het Afsprakenstelsel eHerkenning, maar kent ook daarbuiten toegevoegde waarde. Het ontleent daarbij meerwaarde aan de profilering van SAML.

3.2.2 Verhoudt de standaard zich goed tot andere standaarden?

3.2.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

Het voorgestelde toepassingsgebied overlapt deels met het toepassingsgebied van SAML, dat ook op de lijst voor "pas toe of leg uit" staat. Het toepassingsgebied van SAML is gedefinieerd door:

> *"Federatieve (web)browser-based single-sign-on (SSO) en single-sign-off. Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen."*

eHerkenning is een specifieke toepassing (profiel) van SAML.

Waar SAML zich veeleer richt op het na eenmalige login verkrijgen van toegang tot verschillende diensten van verschillende partijen (SSO), richt het overheidskoppelvlak eHerkenning zich op enkelvoudige toegang tot een dienst. De overlap zit daarbij in het verschaffen van toegang tot dienstverlening op basis van authenticatiegegevens.

Op basis van bovenstaande, beveelt de expertgroep de beheerorganisatie van eHerkenning aan, de toepassingsgebieden van beide standaarden beter met elkaar in samenhang te brengen.

Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

De standaard eHerkenning overheidskoppelvlak biedt een profiel op de standaard SAML v2.0, waarbij een aantal keuzes is gemaakt ten aanzien van gebruik van deze laatste standaard. Deze keuzes in eHerkenning beperken dus de keuzevrijheid in SAML voor het vastgestelde toepassingsgebied. Oplossingen die voldoen aan eHerkenning zijn daardoor beter interoperabel met elkaar, waar niet-gestandaardiseerd gebruik van SAML v2.0 kan leiden tot niet-interoperable keuzes en maatwerk tussen partijen.

3.2.2.2 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Potentieel concurrerende standaarden en oplossingen voor de standaard eHerkenning overheidskoppelvlak zijn:

- *Niet gestandaardiseerde oplossingen van één overheidsdienstverlener*
  De meerwaarde van eHerkenning is gelegen in de standaardisatie op één koppelvlak binnen eHerkenning, waardoor het probleem van de diversiteit aan authenticatievoorzieningen wordt verkleind.

- *Authenticatie op basis van PKIoverheid certificaten (PKI)*
  De meerwaarde van eHerkenning is gelegen in de grotere eenvoud in gebruik. Daarnaast is PKI als oplossing voor een van de betrouwbaarheidsniveaus voor authenticatie in te zetten als authenticatiemiddel binnen eHerkenning, er is dus sprake van compatibiliteit (betrouwbaarheidsniveau 4).

- *A-Select standaard van DigiD*
  De meerwaarde van eHerkenning is gelegen in het feit dat eHerkenning zich baseert op een internationale standaard (SAML), die bovendien al op de lijst voor "pas toe of leg uit" staat. Daarnaast wordt A-Select momenteel uitgefaseerd.

Standaarden, die raken aan het toepassingsgebied van de standaard en zijn genoemd in de discussie van de expertgroep, zijn de volgende:

- *XACML*[13]
  XACML, een afkorting voor "eXtensible Access Control Markup Language", maakt het mogelijk om tot op een zeer diep detailniveau de autorisatie van gebruikers en systemen te definiëren en af te dwingen. De expertgroep die zich heeft gebogen over WS-Policy en XACML[14], heeft eerder al aangegeven dat XACML voor autorisatiedoeleinden in aanvulling op het SAML ingezet zou kunnen worden. Het overheidskoppelvlak eHerkenning maakt echter geen gebruik van XACML.

- *OAuth*[15]
  Een standaard die een autorisatie raamwerk specificeert, dat het mogelijk maakt dat toepassingen van derden toegang krijgen tot webdiensten en resources. De toepassing van OAuth is veeleer gelegen in het consumentendomein en de individuele gebruiker en veel minder in het zakelijke domein. Een populaire standaard voor het verlenen van toegang tot toepassingen in het consumenten domein, die is gebaseerd op de OAuth 2.0 standaard, is OpenID Connect[16].

- *STORK*[17]
  Een Europees project waarin een raamwerk met een stelsel van betrouwbaarheidsniveaus is ontwikkeld. Ten behoeve van interoperabiliteit binnen de Europese Unie baseert het netwerk voor eHerkenning haar terminologie en processen voor betrouwbaarheidsniveaus op het STORK raamwerk.

3.2.2.3 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)

De standaard eHerkenning overheidskoppelvlak is geen internationale standaard, maar biedt een profiel bovenop de (internationale) SAML v2.0 standaard.

3.2.2.4 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn? (toelichtende vraag)

Het eHerkenning overheidskoppelvlak biedt een specificatie voor technische interoperabiliteit op basis van een SAML profiel. In het expertadvies voor SAML v2.0 is vastgesteld dat additionele afspraken de interoperabiliteit van SAML verder vergroten. In het overheidskoppelvlak eHerkenning wordt nu juist een aantal keuzes gemaakt, die vormgeven aan dergelijke afspraken. Een aantal aanvullende afspraken is nog wel noodzakelijk om juist en interoperabel gebruik van het eHerkenning overheidskoppelvlak te waarborgen. De extra afspraken die benodigd zijn om juist en interoperabel gebruik van het koppelvlak in de praktijk te waarborgen en interoperabiliteit te ondersteunen, zijn vastgelegd in het

13 https://www.oasis-open.org/standards#xacmlv2.0
14 http://lijsten.forumstandaardisatie.nl/open-standaard/ws-policy
15 http://tools.ietf.org/html/draft-ietf-oauth-v2-31
16 http://openid.net/connect/
17 https://www.eid-stork.eu

afsprakenstelsel eHerkenning. Het afsprakenstelsel beschrijft de voorwaarden voor interoperabiliteit op semantisch, juridisch en organisatorisch gebied.

Naar mening van de expertgroep draagt de standaard bij aan verbetering van interoperabiliteit, juist omdat het invulling geeft aan een aantal keuzevrijheden die bij inzet van SAML bestaan.

3.2.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

3.2.3.1 Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?

Het eHerkenning overheidskoppelvlak beoogt het probleem van de diversiteit aan authenticatiekoppelvlakken voor losstaande overheidsdiensten op te lossen ("sleutelbos"). Hierbij worden overheidsdienstverleners geconfronteerd worden met vele keuzemogelijkheden en niet-gestandaardiseerde samenhang tussen de technische koppelvlakken. Bedrijven en andere organisaties kunnen met eHerkenning bij meerdere dienstverleners terecht en hebben daarbij niet meer voor iedere taak een ander authenticatiemiddel nodig. De dienstverlener op zijn beurt weet door eHerkenning met welke dienstafnemer (bedrijf) zij zaken doet en of de betreffende persoon bevoegd is om namens die dienstafnemer zaken te doen met de dienstverlener.

Tegelijkertijd merkt de expertgroep op dat het eHerkenning overheidskoppelvlak bijdraagt aan verdere oplossing van het interoperabiliteitsprobleem rondom authenticatie. In het expertadvies voor SAML v2.0 is ook al vastgesteld dat additionele afspraken zoals die voor het overheids koppelvlak zijn gemaakt, de interoperabiliteit van SAML verder vergroten. Doordat eHerkenning een SAML profiel is, zullen niet alle bestaande SAML implementaties interoperabel zijn met het eHerkenning koppelvlak: dit is echter inherent aan het gebruik van SAML.

De inzet van eHerkenning kan naar mening van de expertgroep ook worden gezien worden als een stap naar nog verdergaande integratie van authenticatiediensten voor overheidsdienstverlening voor de samenleving als geheel (zowel burgers als bedrijven). Het gebruik van DigiD in het burgerdomein legitimeert weliswaar andere keuzes ten aanzien van SAML, maar (ondermeer) consistentie in een aantal technische keuzes zou naar mening van de expertgroep de samenhang tussen DigiD en eHerkenning kunnen vergroten.

3.2.3.2 Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?

Doordat eHerkenning een koppelvlak biedt op basis waarvan meerdere partijen authenticatiediensten kunnen verlenen, kunnen overheidsdienstverleners als gebruiker zonder problemen overstappen naar een andere partij. Daarmee wordt vendor lock-in voorkomen.

Hoewel de aanbieders van dit koppelvlak momenteel hoofdzakelijk uit het Nederlandse bedrijfsleven afkomstig zijn, is er geen belemmering voor buitenlandse bedrijven om het koppelvlak in te zetten (of deelnemer te worden in het hele stelsel).

3.2.3.3 Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?

Voor de diverse maatschappelijke sectoren zijn baten en lasten als volgt te typeren voor het overheidskoppelvlak eHerkenning:

- *Overheidssector (dienstenleveranciers)*: de kosten voor overheidsorganisaties zitten in aansluitkosten (kosten voor het koppelvlak) ,abonnementskosten bij een eHerkenningsmakelaar voor verwerking van transacties en de kosten die gemaakt moeten worden om de dienstverlening achter eHerkenning (digitaal) te ontsluiten (bijvoorbeeld in de vorm van ontwikkelen van digitale inzage en transactiemogelijkheden i.p.v. papier). In de vorm van vermeden kosten zullen baten optreden als besparingen in investeringen voor diverse koppelvlakken en besparingen op aanschaf en beheer van meerdere authenticatiemiddelen.
- *Bedrijven*: bedrijven ondervinden kosten doordat ze genoodzaakt worden om authenticatiemiddelen aan te schaffen om van het koppelvlak (en de elektronische dienstverlening) gebruik te kunnen maken. Ook wordt een jaarlijkse bijdrage betaald voor gebruik van deze middelen. De verwachting is dat bedrijven daarentegen administratieve lastenverlichting zullen ervaren door overstap van papieren naar digitale transacties en het gebruik van één sleutel.
- *Burgers*: eHerkenning is niet op gebruik door burgers van toepassing (voor niet-zakelijke doeleinden).

Uit een kosten baten analyse die uitgevoerd is voor het hele afsprakenstelsel eHerkenning door Ecorys in 2011[18], blijkt dat over de voorgestelde tijdshorizon (2011-2015), de baten de kosten ruim overstijgen (tientallen miljoenen).

Naast de gemonetariseerde baten worden er ook niet-geldelijke baten onderkend:

- Toename Business to Business (B2B) activiteiten
- Toename Government to Government (G2G) activiteiten
- Verbetering van de betrouwbaarheid door hoger betrouwbaarheidsniveau.

De belangrijkste kosten zitten in de voorgestelde periode in beheer (twee maal de invoeringskosten). De belangrijkste (gekwantificeerde) voordelen van de invoering van eHerkenning hebben betrekking op de administratieve lastenverlichting bij bedrijven en vermeden kosten en efficiencyvoordelen bij de overheidsdienstverleners. Doordat er een standaard komt in de vorm van eHerkenning zullen ontwikkel- en beheerkosten eveneens dalen (vermeden kosten).

Naar mening van de expertgroep wegen daarmee de baten op tegen de kosten.

18 Kosten-batenanalyse eHerkenning Eindrapport, Ecorys, 22 april 2011

3.2.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

In een onderzoek naar veiligheid van eHerkenning[19] uitgevoerd in opdracht van het Ministerie van EL&I, is gesteld dat voor de werking van eHerkenning er een 'noodzakelijk vertrouwen' moet bestaan, dat 'stringente eisen aan de veiligheidsaspecten beschikbaarheid, (data)integriteit en vertrouwelijkheid' stelt. Als één van deze aspecten gecompromitteerd wordt, of lijkt te worden, kan het imago van de dienst ernstig worden beschadigd.

Het eHerkenning koppelvlak (en het afsprakenstelsel) zijn opgesteld onder de ICT-beveiligingsrichtlijnen voor webapplicaties van NCSC[20], als leidraad bij het ontwikkelen, beheren en aanbieden van eHerkenning en bijbehorende infrastructuur. Tevens zijn bij uitwerking van het koppelvlak (en het hele afsprakenstelsel)eisen uit de Baseline Informatiebeveiliging Rijksdienst (BIR)[21] meegenomen in de risico analyse en het normenkader.

Binnen het afsprakenstelsel zijn verder voor gebruik van het koppelvlak duidelijke richtlijnen en procesbeschrijvingen voor incident management op het gebied van vertrouwelijkheid en/of integriteit (operationeel handboek) beschikbaar.

De standaard eHerkenning overheidskoppelvlak baseert zich bovendien op een beveiligingsniveau, waarbij

- gebruik gemaakt wordt van asymmetrische vercijfering op basis van een PKI
- sleutellengtes van minimaal 2048 bit worden afgedwongen
- minimaal SHA256 wordt gebruikt als hashing algoritme
- maatregelen zijn genomen tegen replay aanvallen
- berichten/verklaringen beperkt houdbaar zijn

De expertgroep is van mening dat daarmee de beveiligingsrisico's wat betreft het eHerkenning overheidskoppelvlak acceptabel zijn.

3.2.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Privacy ligt in het ontwerp van de standaard besloten. De eisen met betrekking tot privacy zijn in vastgelegd in de standaard en meer nog, in het afsprakenstelsel. eHerkenning beschermt de privacy doordat bij authenticatie van bedrijven de persoonsgegevens van de gemachtigde alleen binnen het netwerk gecontroleerd worden en niet verstrekt worden aan de ontvangende instantie (de overheidsdienstverlener). Alleen het – niet privacy gevoelige - identificatienummer van een bedrijf en een pseudoniem van de handelende persoon worden verstrekt.

---

19 Onderzoek veiligheid diensten in de Digitale Agenda.nl, http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/03/16/eindrapportage-onderzoek-digitale-agenda.html

20 ICT-beveiligingsrichtlijnen voor webapplicaties, NCSC, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

21 Baseline Informatiebeveiliging Rijksdienst (BIR), http://www.wikixl.nl/wiki/ictu/index.php/Component_baseline_informatiebeveiliging_Rijksdienst

Bij aantoonbaar fraudevermoeden kan middels een procedure de identiteit achter een pseudoniem worden verkregen bij eHerkenning-partij. Een gebruiker van de dienst kan er ook voor kiezen om zijn identiteit na inloggen bij de dienstverlener bekend te maken, bijvoorbeeld door het meegeven van naam of emailadres in de attributen.

3.2.4 Conclusie

De expertgroep is van mening dat de voordelen van eHerkenning overheidskoppelvlak opwegen tegen de risico's en de nadelen.

De overheidsbrede en maatschappelijke baten wegen op tegen de kosten, en privacy en beveiligingsrisico's zijn in de standaard in voldoende mate afgedekt. De standaard biedt ook meerwaarde ten opzichte van de standaard SAML v2.0. De voordelen van de standaard overheidskoppelvlak eHerkenning zijn met name terug te vinden in het terugdringen van de diversiteit in authenticatievoorzieningen en de bijdrage die dit levert aan de vermindering van interoperabiliteitsproblematiek op dit gebied. Het koppelvlak is bovendien als zelfstandig profiel bovenop SAML ook in te zetten buiten het stelsel eHerkenning om.

Er zijn alternatieven voor de standaard, maar deze zijn minder eenvoudig in gebruik, worden uitgefaseerd of kennen in veel beperktere mate inbedding in een uitwerking van afspraken en regels (zoals het afsprakenstelsel eHerkenning) om correct en interoperabel gebruik van de standaard te garanderen.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Op moment van schrijven zijn er 6 erkende aanbieders die de rol van eHerkenningsmakelaar vervullen en het eHerkenning overheidskoppelvlak aanbieden: KPN, Gemnet, Connectis, iWelcome, CreAim en Digidentity[22].

3.3.1.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Het testen en monitoren van dienstverleners is beschreven in de documentatie van het afsprakenstelsel[23]. Ter ondersteuning beheert de beheerorganisatie een online voorziening om deze testen uit te kunnen voeren. De test op conformiteit wordt binnen deze voorziening uitgevoerd middels een eHerkenning test tool voor dienstverleners, een instrument

22 http://www.eherkenning.nl/overheden/aansluiten/aanbieders
23 Afsprakenstelsel eHerkenning v1.4, Testen voor Dienstverleners, http://www.eherkenning.nl

dat berichten verzendt en de antwoorden beoordeelt op conformiteit aan het hele afsprakenstelsel. Naast deze voorziening bieden de marktpartijen die de makelaarsrol invullen eveneens toetsingsvoorzieningen (op commerciële basis).

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

Op moment van schrijven zijn er 40 overheidsdienstverleners aangesloten die gezamenlijk 44 verschillende e-diensten[24] bieden met gebruik van eHerkenning. Dit betreft zowel landelijke (o.a. Berichtenbox voor Antwoord voor Bedrijven, Ministerie van Infrastructuur en Milieu, Ministerie van EL&I, IND) als lokale overheden (o.a. gemeente Rotterdam, gemeente Zwolle, gemeente Zoetermeer).

Verder is een aantal overheidsdiensten in voorbereiding op een implementatie van eHerkenning, waaronder OPTA, CJIB, Inspectie Verkeer en Waterstaat en provincie Groningen.

3.3.2.2 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

Op moment van schrijven is bij alle overheidsorganisaties een oudere versie van het overheidskoppelvlak eHerkenning in gebruik (versie 1.1). De verwachting is dat eind van 2012 versie 1.4 geïmplementeerd en ondersteund wordt door de betrokken partijen.

De (verplichte) technische verschillen tussen versies 1.1 en versies 1.4 zijn beperkt tot

- Invoer van nieuwe KvK vestigingsnummers
- Verplichte timesynchronisatie
- Verplicht gebruik G2 SSL certificaten

Voor het eHerkenning overheidskoppelvlak geldt dat het overheidsdienstverleners is toegestaan oudere versies te gebruiken. Een makelaar wordt alleen verplicht de huidige, gangbare versie van het koppelvlak en de versie ervoor te ondersteunen (N/N-1-principe voor management van versies in de levenscyclus van het koppelvlak). Een makelaar kan er ook voor kiezen nog oudere versies te ondersteunen: daar zit geen eindtermijn aan.

3.3.2.3 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

De aangemelde versie van de standaard biedt uitbreidingen ten opzichte van de vorige versie(s) van de koppelvlak standaard. De huidige versie van het koppelvlak is backwards compatible met eerdere versies, met dien

24 https://extranet.eherkenning.nl/dienstencatalogus.xml

verstande dat nieuwe functionaliteit niet beschikbaar is voor gebruikers die een eerdere versie geïmplementeerd hebben.

Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Het aantal gebruikers en aangesloten dienstverleners is het afgelopen jaar gestegen en neemt nog steeds toe.

In het iNUP is verder vastgelegd dat alle gemeenten de verplichting hebben eHerkenning als NUP-bouwsteen te implementeren, in het kader van Operatie NUP[25]. In de Digitale Agenda.nl[26] is eHerkenning daarnaast genoemd als authenticatiemiddel (gekoppeld aan een autorisatiemiddel) in het kader van het beleidsthema om het voor bedrijven mogelijk te maken elektronisch zaken te doen met de overheid ("recht op elektronisch zakendoen voor bedrijven").

Er kan een kanttekening worden geplaatst bij het huidige verschil tussen authenticatiediensten in het burger- en bedrijvendomein. Voor het bedrijvendomein is eHerkenning de ontwikkelde oplossing , voor het burgerdomein is dat DigiD. Het A3-rapport schetst dat het wenselijk is om deze twee domeinen op termijn naar elkaar toe te laten groeien.

3.3.3 Conclusie

De expertgroep is van mening dat er voldoende draagvlak is voor de standaard: er is marktondersteuning voor de standaard door meerdere leveranciers en er is beleidsmatige ondersteuning voor eHerkenning in het iNUP en de Digitale Agenda.nl. Het aantal aangesloten aanbieders van overheidsdiensten is op moment van schrijven ongeveer 40 (met 44 overheidsdiensten) en neemt in aantal toe.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:

1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

25 Operatie NUP, http://new.kinggemeenten.nl/nup-bouwstenen

26 Digitale Agenda.nl – ICT voor Innovatie en economische groei, http://www.rijksoverheid.nl/documenten-en-publicaties/notas/2011/05/17/digitale-agenda-nl-ict-voor-innovatie-en-economische-groei.html

Voor de standaard eHerkenning overheidskoppelvlak v1.4 geldt dat een opname op de lijst voor 'pas toe of leg uit' wordt voorzien.

3.4.1 Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Een doelstelling van het afsprakenstelsel eHerkenning is het realiseren van een uniform stelsel met gestandaardiseerde koppelvlakken. Streven is daarbij om deze koppelvlakken te implementeren in systemen voor elektronische (web)diensten, ook wanneer deze pas op termijn gebruikt gaan worden voor digitale transactiediensten.

Plaatsing op de 'pas toe of leg uit'-lijst bevestigt het door de overheid ontwikkelde en uitgevoerde beleid voor het realiseren van een landelijke herkennings-/authenticatiedienst. Een verplichting via 'pas toe of leg uit' ziet de expertgroep ook als middel om de in iNUP en Digitale Agenda gemaakte beleidsdoelen en bestuurlijke afspraken daadwerkelijk te bereiken en het gebruik van de eHerkenning standaard in de praktijk te bevorderen. Opname op de lijst voor 'pas toe of leg uit' zal tevens het animo om de standaard overheidsbreed toe te passen versterken en zo adoptie van de standaard bevorderen.

3.4.2 Zijn er naast opname op de lijst aanvullende adoptiemaatregelen nodig?

Behalve verplichting via 'pas toe of leg uit' ziet de expertgroep met name voorlichting en kennisverspreiding als middel om het gebruik van de eHerkenning standaard in de praktijk te bevorderen Deze kennisverspreiding wordt in voldoende mate door het programma eHerkenning zelf gedragen: naar mening van de expertgroep is geen verdere actie van het Forum Standaardisatie op dit punt nodig.

Bij opname op de lijst is er enige overlap met de standaard SAML die al op de 'pas toe of leg uit'-lijst staat. Aanbeveling van de expertgroep aan het Forum is:

- Om aandacht te geven aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie en na te gaan hoe deze twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein.

Een aanbeveling die de expertgroep doet aan de beheerorganisatie voor eHerkenning is:

- na te gaan hoe de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd kunnen worden en waar nodig met een voorstel voor een alternatieve definitie te komen.

3.4.3 Is de inzet van aanvullende adoptie-instrumenten (communicatief, financieel, juridisch), door andere partijen dan het Forum/College Standaardisatie, noodzakelijk?

De afspraak in het iNUP verplicht 415 lokale overheden om per 1 januari 2015 aan te sluiten. De onlangs uitgevoerde impactanalyse van operatie NUP[27] wijst uit dat de gemeenten (en KING/VNG) nu aan de slag kunnen met implementatie. Er hoeft vanuit het Forum Standaardisatie op dit punt geen aanvullende actie worden ondernomen of uitgezet.

Door de consistentie in een aantal technische keuzes aan te brengen zou naar mening van de expertgroep wel de samenhang tussen DigiD en eHerkenning kunnen worden vergroot. Een aanbeveling die de expertgroep doet aan Logius en eHerkenning gezamenlijk is:

- om de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart te brengen en waar mogelijk te verbeteren.

3.4.4 Kan een uitgebreid adoptieadvies van het Forum Standaardisatie helpen bij het wegnemen van knelpunten in de adoptie?

Een uitgebreid adoptieadvies kan een extra stimulans zijn voor overheidsorganisaties die nu nog eigen voorzieningen/ koppelvlakken hanteren voor hetzelfde doel. Voorlichting en kennisverspreiding voor vraagstukken rondom migratie naar eHerkenning, praktijkcases en voorlichting kunnen in de praktijk ondersteuning bieden bij deze overstap.

Daarnaast kunnen dergelijke maatregelen overheidsorganisaties over de streep helpen die nu nog een afwachtende houding aannemen in verband met de status van eHerkenning.

3.4.5 Conclusie

Plaatsing op de 'pas toe of leg uit'-lijst bevestigt het door de overheid ontwikkelde en uitgevoerde beleid voor het realiseren van een landelijke herkennings-/authenticatiedienst. Een verplichting via 'pas toe of leg uit' ziet de expertgroep ook als middel om de in iNUP en Digitale Agenda gemaakte beleidsdoelen en bestuurlijke afspraken daadwerkelijk te bereiken en het gebruik van de eHerkenning standaard in de praktijk te bevorderen.

Bij opname op de lijst is er enige overlap met de standaard SAML die al op de 'pas toe of leg uit'-lijst staat. Aanbeveling van de expertgroep aan het Forum is:

- Om aandacht te geven aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie en na te gaan hoe deze twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein.

Een aanbeveling die de expertgroep doet aan de beheerorganisatie voor eHerkenning is:

- na te gaan hoe de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd

27 http://new.kinggemeenten.nl/operatie-nup/nieuws/eherkenning-implementeerbaar

kunnen worden en waar nodig met een voorstel voor een alternatieve definitie te komen.

Een aanbeveling die de expertgroep doet aan Logius en eHerkenning gezamenlijk is:

- om de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart te brengen en waar mogelijk te verbeteren.

4 Advies aan Forum en College

4.1 Samenvatting van de toetsingscriteria

Samengevat is het oordeel van de expertgroep op de toetsingscriteria als volgt:

4.1.1 Open standaardisatieproces

De documentatie is na aanmelding beschikbaar, de besluitprocedure is voldoende toegankelijk, er is een bezwaarprocedure en de standaardisatieorganisatie is onafhankelijk en duurzaam. De standaard voldoet naar mening van de expertgroep echter pas aan de openheidscriteria als ook aan de volgende voorwaarde is voldaan:

- De bepalingen die gelden ten aanzien van het intellectueel eigendom (en merkrecht) moeten duidelijker worden gemaakt en moeten in aanvulling op de huidige documentatie van de standaard worden gepubliceerd.

4.1.2 Toegevoegde waarde

De expertgroep is van mening dat de voordelen van eHerkenning overheidskoppelvlak opwegen tegen de risico's en de nadelen.

De overheidsbrede en maatschappelijke baten wegen op tegen de kosten, en privacy en beveiligingsrisico's zijn in de standaard in voldoende mate afgedekt. De standaard biedt ook meerwaarde ten opzichte van de standaard SAML v2.0. De voordelen van de standaard overheidskoppelvlak eHerkenning zijn met name terug te vinden in het terugdringen van de diversiteit in authenticatievoorzieningen en de bijdrage die dit levert aan de vermindering van interoperabiliteitsproblematiek op dit gebied. Het koppelvlak is bovendien als zelfstandig profiel bovenop SAML ook in te zetten buiten het stelsel eHerkenning om.

Er zijn alternatieven voor de standaard, maar deze zijn minder eenvoudig in gebruik, worden uitgefaseerd of kennen in veel beperktere mate inbedding in een uitwerking van afspraken en regels (zoals het afsprakenstelsel eHerkenning) om correct en interoperabel gebruik van de standaard te garanderen.

4.1.3 Draagvlak

De expertgroep is van mening dat er voldoende draagvlak is voor de standaard: er is marktondersteuning voor de standaard door meerdere leveranciers en er is beleidsmatige ondersteuning voor eHerkenning in het iNUP en de Digitale Agenda.nl. Het aantal aangesloten aanbieders van overheidsdiensten is op moment van schrijven ongeveer 40 (met 44 overheidsdiensten) en neemt in aantal toe.

4.1.4 Opname bevordert adoptie

Plaatsing op de 'pas toe of leg uit'-lijst bevestigt het door de overheid ontwikkelde en uitgevoerde beleid voor het realiseren van een landelijke herkennings-/authenticatiedienst. Een verplichting via 'pas toe of leg uit' ziet de expertgroep ook als middel om de in iNUP en Digitale Agenda gemaakte beleidsdoelen en bestuurlijke afspraken daadwerkelijk te bereiken en het gebruik van de eHerkenning standaard in de praktijk te bevorderen.

Bij opname op de lijst is er enige overlap met de standaard SAML die al op de 'pas toe of leg uit'-lijst staat. Aanbeveling van de expertgroep aan het Forum is:

- Om aandacht te geven aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie en na te gaan hoe deze twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein.

Een aanbeveling die de expertgroep doet aan de beheerorganisatie voor eHerkenning is:

- na te gaan hoe de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd kunnen worden en waar nodig met een voorstel voor een alternatieve definitie te komen.

Een aanbeveling die de expertgroep doet aan Logius en eHerkenning gezamenlijk is:

- om de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart te brengen en waar mogelijk te verbeteren.

4.2 Advies aan Forum en College

De expertgroep adviseert in meerderheid de standaard overheidskoppelvlak eHerkenning, versie 1.4, op te nemen op de lijst van 'pas toe of leg uit' indien aan de volgende voorwaarden is voldaan:

- Vermelden en publiceren van de bepalingen ten aanzien van intellectueel eigendomsrecht in aanvulling op de documentatie van de standaard.

Met als toepassingsgebied:
"Authenticatie voor webdiensten van overheidsdienstverleners aan bedrijven en organisaties en het vaststellen van de bevoegdheid voor de gevraagde dienst."

En als werkingsgebied:
"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector."

Op moment van schrijven spreken drie partijen, te weten de Belastingdienst, Logius en het Ministerie van BZK zich echter nog niet uit over opname op de lijst.

4.3 Aanbevelingen ten aanzien van de adoptie van de standaard

Bij opname op de lijst is er enige overlap met de standaard SAML die al op de 'pas toe of leg uit'-lijst staat. Aanbeveling van de expertgroep aan het Forum is:

- Om aandacht te geven aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie en na te gaan hoe deze twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein.

Een aanbeveling die de expertgroep doet aan de beheerorganisatie voor eHerkenning is:

- na te gaan hoe de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd kunnen worden en waar nodig met een voorstel voor een alternatieve definitie te komen.

Een aanbeveling die de expertgroep doet aan Logius en eHerkenning gezamenlijk is:

- om de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart te brengen en waar mogelijk te verbeteren.

5 Referenties

[1] *Actieplan Nederland Open in Verbinding*, 's-Gravenhage: Ministerie van Economische Zaken, 2007.

[2] "Pas toe of leg uit" is vastgelegd in de "Instructie rijksdienst bij aanschaf ICT-diensten of ICT- producten" van 8 november 2008, en daarnaast in convenanten en afspraken met decentrale overheden. Zie: http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/

[3] " Instellingsbesluit College en Forum Standaardisatie 2010". Zie: https://zoek.officielebekendmakingen.nl/stcrt-2010-4499.html

[4] Criteria en procedure voor 'pas toe of leg uit', vastgesteld door het College Standaardisatie op 23 juni 2011. Zie: http://www.forumstandaardisatie.nl/fileadmin/os/images/Toetsingsprocedure_en_criteria_v1_0.pdf