

**Forum Standaardisatie**

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

Opname eHerkenning op de lijst voor 'pas toe of leg uit'

FORUM STANDAARDISATIE

Agendapunt:	07.		
Bijlagen:	Expertadvies en consultatiereacties		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	26 oktober 2012	Versie	0.9
Betreft:	Opname eHerkenning op de lijst voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?

Het eHerkenning overheidskoppelvlak beoogt het probleem van de diversiteit aan authenticatievoorzieningen, gericht op het bedrijvendomein, voor losstaande overheidsdiensten op te lossen ("sleutelbos"), waardoor zowel bedrijven als afnemende organisaties geconfronteerd worden met vele keuzemogelijkheden en niet-gestandaardiseerde samenhang tussen de technische koppelvlakken. In het verleden is door het Forum Standaardisatie de wens uitgesproken te komen tot betere kaders rondom identificatie, authenticatie en autorisatie. eHerkenning kan voor een dergelijk kader bieden, conform advies van de Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 advies).

Hoe is het advies tot stand gekomen?

Een expertgroep is eenmaal bijeen gekomen om toetsing van de standaard uit te voeren. Tijdens de bijeenkomst op 2 juli 2012 is door een meerderheid van de experts een positief advies gegeven voor opname op de 'pas toe of leg uit'-lijst, mits is voldaan aan het wegnemen van een geconstateerd knelpunt. Dit advies is publiek geconsulteerd hetgeen geleid heeft tot zes reacties.

Zijn er risico's verbonden aan de keuze?

Het overheidskoppelvlak eHerkenning is een toepassingsprofiel op de SAML standaard gericht op authenticatie in het bedrijvendomein. In Nederland zijn meer van dergelijke profielen in gebruik. Zo bevat DigiD een toepassingsprofiel gericht op het burgerdomein. Als deze profielen onderling niet compatible zijn, heeft het gebruik van één onderliggende standaard geen toegevoegde waarde. In en dergelijk geval dient een gebruiker die actief is in verschillende domeinen namelijk nog steeds meerdere koppelvlakken te implementeren. Dit brengt extra kosten en onderhoudslasten met zich mee. Het eHerkenningskoppelvlak is een waardevol toepassingsprofiel gericht op het bedrijvendomein, maar het is noodzakelijk dat op zo kort mogelijke termijn de verschillende profielen met elkaar in overeenstemming worden gebracht om bij te dragen aan de interoperabiliteit in het gehele authenticatie- en autorisatiedomein.

Gevraagd besluit**Datum**

23 maart 2012

Constateringen

Het Forum Standaardisatie doet de volgende constateringen:

1. De standaard SAML voor uitwisseling van authenticatie- en autorisatiegegevens staat sinds 20 mei 2009 op de 'pas toe of leg uit'-lijst. SAML is een internationale, generieke standaard die ruimte laat voor nadere invulling voor specifieke situaties. Voor interoperabiliteit zijn daarom aanvullende afspraken nodig die worden vastgelegd in zogenoemde SAML-profielen.
2. eHerkenning heeft voor het domein van bedrijven en organisaties een SAML-profiel ontwikkeld ("eHerkenning overheidskoppelvlak") en aangemeld voor opname op de 'pas toe of leg uit'-lijst.
3. DigiD 4 en DigiD machtigen hebben ieder ook een eigen SAML-profiel voor het domein van burgers ontwikkeld.
4. Het opnemen van "eHerkenning overheidskoppelvlak" op de 'pas toe of leg uit'-lijst heeft toegevoegde waarde, maar dit kan qua standaardisatie niet het einddoel zijn.
5. De voordelen van standaardisatie worden door het bestaan van verschillende SAML-profielen namelijk niet volledig benut. Aansluitende overheden en softwareleveranciers hebben daardoor meermaals aansluit- en implementatiekosten. Bovendien brengt het onderhoud van meerdere koppelvlakken aanvullende kosten met zich mee voor de beheerder (Logius).

Besluit

Forum Standaardisatie roept daarom de verantwoordelijke ministeries (BZK en EL&I) op om een opdracht te verlenen aan Logius om:

1. **vóór juli 2013** één gestandaardiseerd SAML-profiel te realiseren, en dit vervolgens te implementeren in eHerkenning, DigiD en andere (toekomstige) authenticatie- en autorisatiediensten van de Nederlandse overheid.
2. daarbij actief aan te sluiten bij het Kantara initiatief: eGov Profile, dat een erkende internationale best-practice biedt.
3. dit SAML-profiel vervolgens aan te melden voor opname op de 'pas toe of leg uit'-lijst.

Zodra deze opdracht aan Logius is verstrekt, wordt College Standaardisatie gevraagd in te stemmen met:

1. de opname van eHerkenning overheidskoppelvlak 1.4 op de lijst voor 'pas toe of leg uit'.
2. het functionele toepassingsgebied *"Authenticatie voor webdiensten van overheidsdienstverleners aan bedrijven en organisaties en het vaststellen van de bevoegdheid voor de gevraagde dienst."*;
3. het organisatorische werkingsgebied *"Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector"*;

Overige aanbevelingen:

Datum
23 maart 2012

Aan de indiener:

- Publiceer het vastgestelde versiebeleid van de standaard in aanvulling op de documentatie van de standaard.
- Maak de wijzigingen op de standaard in de verschillende versies in de documentatie van het eHerkenningssysteem inzichtelijk
- Maak de documentatie van de standaard publiek beschikbaar zonder aanmeldingsproces.

Aan het Forum:

- Geef als Forum aandacht aan de samenhang tussen standaarden in het domein van identificatie, authenticatie en autorisatie. Ga hierbij na hoe de twee standaarden zich tot elkaar verhouden in een raamwerk voor dit domein. Draag hiertoe, waar mogelijk, bij aan de ontwikkeling van het NORA katern: informatie beveiliging.

Toelichting

Waar gaat het inhoudelijk over?

De standaard overheidskoppelvlak eHerkenning v1.4 beschrijft het koppelvlak tussen een (overheids)dienstverlener en de eHerkenningmakelaar. De standaard is een elektronisch middel voor de authenticatie van bedrijven en organisaties, wanneer zij digitaal diensten afnemen van (overheids)dienstverleners (zoals DigiD dat authenticatiemiddel is voor burgers). 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.

Hoe is het proces verlopen?

Na aanmelding van de standaard door het programma eHerkenning, heeft een intakegesprek plaatsgevonden. Dit gesprek leidde tot een positief advies voor het in procedure nemen van eHerkenning. Op 2 juli 2012 is een vijftiental experts uit de overheid, bedrijfsleven en academische wereld bijeengekomen om de standaard te toetsen. 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 het adviesrapport opgesteld. De expertgroep adviseerde in meerderheid, maar niet unaniem voor opname op de lijst, mits aan de genoemde voorwaarde is voldaan. Drie partijen, te weten de Belastingdienst, Logius en het Ministerie van BZK spraken zich op dat moment nog niet uit over opname op de lijst.

Het expertadvies is publiekelijk geconsulteerd en hierop zijn 6 reacties binnengekomen. Drie respondenten (Kadaster, Logius en Kantara) onderschreven het advies van de expertgroep om eHerkenning op de lijst voor pas toe of leg op te nemen. Eén respondent (Belastingdienst) is tegen opname op de lijst. De twee overige respondenten (Kennisnet, UWV) hebben zich om uiteenlopende redenen (nog) niet expliciet uitgesproken.

Datum
23 maart 2012

De belangrijkste opmerkingen uit de consultatie zijn:

- Kennisnet steunt het initiatief, maar ziet de sectorale belangen van onderwijs onvoldoende vertegenwoordigd/behartigd. Het programma eHerkenning ziet hierin een mogelijkheid om samenwerking op te zetten en de belangen van de onderwijssector bij eHerkenning in te brengen.
- Kennisnet geeft aan dat een verkenning van eHerkenning voor gebruik in het onderwijs op korte termijn verschijnt.
- Kantara geeft in haar reactie aan dat eHerkenning grotendeels in lijn lijkt te zijn opgesteld met het door Kantara gehanteerde 'eGov profile' op SAML. Het programma eHerkenning geeft aan dat verdere afstemming tussen het eGov profiel en eHerkenning een zinvolle aanvulling is op de voorgestelde vervolgvactiteiten in het expertadvies.
- De Belastingdienst ziet in opname van eHerkenning op de lijst een mogelijke hinderpaal voor het eID initiatief. De expertgroep is echter van mening, dat eHerkenning in lijn met de visie van het ID stelsel wordt ontwikkeld en invulling geeft aan een deel van de functionaliteit van eID. Afstemming met DigiD is in het expertadvies door de expertgroep al genoemd als middel om de samenhang te verbeteren.
- Het UWV verwijst naar de complexiteit van de benodigde architectuur voor implementatie. De expertgroep is van mening dat dit juist voor alleen het koppelvlak niet het geval hoeft te zijn.
- Het UWV ziet de behoefte om ook authenticatie te verzorgen voor niet-natuurlijke personen (systemen) niet terug in het expertadvies. De expertgroep is van mening dat de scope van de standaard in de context van de lijst zich nu in de scope duidelijk beperkt tot niet-natuurlijke personen, waarvan de bevoegdheid aan de hand van een natuurlijke persoon kan worden vastgesteld.
- Het UWV verwijst naar de tot dusver relatief geringe deelname van gemeenten (10%). De expertgroep wijst er op dat dit juist een reden is om adoptie van de standaard te bevorderen door op name op de lijst.
- Logius noemt strikte handhaving van de afbakening van het toepassingsgebied noodzakelijk ten aanzien van het gebruik van eHerkenning, dus alleen gebruik voor webdiensten en voor organisaties/bedrijven.
- Daarnaast vraagt Logius Forum standaardisatie te bekijken of eHerkenning niet beter als voorziening kan worden getoetst en kan worden voorgeschreven. Het koppelvlak is immers slechts een onderdeel binnen het stelsel eHerkenning

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.

- *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 als toepassingsprofiel ook meerwaarde ten opzichte van de onderliggende standaard SAML v2.0.

Datum

23 maart 2012

- *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.

- *Opname bevordert adoptie*

Opname 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.

Wat is de conclusie van de expertgroep en de consultatie¹?

Een meerderheid van de expertgroep adviseert het college om eHerkenning op te nemen op de lijst met open standaarden voor "pas toe of leg uit".

Als functioneel toepassingsgebied wordt daarbij voorgesteld:

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

Als organisatorisch werkingsgebied wordt voorgesteld:

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

In het oorspronkelijke expertadvies was de voorwaarde opgenomen dat de beheerder van de standaard de bepalingen ten aanzien van intellectueel eigendomsrecht en merkrecht in aanvulling op de documentatie van de standaard, moest publiceren. De indiener heeft inmiddels aan deze voorwaarde voldaan.

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

¹ Het expertadvies is gepubliceerd op de website van het Forum:
<https://www.forumstandaardisatie.nl/sites/default/files/FS/2012/1105/120806-Expertadvies-eHerkenning-overheidskoppelvlak.pdf>

Aandachtspunten:

- Er is overlap met SAML. Het overheidskoppelvlak is een toepassingsprofiel op SAML dat het gebruik van SAML binnen deze specifieke toepassing vorm geeft.
- De technische keuzes die voor authenticatie in het burgerdomein zijn gemaakt bij DigiD, zijn niet allemaal dezelfde als bij eHerkenning. Dit hangt samen met keuzes in de invulling van het SAML profiel.

Datum

23 maart 2012

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

Concreet doet de expertgroep in meerderheid de volgende aanvullende aanbevelingen:

- Geef als Forum aandacht 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.
- Ga als beheerorganisatie van eHerkenning na of de toepassingsgebieden van SAML en overheidskoppelvlak eHerkenning beter op elkaar afgestemd kunnen worden en kom waar nodig met een voorstel voor een alternatieve definitie.
- Breng als Logius en eHerkenning gezamenlijk de samenhang (en met name de consistentie in een aantal technische keuzes) tussen DigiD en eHerkenning in kaart en verbeter die samenhang waar mogelijk.

Bijlagen

- Expertadvies eHerkenning overheidskoppelvlak
- Overzicht reacties consultatieronde
 - Belastingdienst
 - Logius
 - KvK
 - Ministerie van EL&I
 - UWV

(zie: <http://lijsten.forumstandaardisatie.nl/open-standaarden/eherkenning-overheidskoppelvlak>)