



CS-20111115.08

Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag
www.forumstandaardisatie.nl

notitie

COLLEGE STANDAARDISATIE

Agendapunt:	6		
Bijlagen:	1		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	30 september 2011	Versie	1.0
Betreft:	Handreiking betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten		

Oplegnotitie College Standaardisatie 15 november 2011

Datum

Waarom is authenticatie belangrijk?

Bij elektronische transacties met bedrijven en burger moeten overheden weten met wie ze van doen hebben. Daarvoor zijn authenticatiemiddelen nodig. De zwaarte van het in te zetten middel hangt af van de aard van de transactie en de gevolgen ervan (zoals financiële of juridische gevolgen).. Om overheidsorganisaties te helpen bij het maken van een keuze voor het gewenste betrouwbaarheidsniveau voor een elektronische dienst is deze handreiking geschreven, die aansluit op de Europese classificatie (STORK) die vier betrouwbaarheidsniveaus onderkent.

Waarom is een keuze belangrijk?

Overheidsorganisaties hanteren bij het vaststellen van betrouwbaarheidsniveaus bij authenticatie voor elektronische diensten geen methodisch en eenduidig kader. Dat brengt enerzijds risico's met zich (het gekozen niveau en de daaraan gekoppelde middelen sluiten niet aan op de eisen die de elektronische dienst stelt) en gaat anderzijds ten koste van duidelijkheid en zekerheid voor gebruikers van e-diensten. De voorliggende handreiking helpt beleidsmakers, architecten, informatiebeveiligers, juristen en bestuurders om op basis van een eenvoudig en generiek beoordelingsmodel, een beredeneerde keuze te maken voor het benodigde betrouwbaarheidsniveau.

Waarom kunt u met een 'gerust hart' ja zeggen tegen deze handreiking?

De ontwikkelde handreiking is het resultaat van een intensieve samenwerking tussen uitvoeringsorganisaties, decentrale overheden en ministeries. Verder is de handreiking indringend besproken in het Forum Standaardisatie. De handreiking wordt inmiddels door meerdere partijen in de praktijk beproefd. Het Bureau Forum Standaardisatie zal de handreiking actief beheren en aanpassen aan de wensen uit de praktijk. Ook zal ondersteuning worden geboden bij het gebruik.

Zijn er risico's verbonden aan de keuze?

Zoals de naam al zegt is de publicatie een handreiking. Het helpt bestuurders, maar zij blijven zelf verantwoordelijk voor het gekozen betrouwbaarheidsniveau. Indien zij menen dat gebruik van de handreiking voor hun specifieke dienst niet wenselijk is, moeten zij een volledige risico-analyse uitvoeren.

Beslispunt

Het College Standaardisatie wordt gevraagd in te stemmen met:

- de voorliggende handreiking betrouwbaarheidsniveaus;
- het beleggen van het beheer van de handreiking bij het Bureau Forum Standaardisatie;
- het advies om in de eigen organisatie bekendheid te geven aan de handreiking.

1. Toelichting

Datum

8 september 2011

Aanleiding

Van diverse kanten heeft het Forum Standaardisatie signalen gekregen dat het voor uitvoerders van publieke diensten lastig te beoordelen was welk betrouwbaarheidsniveau nodig is voor authenticatie bij elektronische diensten. Een te laag betrouwbaarheidsniveau kan aanzienlijke risico's mee brengen op het gebied van fraude en privacy, een te hoog betrouwbaarheidsniveau is vaak aanzienlijk duurder dan nodig. Het beeld is dat vaak relatief ad hoc een keuze werd gemaakt rond het te gebruiken betrouwbaarheidsniveau. Meer eenduidigheid in de keuze van de betrouwbaarheidsniveaus kan ook helpen om als overheid meer als een eenheid over te komen en onverklaarbare verschillen in de keuzes rond betrouwbaarheidsniveau's te voorkomen.

Directe aanleiding om te starten met de handreiking was de onmogelijkheid om het toepassingsgebied van het Programma van Eisen van PKI-overheid te bepalen. Omdat een concreet toepassingsgebied een vereiste is voor het plaatsen van standaarden op de pas toe of leg uit lijst van College Standaardisatie, achtte het Forum opname van het Programma van Eisen PKI-overheid op die lijst (nog) niet mogelijk. In het project is hier expliciet aandacht aan besteed.

Aanpak

Aangesloten is bij de indeling in betrouwbaarheidsniveaus die binnen de EU is ontwikkeld in het zogenoemde STORK-project¹. Die indeling is ook aangehouden bij het indelen van authenticatiemiddelen in het kader van eHerkenning.

Er bestaan al methoden voor risicoanalyse op dit terrein, onder meer ontwikkeld door de Amerikaanse overheid. Die methoden zijn echter nogal gedetailleerd en tijdsintensief. Juist omdat dienstverleningsprocessen in Nederland al tamelijk gestandaardiseerd zijn (oa. door toepasselijkheid van de Algemene wet bestuursrecht op beslisprocessen) is een dergelijke gedetailleerde aanpak voor veel diensten van Nederlandse overheidsdienstverleners niet nodig. In deze handreiking is ervoor gekozen een generiek en collectief model voor inschatting van betrouwbaarheidsniveaus te ontwikkelen, gebaseerd op wettelijke vereisten aan de (electronische) dienst en belangen die rond de (electronische) dienst een rol spelen.

Dit model zal naar alle waarschijnlijkheid voor het gros van de gevallen goed toepasbaar zijn. Als dat niet het geval is kan de betrokken organisatie een meer uitgebreide risico-analyse uitvoeren. Het Forum Standaardisatie heeft in juni 2011 vastgesteld dat deze handreiking een bruikbaar instrument oplevert voor overheidsorganisaties bij het bepalen van betrouwbaarheidsniveaus, en tevens helderheid geeft over het toepassingsgebied van PKI-overheid.

¹ *Secure idenTity acrOss boRders linKed*

Proces**Datum**

8 september 2011

Met een groep van ca. 25 betrokkenen uit zowel beleid als uitvoering is in een aantal iteratieve sessies de voorliggende handreiking ontwikkeld. De deelnemers hebben de handreiking ook voor de vaststelling van het betrouwbaarheidsniveau van hun eigen diensten beproefd. De ervaringen die daarbij zijn opgedaan zijn verwerkt. In een bijeenkomst van de werkgroep d.d. 6 september is ingestemd met de 1.0 versie van de handreiking, waarin ook nog enige opmerkingen en suggesties van het Forum zijn verwerkt. Daarnaast is een voorstel voor beheer en doorontwikkeling van de handreiking besproken en akkoord verklaard. Concrete vervolgacties in het kader van beheer en doorontwikkeling zijn:

- uitbreiding met machine-to-machine verkeer;
- uitbreiding met verkeer tussen overheidsorganisaties (bv. uitwisseling van gegevens in het kader van basisregistraties);
- het inrichten van een platform voor het uitwisseling van ervaringen bij toepassing van de handreiking én bij keuze voor een concreet betrouwbaarheidsniveau. Dit zowel om van elkaar te leren, als eenduidigheid bij die keuze te bevorderen.

Het Forum Standaardisatie heeft aangegeven een rol te blijven spelen bij beheer en doorontwikkeling van de handreiking. Dit past ook bij de activiteiten van het Forum: de handreiking heeft de potentie zich door te ontwikkelen tot een standaard op het terrein van juridische en organisatorische interoperabiliteit. De benodigde activiteiten zullen bij het Bureau Forum Standaardisatie worden ondergebracht. De leden van de werkgroep zullen nauw betrokken blijven en tevens zal gezorgd worden voor uitbreiding van de groep, oa. met andere uitvoeringsorganisaties (in Manifestgroep-verband), provincies en gemeenten (laatstgenoemden waren tot nog toe zijdelings betrokken). Een uitgebreidere beschrijving van de aanpak rond beheer en doorontwikkeling vindt u in de bijgevoegde notitie.

Het College Standaardisatie wordt geadviseerd in te stemmen met de handreiking en de aanpak van het vervolgtraject. Daarnaast wordt het College geadviseerd in de eigen organisatie (voor zover nog niet betrokken bij de ontwikkeling) bekendheid te geven aan de handreiking.