

Van	Toestelnummer	Memonummer
Arjen Haasnoot	3796054	0.7
Datum	Bijlage(n)	
22-8-2008		
Aan	Informatiekopie aan	
Forum Standaardisatie	Niels van Campen Erik Wijnen	

Onderwerp

voortgang en voorstel aanpak vraagstukken e-herkenning voor bedrijven

Verzoek aan Forum Standaardisatie

Het Forum Standaardisatie wordt gevraagd:

1. In te stemmen met het groeipad van het authenticatiestelsel.
2. Van het begin af betrokken te zijn bij het opstellen van de berichtenspecificatie, het programma van eisen voor de herkenningmakelaar en de conformiteitstoets.
3. Te zijner tijd berichtenspecificatie 1.0 vast te stellen.

Programma e-Herkenning bedrijven

In dit memo worden de hoofdlijnen weergegeven voor het programma e-Herkenning voor bedrijven. Daarna wordt een aantal voor het Forum Standaardisatie relevante deelprojecten en producten beschreven. Het programma bestaat uit een samenhangend pakket projecten die bedoeld zijn om oplossingen te bieden voor vraagstukken rondom elektronische herkenning van bedrijven (Niet Natuurlijke Personen) in hun contacten met verschillende e-Overheidsdienstverleners. Doel van dit programma is het bij elkaar brengen van het aanbod van middelen voor e-Herkenning van bedrijven en de vraag naar gebruikersherkenning door e-overheidsdienstverleners. Hiertoe wordt een authenticatiestelsel niet natuurlijke personen (hierna het authenticatiestelsel) ingericht. Het authenticatiestelsel omvat een set afspraken en een infrastructuur die is gebaseerd op het gebruik van open standaarden. De werking van het authenticatiestelsel is gebaseerd op het uitwisselen van gestandaardiseerde elektronische berichten tussen verschillende partijen.

Waarom een programma e-Herkenning bedrijven?

Elektronische herkenning van de gebruiker is een voorwaarde voor de ontwikkeling van elektronische dienstverlening door de overheid. Voor elektronische herkenning van de burger is DigiD ontwikkeld. Voor de herkenning

van bedrijven is nog geen goed werkende oplossing voorhanden. De vraag naar e-Herkenning van bedrijven door overheidsdienstverleners bestaat al enige jaren en wordt door toenemende beschikbaarheid van e-overheidsdiensten groter. De techniek en het aanbod van e-Herkenningsmiddelen bestaan ook al enkele jaren. Tot op heden kunnen vraag en aanbod elkaar niet goed vinden. Grote e-Overheidsdienstverleners ontwikkelen daarom 'eigen' maatwerkoplossingen. Kleine en middelgrote dienstverleners ervaren het gemis aan herkenningmiddelen en nemen bij gebrek aan beter soms genoegen met een minder veilige herkenningmethode dan wenselijk is. Kortom er is op de 'herkenningmiddelenmarkt' sprake van systeemfalen. De realisatie van het authenticatiestelsel biedt een oplossing voor verschillende problemen. De rol van de overheid bij de totstandkoming van het authenticatiestelsel is voorwaardenscheppend, in een goede dialoog met de markt, die van de oplossingen gebruik maakt en die in de oplossingen dient te voorzien. Met het oog op fraudepreventie, het juridisch kader en de internationale context van e-overheidsdienstverlening dienen op korte termijn middelen voor elektronische herkenning van een hoge (gekwificeerde) kwaliteit beschikbaar te zijn.

Welke problemen lost het programma op?

Het programma e-Herkenning bedrijven is gericht op het tot stand brengen van het authenticatiestelsel. Het authenticatiestelsel lost een aantal problemen tegelijk op. E-overheidsdienstverleners kunnen gebruikers (bedrijven) herkennen zonder zelf e-herkenningmiddelen te hoeven uitgeven. Gebruikers kunnen met één herkenningmiddel (mits van het juiste niveau) terecht bij alle overheidsdienstverleners. Hiermee wordt het probleem van het digitale sleutelbos, waarbij de gebruiker voor toegang tot verschillende e-overheidsdiensten afzonderlijke sleutels nodig heeft, voorkomen. E-overheidsdienstverleners en aanbieders van herkenningmiddelen kunnen op basis van non-discriminatoire criteria makkelijk toetreden tot het stelsel. Er is sprake van marktwerking tussen de aanbieders van herkenningmiddelen. Binnen het stelsel kunnen bestaande voorzieningen worden (her)gebruikt. Reeds werkende toepassingen hoeven daardoor niet te worden afgeschaft. Wel zullen soms organisatorische en technische aanpassingen nodig zijn om deel te kunnen nemen aan het stelsel. Door (her)gebruik van bestaande (markt) middelen wordt geen geld verspild aan het optuigen van nieuwe voorzieningen. Omdat bestaande middelen worden benut, kan bovendien op korte termijn worden gestart. De samenhang tussen de bestaande voorzieningen zoals NTP, OTP en OSB zal worden versterkt. Door brede beschikbaarheid van e-herkenning van bedrijven zal de elektronische dienstverlening door de overheid zich verder kunnen ontwikkelen.

Regie, beleid en uitvoering

Het programma e-Herkenning voor bedrijven wordt ingericht als een interdepartementaal project onder regie / politiek opdrachtgeverschap van het ministerie van Economische Zaken (EZ). EZ voert in nauwe samenwerking met de betrokken ministeries BZK, Financiën en LNV. de regie over de samenwerking tussen de betrokken partijen (e-overheidsdienstverleners, aanbieders van herkenningmiddelen en ondersteunende diensten). Binnen het programma komt zowel het beleid als de uitvoering aan de orde. Het beleidstraject wordt getrokken door EZ in nauwe samenwerking met genoemde ministeries en een goede dialoog met de betrokken private organisaties. De uitvoering wordt getrokken door de stichting ICTU, binnen het programma Antwoord voor Bedrijven (EZ is penvoerder). De programmaovereenkomst voor het programma Antwoord voor Bedrijven zal met het oog op deze activiteiten uitgebreid. Het programma Antwoord voor Bedrijven zal per 1 januari 2009 opgaan in het programma e-Overheid voor Bedrijven.

Pilots

Vanaf september 2008 worden binnen het programma Antwoord voor Bedrijven pilots gestart waarbij bedrijven, met behulp van herkenningmiddelen, langs elektronische weg rechtsgeldige transacties kunnen verrichten met e-overheidsdienstverleners.

De eerste pilots zijn kleinschalig. Zo wordt begonnen met het exporttraject van pootaardappelen. De pootaardappelboer heeft voor de export van zijn product verschillende overheidsdocumenten nodig. De uitgifte van het ene document is daarbij afhankelijk van de beschikbaarheid van het andere. De documenten worden momenteel door een koerier rondgebracht. In dit traject treedt regelmatig vertraging op. In de pilot zullen de pootaardappelboeren langs digitale weg de benodigde certificaten verkrijgen en transacties kunnen afwickelen. Voor dit proces is e-herkenning een vereiste.

Op dit moment worden er gesprekken gevoerd met de zuivelsector over de start van pilots. In de loop van 2009 zullen pilots met grote e-overheidsdiensten, zoals de belastingdienst, worden gestart. Daarmee komt elektronische dienstverlening beschikbaar voor transacties waar elk bedrijf mee te maken heeft. Dankzij de groei in het volume van elektronische transacties zal het authenticatiestelsel van de grond komen.

Standaardisatie

Internationaal

De EU-dienstenrichtlijn vereist dat e-Overheidsdienstverlening voor alle personen en bedrijven in de EU toegankelijk moet zijn. Dit betekent dat het authenticatiestelsel moet voldoen aan internationale standaarden. Uitgangspunt is dat wordt ingezet op hergebruik van bestaande middelen en bewezen technologie van gekwalificeerd niveau.

Afsprakenstelsel

Het authenticatiestelsel bestaat uit een set afspraken en een infrastructuur die is gebaseerd op het gebruik van open standaarden. Op bestuurlijk niveau worden de opeenvolgende versies van het afsprakenstelsel bekrachtigd. Het afsprakenstelsel omvat:

- de procedure voor toetreding tot het authenticatiestelsel als geheel;
- eisen aan het inschrijvingsproces bij iedere individuele herkenningvoorziening;
- eisen aan de herkenningmiddelen;
- kwaliteitseisen aan de herkenningvoorziening en aan de organisatie die de voorziening aanbiedt;
- Gebruikte standaarden voor informatie-uitwisseling.

De werking van het afsprakenstelsel berust voor een belangrijk deel op het gezamenlijk gebruiken van een berichtenspecificatie en het juist inrichten van de architectuur waarmee deze berichten worden uitgewisseld.

Berichtenspecificatie

Het authenticatiebericht is te zien als een mandje waarmee de gebruiker langs verschillende onderdelen van het authenticatiestelsel wordt gestuurd om authenticatie-informatie op te halen. Als het mandje gevuld is met de gegevens die de dienst aanbieder vraagt, wordt de gebruiker binnengelaten. De inhoud van het mandje en de verbindingen waarover het getransporteerd wordt, zijn dusdanig beveiligd dat er geen valse authenticatie-informatie, die niet afkomstig is van een onderdeel van het stelsel, ingestopt kan worden.

Het uitwisselen van een beveiligd bericht maakt het mogelijk dat ieder onderdeel in het stelsel zijn eigen afgebakende verantwoordelijkheid heeft. Ieder onderdeel geeft antwoord op één vraag en levert een bepaald element van de authenticatie-informatie. Daarbij vertrouwt een onderdeel op de elementen die door voorgaande onderdelen al zijn toegevoegd. Het volgende onderdeel hoeft niet te weten hoe een

conclusie tot stand is gekomen, het hoeft alleen te weten dat die conclusie betrouwbaar is.

Voor de meeste processen geldt dat een simpele ‘hoofdknik’ van een betrouwbare derde waarmee bevestigd wordt dat degene die zich authenticceert bevoegd is om namens een bepaalde niet natuurlijke persoon te handelen volstaat.

Het authenticatiebericht wordt getekend met een elektronische handtekening die onder de PKIoverheid is verkregen. Dat biedt een logische verankering van de publieke verantwoordelijkheid om te zorgen dat de onderdelen van het stelsel elkaar kunnen vertrouwen.

Op basis van het SAML 2.0 protocol is een internationaal geaccepteerde taal beschikbaar om een dergelijk bericht vast te leggen. Daarbij is het belangrijk op te merken dat de beschikbaarheid van een dergelijke “taal” slechts het begin is. Het legt niet vast welke woorden gebruikt worden. Technisch gesproken: hoe de attributen gedefinieerd worden.

Het uitwerken van de berichtenspecificatie is geen geringe opgave. Het kan vergeleken worden met het proces om op basis van internationale standaarden de berichtenspecificaties voor de OSB te bepalen en door het Forum Standaardisatie te laten vaststellen. Na vaststelling door het Forum Standaardisatie zal de specificatie actief beheerd moeten worden.

Het vaststellen van een standaard voor dit bericht sluit aan op de ontwikkeling die GBO.Overheid gepland heeft voor DigiD (waaronder het omzetten van het huidige DigiD authenticatiebericht naar SAML).

Bij het vastleggen van deze nadere specificaties is het van belang dat aangesloten wordt bij het interoperabiliteitsraamwerk / NORA 3.0 in wording en dat daarbij nadrukkelijk wordt gekeken naar Europese interoperabiliteit.

Het opstellen van een robuuste specificatie vergt tijd. Het is ongewenst om met pilots te wachten tot de specificatie gereed is. Daarom zal op korte termijn een beperkte specificatie gerealiseerd moeten worden (versie 0.1). Een belangrijke component hiervan is vast te stellen welke bestaande internationale standaarden als uitgangspunt worden gekozen.

Gelet op de wens om snel van start te gaan, zal er sprake zijn van een groeipad waarbij begonnen wordt met beperkte berichtenspecificatie 0.1 (waarmee bij pilots rechtsgeldige elektronische transacties mogelijk worden gemaakt) en gewerkt worden naar berichtenspecificatie 1.0 die wordt vastgesteld door het Forum Standaardisatie.

Programma van Eisen voor herkenningmakelaar

De herkenningmakelaar is het schakelpunt tussen e-overheidsdienstverlener, de aanbieder(s) van herkenningmiddelen en de gebruiker. Het programma van eisen voor de herkenningmakelaar gaat uit van de berichtenspecificatie en werkt verder uit welke dynamiek, welke berichtenstromen, in het afsprakenstelsel mogelijk zijn en hoe die worden gerouteerd. Het programma van eisen werkt ook de technische vereisten voor aansluiting uit en beschrijft hoe de herkenningmakelaar samenhangt met andere berichtenverkeerdiensten die onderdeel zijn van de e-overheid, zoals de OSB.

Conformiteitstoets

Vanwege de veelheid van partijen die aan het afsprakenstelsel en de berichtenspecificatie moeten voldoen is het van belang dat een conformiteitstoets wordt opgesteld op basis waarvan in het aansluitproces gevalideerd kan worden of aan de minimale eisen is voldaan.

De resultaten van hiervoor genoemde deelprojecten dienen na afronding in beheer genomen te worden bij een organisatie die in de publiek – private context de standaardisatie blijft bewaken, een koppeling met het Forum Standaardisatie ligt daarbij voor de hand. De organisatie die de standaardisatie bewaakt in de beheerfase is de herkenningmakelaar.

Groeipad

Het is belangrijk om vroeg in het traject een beperkte concept invulling van de benodigde standaarden op te leveren en deze dusdanig te benutten dat volgende versies in alle voorzieningen geïmplementeerd kunnen worden; wachten tot de standaard volledig is uitgebalanceerd betekent dat de standaardisatie te laat komt om de verschillende voorzieningen samen te laten hangen. Het is een vereiste om als onderdeel van dit traject werkende pilots op te leveren die de werking van de standaard demonstreren (showcases).