



FORUM STANDAARDISATIE

Agendapunt:	Authenticatie		
Bijlagen:			
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	21 april 2008	Versie	0.1
Betreft:	Authenticatie en autorisatie in Nederland: een voorstel voor verdere ontwikkeling		

Inleiding

In het College Standaardisatie is in 2007 tweemaal van gedachten gewisseld over het thema authenticatie. In de laatste vergadering van het College heeft de voorzitter aan het forum gevraagd aan te geven wat nodig is om een besluit te nemen.

Het Forum constateert dat

- het thema authenticatie - zeker in samenhang met het daarmee nauw verbonden onderwerp autorisatie - complex is;
- dat de hoofdlijnen om tot werkbare oplossingen te geraken niettemin - op basis van de "Verkenning Authenticatie" uit 2007 - helder zijn;
- dat veel activiteiten worden ontwikkeld door veel partijen om het onderwerp verder te brengen, maar dat de samenhang daarin lijkt te ontbreken;
- dat een doorbraak moet worden bereikt in de samenwerking tussen de overheid en private organisaties.

Vanuit die constatering bevat dit memorandum een voorstel voor de verdere aanpak, waarvoor de instemming van het College wordt gevraagd. Voorafgaand daaraan worden de contouren van het vraagstuk nog eens aangegeven, gevolgd door een samenvatting van de hoofdlijnen uit de "Verkenning Authenticatie".

Een dienstbare publieke sector als bondgenoot van de samenleving

Burgers en bedrijven willen een overheid¹

- *waar je met je vragen terecht kunt:* die state-of-the-art-service biedt aan burgers en bedrijven, waar men zeven dagen per week 24 uur per dag terecht kan;
- *die niet naar de bekende weg vraagt:* die de administratieve lasten waarmee zij burgers en bedrijven confronteert, tot een onvermijdelijk minimum beperkt;
- *die je niet voor gek kunt houden:* waarvan vaststaat dat ze slagvaardig optreedt bij fraude en handhaving van wet- en regelgeving, vergunningen en dergelijke;
- *die weet waarover ze het heeft:* waarvan duidelijk is dat haar beleidsontwikkeling stoelt op een gedegen informatiepositie;

¹ Het woord Overheid wordt hier gebruikt in de brede zin van "organisaties in het publieke domein", d.w.z. inclusief maatschappelijke sectoren als zorg en onderwijs.



FORUM STANDAARDISATIE

- *waarop je kunt vertrouwen*: die waakt voor rechtszekerheid en rechtsgelijkheid;
- *die niet meer kost dan nodig is*: die laat zien dat ze, door een goede organisatie en met inzet van moderne hulpmiddelen, haar taken efficiënt vervult;
- *die weet samen te werken met bedrijven en andere organisaties*: die burgers en bedrijven niet lastig valt met steeds weer eigen oplossingen, maar op verstandige wijze benut wat elders al ontwikkeld is.²

Nederlandse burgers en bedrijven ervaren een dienstverlening en handhaving die nog ver van dit ideaal verwijderd is. Verbetering van de dienstverlening aan burgers en bedrijven is dan ook een belangrijke pijler van het kabinetsbeleid.

Elektronische transacties (de “e-Overheid”) spelen daarbij een belangrijke rol.

Misschien nog sneller dan in het publieke domein zijn elektronische transacties de afgelopen jaren onmisbaar geworden tussen burgers (in hun rol van consument) en bedrijven en tussen bedrijven onderling.³

Hulpmiddelen

Net als in de fysieke wereld zijn voor elektronische transacties vormen van **authenticatie** (*is degene die zich aanmeldt wie hij pretendeert te zijn?*) en van **autorisatie** (*welke transacties mag hij dan verrichten?*⁴) noodzakelijk.

Voor de elektronische transacties zijn daarom, zowel in het publieke domein als bij bedrijven, tal van authenticatiemiddelen ontwikkeld. De meest betrouwbare zijn gebaseerd op een eerste identificatie van de burger/klant ‘aan het loket’, registratie van de identiteit en vervolgens uitgifte van een ‘sterk’ (dwz goed beveiligd) authenticatiemiddel. De bekendste zijn de middelen die door de banken worden uitgegeven (veelal pas met token) en voor de overheid DigiD. Daarnaast spelen een aantal TTP⁵-achtige organisaties zoals Diginotar een rol.

Probleemstelling

Overheid én bedrijfsleven willen een sterke groei van elektronische transacties. Vertrouwen van burgers en bedrijven in de daarvoor ontwikkelde methoden en systemen is cruciaal.

Gezamenlijke actie is dringend nodig om adequate beveiliging te verzekeren en het vertrouwen van de burger/klant te borgen.

² Vrij naar een passage uit de brief aan de Tweede Kamer van de ministers van BZK en VROM en de staatssecretaris van EZ d.d. 3 maart 2003, TK 2002-2003, 26387, nr. 18

³ Het Forum ziet het overigens niet als een taak van de overheid om, naast de Standaard die de EU in Richtlijn 1999/93/EG heeft vastgelegd voor de elektronische handtekening, standaarden tot stand te brengen voor authenticatie tussen bedrijven onderling en bedrijven en hun klanten (B2B en B2C); dit memo handelt uitsluitend over standaarden voor authenticatie bij transacties tussen overheden en burgers (G2C), overheden en bedrijven (G2B) en overheden onderling (G2G).

⁴ Deze vraag is tweeledig:

- welke transacties mag een persoon met deze organisatie verrichten?
- heeft een persoon mandaat om namens een andere (rechts)persoon handelend op te treden?

⁵ Trusted Third Party



FORUM STANDAARDISATIE

Doordat veel private en publieke organisaties ieder hun eigen **authenticatiemiddel** uitgeven is de beveiliging suboptimaal en/of kostbaar. Immers, ieder moet voor zich de noodzakelijke investeringen doen.

Zo ontstaat voor de consument een ‘digitale sleutelbos’ met te veel authenticatiemiddelen waarvan de betrouwbaarheid beperkt is.

DigiD voor burgers is in zijn huidige vorm onvoldoende beveiligd voor “zwaardere” transacties.⁶ Bovendien functioneert DigiD voor bedrijven onvoldoende en dreigt de ondersteuning ervan binnenkort beëindigd te worden.

Verder zijn in Europees verband nog geen duidelijke lijnen voor elektronische authenticatie en autorisatie vastgesteld. Zonder dat zal het “ene elektronische loket” zoals voorzien in de Dienstenrichtlijn illusoir blijken. Indien Nederland erin slaagt op korte termijn een heldere aanpak voor deze vraagstukken te kiezen heeft het de mogelijkheid in Europees verband mede de toon te zetten. Langer wachten betekent dat wij elders gemaakte keuzes zonder meer zullen moeten accepteren.

Ook zijn in het publieke domein oplossingen voor het **autorisatievraagstuk** nog in een pril stadium van ontwikkeling.⁷ Hoewel autorisatie nauw samenhangt met authenticatie (zonder elektronische authenticatie geen elektronische autorisatie) is het verstandig de beide vraagstukken wel goed te blijven onderscheiden.

In dit verband is tenslotte nog van belang dat het Ministerie van EZ recent aan CapGemini opdracht heeft gegeven aan de hand van een aantal use cases de behoeften bij dienstenaanbieders op het gebied van authenticatie van niet-natuurlijke personen en de aanwezige markt- en overheidsmiddelen in kaart te brengen met aanbevelingen voor het vervolg. Dit onderzoek moet op 1 juli 2008 zijn afgerond.⁸

Samenwerking

Samenwerking is hier geboden. Daartoe zouden partijen hun authenticatiemiddelen beschikbaar moeten stellen voor andere aanbieders van diensten en zouden die partijen en de gebruikers moeten kunnen vertrouwen op die authenticatiemiddelen.

Het ligt voor de hand dat de overheid hier een rol in speelt. Zij geeft immers ook de ‘analoge’ identificatiemiddelen uit en borgt deze voor algemeen gebruik.

De overheid kan daarbij een aantal rollen vervullen. Zo zou zij het noodzakelijke toezicht op authenticatie vorm kunnen geven evenals het toezicht op de privacyaspecten en standaardisatie en certificering kunnen bevorderen in samenwerking met de marktsector die evenzeer een aantal rollen op zich kan nemen.

Het forum stelt voor daarbij de hoofdlijnen van de “Verkenning Authenticatie” tot vertrekpunt voor de komende drie jaar te nemen:

- uniformeer het begrippenkader;
- stel kwaliteitsklassen en bijbehorende criteria vast;

⁶ Het lichte (BSN met wachtwoord) en middenniveau (BSN met SMS) zijn voor natuurlijke personen wel beschikbaar.

⁷ Hieraan wordt gewerkt in het programma G(emeenschappelijke) M(achtigings) V(oorziening).

⁸ Daarnaast lopen nog een aantal andere onderzoeken waarvan het te ver zou voeren die hier op te sommen.



FORUM STANDAARDISATIE

- schaal authenticatiemiddelen in;
- sluit waar mogelijk aan op internationale standaarden;
- laat authenticatieserviceproviders, waaronder DigiD, hun rol spelen;
- accepteer als overheid ook authenticatiemiddelen van non-overheid issuers;
- werk het concept “authenticatieserviceprovider” uit, inclusief regulering.

Doe dit alles in samenwerking tussen overheid en bedrijfsleven.

Voorstel

Authenticatie en autorisatie voor e-transacties vormen een ingewikkeld conceptueel vraagstuk dat dringend moet worden opgelost om een veilig gebruik van internet in zowel het publieke als het private domein mogelijk te maken. De tijd om tot oplossingen te komen dringt. Bedrijven beschouwen het probleem als buitengewoon urgent. In Europees verband zullen op korte termijn belangrijke keuzes gemaakt moeten worden. Het is voor Nederland belangrijk daarbij niet volgend maar leading te zijn.

Authenticatie en autorisatie vormen bovendien een organisatieoverstijgend vraagstuk. Het gevaar is dat niemand zich er eigenaar van voelt, dan wel juist iedereen zijn eigen oplossing ontwikkelt. Het Forum Standaardisatie meent dat het College Standaardisatie bij uitstek gepositioneerd is om als sponsor van dit vraagstuk op te treden.

Om het proces op gang te krijgen zijn van groot belang:

- het helder en éénduidig neerzetten van een begrippenkader;
- het verkennen van de rollen van de marktsector en van de overheid.

Voorgesteld wordt dat het College Standaardisatie het Forum opdraagt om voor 1 september 2008:

- de mogelijkheden voor het vaststellen van standaarden voor authenticatie bij elektronische transacties tussen burgers en de overheden, bedrijven en overheden en tussen overheden onderling te onderzoeken;⁹
- het autorisatievraagstuk daarbij te betrekken;
- een helder en éénduidig begrippenkader op te stellen;
- in nader te bepalen vorm de mogelijkheden van een doorbraak in de samenwerking op dit punt tussen overheid en bedrijfsleven te verkennen;¹⁰

dit met het oogmerk te komen tot voorstellen voor een daadwerkelijke aanpak die kan starten per 1 november 2008.

⁹ Zulks in nauw contact met de uitvoerders van het door EZ aan CapGemini opgedragen onderzoek.

¹⁰ Daarbij dient te worden afgestemd met de activiteiten van het Platform Authenticatie van ECP.NL.