MEMO

Aan: Forum Standaardisatie
Betreft: authenticatie in Nederland: een voorstel voor verdere ontwikkeling
Van: BZK, EZ
Datum: 09 februari 2008

Één goede sleutel is genoeg…..

1 Inleiding

Overheidsorganisaties bieden steeds meer diensten elektronisch aan aan burgers en bedrijven. Voor deze diensten is het noodzakelijk om te beschikken over een authenticatieservice[1] die de identiteit van de burger of het bedrijf met voldoende mate van zekerheid vaststelt. De overheid maakt hiervoor in het algemeen gebruik van de service die centraal wordt geboden met DigiD.

Het betrouwbaarheidsniveau van de dienstverlening van een authenticatieservice zal moeten aansluiten bij het risicoprofiel van een specifieke webdienst. Zo zal voor webdienst waarbinnen gebruikers gevoelige informatie uitwisselen een hoger zekerheidsniveau nodig zijn, dan voor een webdienst waarbinnen gebruikers alleen openbare informatie opvragen.
Alle huidige door de overheid aangeboden webdiensten kennen maximaal een risicoprofiel die passen binnen de door DigiD aangeboden betrouwbaarheidsniveaus “Basis” en “Midden”. Op termijn zullen hogere veiligheidsniveau’s noodzakelijk zijn als meer geavanceerd diensten worden aangeboden. Sowieso is een tendens zichtbaar naar gebruik van zwaardere beveiligingsniveau’s - vanuit de optiek van de huidige elektronische overheidsdienstverlening is zijn die praktisch gesproken nog niet nodig, maar het is een ontwikkeling die zeker niet ware af te wijzen.

2 Nieuwe vragen

De vraag die langzamerhand aan de orde komt is: moet de overheid zélf een eigen authenticatieservice bieden en (blijvend) verder ontwikkelen?
Deze vraag wordt ingegeven door het feit dat maatschappelijk steeds massaler elektronische diensten worden aangeboden, waarbij vele organisaties hun eigen authenticatieservice ontwikkelen. Aangezien dit niet kosteneffectief is, en de eisen aan zo’n voorziening steeds strikter worden, ziet men de ontwikkeling dat

[1] Onder authenticatie wordt in dit verband verstaan: elektronische verificatie van een geregistreerde identiteit

gespecialiseerde bedrijven authenticatieservices op de markt aanbieden aan aanbieders van elektronische diensten.
Er is veel voor te zeggen dat de overheid gebruik zou gaan maken van de voorzieningen die in de markt aanwezig zijn. Maar ook kan de authenticatievoorziening van de overheid voor marktpartijen worden opengesteld: de overheidsvoorziening wordt immers ook door de overheid geborgd en is voor alle Nederlanders beschikbaar, hetgeen een voordeel is[2]. Het kan de verdere ontwikkeling van elektronische dienstverlening in Nederland bevorderen, en daarmee ook economisch interessant zijn.

3 Een logische gedachte?

Bovenstaande (gezamenlijk gebruik van een infrastructurele voorziening) lijkt een logische gedachte. Maar waarom zou deze ontwikkeling zich dan niet spontaan voordoen? Daarvoor is een tweetal oorzaken aan te wijzen:

A Het betreft een nieuw en relatief nog onbekend terrein. Dit impliceert dat de marktwerking nog niet tot echte wasdom is gekomen.
Dit uit zich zowel in het feit dat ‘zelf doen’ (en dus weer opnieuw het wiel uitvinden) nog steeds veel voorkomt. Een authenticatievoorziening wordt derhalve nog te weinig beschouwd als een soort nuts- of infrastructurele voorziening. Er vindt dus ook onvoldoende volwassen bedrijfseconomische afweging plaats bij de inzet. Dit geldt zeker ook bij de overheid, hetgeen leidt tot veel discussie over onder andere de financieringswijze van DigiD.
Ook uit zich dit in de waarde die sommige organisaties hechten aan ‘hun eigen voorziening’ uit een oogpunt van *branding*. Men ziet dit bijvoorbeeld in de banksector, en ook bij de overheid (‘onze eigen DigiD’).

B Gebruik van een authenticatievoorziening die door een andere partij wordt geleverd impliceert dat men moet kunnen vertrouwen op deze partij. Dit is van groot belang: immers, het gaat om een vorm van elektronische identificatie van een klant of gebruiker.
Aan de orde zijn daarbij zowel het vertrouwen in een juiste afhandeling van een authenticatie, als het vertrouwen dat adequaat wordt omgegaan met de klantgegevens van de opdrachtgever. Dit laatste zowel uit een oogpunt van privacy als uit een oogpunt van commerciële belangen.
Dit vertrouwen is echter nog niet adequaat geborgd middels toezicht en controle.

[2] Kanttekening daarbij is, dat DigiD niet geschikt is voor authenticaties die een hoog betrouwbaarheidsniveau vragen. De overheid werkt overigens inmiddels aan de uitgifte van de gecertificeerde elektronische handtekening op de Nederlandse identiteitskaart.

Het tweede punt levert verreweg de belangrijkste obstakels voor het medegebruik. De kwestie is, of de overheid hier een rol zou kunnen spelen om de verdere ontwikkeling van authenticatie te bevorderen.
Het antwoord hier op is positief om een aantal redenen:

- het economisch belang voor Nederland van de verdere ontwikkeling van elektronische dienstverlening
- het belang van Nederlandse burgers en bedrijven bij een betrouwbare authenticatie en een meer beperkte set authenticatiemiddelen
- het belang van veiligheid op het internet

4 Wat is de rol voor de overheid

Teneinde de rol van de overheid beter in beeld te krijgen, dient eerst het authenticatieproces nader te worden bezien[3].
Goed onderscheid moet worden gemaakt naar de diverse rollen of verantwoordelijkheden die in het dit proces zijn te onderscheiden. De volgende rollen komen naar voren (waarvan sommige in de huidige praktijk dus nog niet goed zijn uitgekristalliseerd)[4]:

A De klant: een burger of bedrijf die aangeboden elektronische diensten wil afnemen, en zich daartoe kenbaar moet maken via het internet en zich daar moet authenticeren.

B De aanbieder van elektronische dienstverlening, de gebruiker. De gebruiker heeft authenticatie van zijn klanten nodig om transacties elektronisch te kunnen afwikkelen. De gebruiker beoordeelt daarbij welk betrouwbaarheids- of veiligheidsniveau voor zijn transacties noodzakelijk is, en maakt kenbaar aan de klant wat voor authenticatiemiddel (dus) gebruikt moet worden.

C Een aanbieder van authenticatiemiddelen, oftewel een authenticatie service verlener (ASP). Dit is een organisatie die authenticatiemiddelen beheert en uitgeeft aan burgers en/of bedrijven, én die bereid is deze middelen te laten classificeren en door andere organisaties te laten gebruiken.
De ASP is daarmee een Trusted Third Party (TTP), die ten behoeve van de klant en de gebruiker, het gebruik van authenticatiemiddelen (op verschillende betrouwbaarheidsniveau's) aanbiedt ten behoeve van een door beide partijen gewenste elektronische transactie. Het resultaat van die koppeling wordt doorgegeven aan de gebruiker en de klant (een soort elektronisch 'OK'), zodat de gewenste transactie kan worden afgewikkeld.

D Een standaardisatie-autoriteit, die een classificatie afgeeft voor de betrouwbaarheid van authenticatiemiddelen. Met andere woorden: zij geeft aan, aan welke eisen moeten worden voldaan voor een bepaald

[3] Onder andere is door KPMG een studie verricht, op initiatief van het Standaardisatieforum van GBO.
[4] Enerzijds behoeven niet alle genoemde verantwoordelijkheden behoeven in afzonderlijke organisaties te zijn ondergebracht, anderszijds zullen voor sommige afzonderlijke verantwoordelijkheden meer organisaties aanwezig zijn (bijvoorbeeld het toezicht).

betrouwbaarheidsniveau van authenticatie. Het gaat hier met name om eisen op het gebied van identiteitsvaststelling, uitgifteprocedures, beveiliging (ook tav privacy) en (mogelijk) technische voorzieningen.

E Een beoordelende partij, de certificeerder. Deze beoordeelt en classificeert authenticatiemiddelen op betrouwbaarheidsniveau, aan de hand van toepassing van de eisen van de standaardisatie-autoriteit.

F Een aanbieder van identiteitsverificatie, die bereid is te (laten) verifiëren of de door een authenticatie-service-verlener geregistreerde persoonsgegevens overeenkomen met de gegevens van deze verificateur.
Zo'n verificatie kan aanmerkelijk het betrouwbaarheidsniveau én het bereik van een authenticatiemiddel verhogen, afhankelijk van de aard, het bereik en de kwaliteit van de gegevens van de verificateur. Indien de overheid bereid zou zijn (met behulp van het BSN en binnen de overheidsorganisatie zelf) haar formele persoonsgegevens te koppelen aan een authenticatiemiddel, zou dit een belangrijke bijdrage kunnen leveren aan de betrouwbaarheid van elektronische transacties en de breedte van de klantenkring voor authenticatiemiddelen. Of dit kan, is afhankelijk van de vraag of het BSN (uiteraard op vrijwillige basis) gebruikt mag worden in het verkeer tussen burger en ASP (een politieke vraag). Overigens wordt een vergelijkbare systematiek heden ook toegepast, maar dan op basis van een voorgaande (overigens wettelijk verplichte) identificatie van een burger door een bedrijf (bijvoorbeeld een bank).

G Een onafhankelijke toezichthouder, ten behoeve van het toezicht op het operationeel correct functioneren van partijen, ook wat betreft de privacy-aspecten.

Het is duidelijk dat de overheid een rol zou kunnen spelen bij praktisch alle genoemde verantwoordelijkheden. Bij sommige rollen (toezicht, klant, gebruiker) 'moet' zij dat ook, bij andere (ASP) is het beter de markt aan bod te laten komen. En ook is duidelijk dat iets dergelijks geldt voor marktpartijen: zij kunnen óók praktisch alle rollen vervullen, maar de ene goed en de andere minder goed (zoals toezichthouder en verificateur).

Als er aan een taakverdeling tussen markt en overheid wordt gedacht, dan zou, buiten de rollen van klant (A) en gebruiker (B), aan het volgende beeld kunnen worden gedacht:

C authenticatie service verlener	markt (de overheid zou DigiD in de markt kunnen inbrengen)
D standaardisatie-autoriteit:	overheid en markt (standaardisatieforum)
E certificeerder	markt
F verificateur	overheid (BZK)
G toezichthouder	overheid (Opta en Cbp)

Bij een dergelijke taakverdeling is het overigens mogelijk dat in de markt een nieuwe figuur ontstaat die vraag en aanbod van authenticatiemiddelen bij elkaar brengt: een authenticatiemiddelen-makelaar.

5 Initiatief van de overheid: een voorstel en een verzoek

Belangrijk voor de verdere ontwikkeling van elektronische authenticatie is, dat de overheid een verantwoordelijkheid neemt voor de punten F en G, voor zowel de overheid als de markt – dus ten behoeve van 'Nederland BV'.
Dit zal dienstbaar zijn aan de ontwikkeling van adequate authenticatie voor de elektronische dienstverlening, en daarmee voor de economische ontwikkeling zowel als voor het functioneren van de overheid in Nederland. Voorts bevorderd dit naar het zich laat aanzien verbeteringen uit een oogpunt van privacybescherming.

Realisatie van zo'n initiatief zou, indien dit de markt activeert, kunnen betekenen dat men straks met een authenticatiemiddel van de banken zaken kan doen met de Belastingdienst en de gemeente, zowel als met de autoverhuurder of de supermarkt. En met een DigiD van de overheid kan men dan terecht bij de Hema, bij bol.com of een gemeente. Enzovoorts….
De burger en het bedrijf worden zo optimaal bediend bij de toegang tot de elektronische snelweg, de digitale sleutelbos kan definitief worden bijgezet in het museum, en de elektronische dienstverlening krijgt een belangrijke impuls.

Een dergelijk initiatief is innovatief, en past binnen de ontwikkelingen rond authenticatie die worden waargenomen bij de EU en in andere landen.
Bovendien kan het een goede start zijn van verdere samenwerking tussen overheid en bedrijfsleven, wat van belang is voor de noodzakelijke verdere ontwikkelingen op authenticatieterrein en voor de positie van Nederland, zowel voor de overheid als het bedrijfsleven.

Het voorstel dat voorligt is, om als eerste stap nader onderzoek te verrichten naar deze verdere ontwikkeling in samenspraak met marktpartijen.
Met name de volgende aspecten dienen nader te worden bezien en uitgewerkt:

- *marktkansen / business-case*
- *privacybescherming*
- *mogelijkheden voor overdracht van DigiD naar de markt.*

Op basis van de uitkomsten kan worden nagedacht over een ontwikkelingstraject.