FS-2007307.05B

KPMG

Information Risk Management

Forum Standaardisatie

Verkenning Authenticatie

Roeien met de riemen die je hebt?

ADVISORY

AUDIT ▪ TAX ▪ ADVISORY

Forum Standaardisatie

Verkenning authenticatie

Roeien met de riemen die je hebt?

KPMG Information Risk Management
Amstelveen, maart 2007
Dit rapport heeft 25 pagina's
R.2007.ISC.18
AvZ/PP/JS/nv

Forum Standaardisatie
Verkenning authenticatie
KPMG Information Risk Management
Amstelveen, maart 2007

Inhoudsopgave

Managementsamenvatting

In een verkenning naar authenticatie, uitgevoerd op verzoek van het Forum Standaardisatie, is duidelijk geworden dat in Nederland burgers en organisaties rijkelijk worden voorzien van middelen waarmee ze in communicatie op het internet hun identiteit kunnen bewijzen. Passen, wachtwoorden en biometrische gegevens: ieder beschikt inmiddels over een uitgebreide verzameling aan dergelijke zogenaamde authenticatiemiddelen. Geen probleem dus, zo lijkt het.

Echter, bij nadere beschouwing blijkt de huidige situatie rond authenticatie wel degelijk voor een veelheid aan problemen te zorgen, zoals:

- onnodige kosten voor organisaties (uit overheid en bedrijfsleven) die met hun gebruikers transacties willen uitvoeren;

- een toenemende kans op identiteitsfraude doordat gebruikers een zodanige overdaad aan authenticatiemiddelen (een digitale “sleutelbos”) hebben dat een slordig beheer ervan in de hand wordt gewerkt;

- een relatief hoge drempel voor organisaties die op het internet op een betrouwbare manier zaken willen doen, doordat zij daartoe eerst een infrastructuur voor het uitgeven en beheren van authenticatiemiddelen moeten inrichten en onderhouden.

In deze situatie is verbetering te brengen door een aantal zaken te standaardiseren, te weten:

- de gebruikte terminologie, zodat in de communicatie over dit onderwerp verwarring wordt voorkomen (er bestaan namelijk vele definities voor de gebruikte termen);

- kwaliteitsklassen voor authenticatiemiddelen, waarmee de mate van zekerheid die aan het gebruik van een bepaald authenticatiemiddel mag worden ontleend voor alle betrokken partijen duidelijk is.

Aanvullend is een tweetal initiatieven onderkend die het eveneens een wezenlijke bijdrage aan een gezonde situatie rond authenticatie in Nederland (en buitenland) kan leveren:

- de overheid kan, met de authentieke registers zoals het GBA als basis, authenticatiemiddelen uitgeven die als fundament kunnen worden gebruikt bij het uitgeven van authenticatiemiddelen door de private sector;

- het inrichten van een zogenaamde “authenticatie serviceprovider” kan ervoor zorgen dat aanbieders van diensten op het internet gebruik kunnen maken van de authenticatiemiddelen die door andere organisaties zijn uitgegeven. Hiermee kan de digitale sleutelbos van gebruikers beperkt blijven, behoeven dienstaanbieders aanzienlijk minder kosten te maken en wordt bestrijding van identiteitsfraude versterkt. Dit concept biedt ook kansen voor de Nederlandse positie in het internationale veld.

Bij het bovenstaande moet worden opgemerkt dat samenwerking tussen overheid en bedrijfsleven essentieel is om de initiatieven te realiseren en te laten aanslaan. Binnen de eigen verantwoordelijkheden van overheid en bedrijfsleven lijken daar goede mogelijkheden toe te zijn.

“Roeien met de riemen die je hebt?” Nee, door de riemen met elkaar te delen kunnen we samen meer kracht ontwikkelen.

1 Inleiding

1.1 Opdracht

Aan KPMG is door ICTU/GBO.overheid ten behoeve van het Forum Standaardisatie de volgende opdracht verstrekt: voer een verkennend onderzoek uit naar mogelijkheden voor synergie tussen en binnen de overheid en het bedrijfsleven ter zake van identificatie en authenticatie van burgers en organisaties in de elektronische (internet) omgeving.

1.2 Werkwijze

Dit onderzoek is verkennend van aard en uitgevoerd in de periode februari en maart 2007. Op basis van de onderzoeksvraag is een interviewvragenlijst opgesteld en gevalideerd door de opdrachtgever. Er zijn door opdrachtgever in overleg met KPMG acht personen geselecteerd en geïnterviewd. Een overzicht van de geïnterviewden is opgenomen als bijlage A. Deze interviews zijn voor het onderzoek, naast literatuur, gebruikt als bron van informatie. Het beeld dat op grond van de verzamelde informatie ontstond is op 7 maart 2007 met het Forum Standaardisatie besproken. Dit heeft geresulteerd in het onderhavige rapport.

1.3 Uitgangspunten

Bij dit onderzoek zijn de volgende uitgangspunten gehanteerd:

- er bestaan vele definities voor de terminologie rond het onderzoeksonderwerp. Het onderzoek beoogt niet hierin uitsluitsel te geven;
- de overheid heeft het exclusieve recht én de plicht om wettelijke identificatiebewijzen uit te geven;
- de behoefte aan authenticatie ten behoeve van communicatie op het internet zal de komende jaren sterk groeien;
- de verkenning richt zich op standaardisatie die breder is dan alleen standaardisatie binnen de overheid;
- de technische dimensie van authenticatie wordt als gegeven aangenomen.

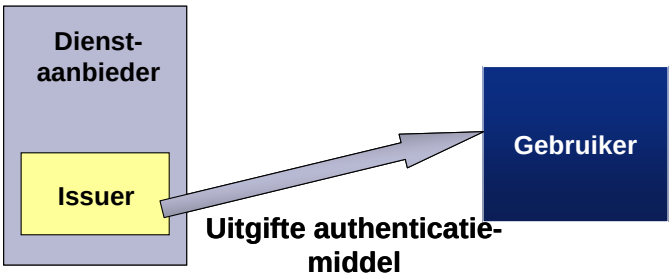
2 Gehanteerde begrippen

In dit rapport worden diverse specifieke begrippen gehanteerd. Onderstaande begrippenlijst geeft een vereenvoudigde omschrijving van deze begrippen. Bijlage B bevat voor de geïnteresseerde lezer formele, gangbare definities van deze begrippen.

- Identiteitsfraude: Het zich voordoen als een ander (bijvoorbeeld het onbevoegd onder de naam van een ander transacties uitvoeren).
- Identificatie: Het claimen van een identiteit (“Ik ben Jan”).
- Authenticatie: Het bewijzen van een geclaimde identiteit (bijvoorbeeld met een geheim wachtwoord dat alleen Jan en zijn communicatiepartner kennen).
- Authenticatiemiddel: Het middel dat wordt gebruikt bij authenticatie, i.c. iets wat de gebruiker weet, bezit of is (bijvoorbeeld een wachtwoord, een pasje of een vingerafdruk).
- Kwaliteitsniveau: de mate waarin een authenticatiemiddel zekerheid verschaft over een geclaimde identiteit.
- Autorisatie: De bevoegdheid tot het uitvoeren van een handeling.
- Dienstaanbieder: Een aanbieder van een dienst die via internet wordt ontsloten.
- Gebruiker: Een individu of organisatie die van een dienst op internet gebruikmaakt of wil maken.
- Issuer: Een organisatie die authenticatiemiddelen uitgeeft.
- Authenticatie serviceprovider: Een organisatie die, als een intermediair voor een dienstaanbieder, de authenticatie van een gebruiker bij een issuer afhandelt.

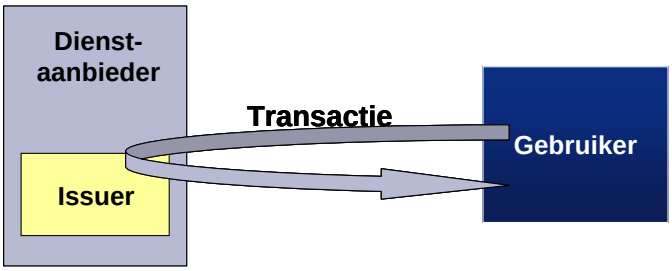
3 Huidige situatie

Elke dienstaanbieder bepaalt, voor gebruikers die van “zijn” dienst gebruik willen maken, of hij zekerheid over de identiteit van die gebruikers wil hebben. En, indien dat zo is, welke mate van zekerheid hij wenst. Op basis daarvan zorgt de dienstaanbieder ervoor dat die gebruiker over een authenticatiemiddel beschikt waarmee authenticatie van de geclaimde identiteit met de gewenste zekerheid kan plaatsvinden (figuur 1): de dienstaanbieder treedt zelf als issuer van die authenticatiemiddelen op.



Figuur 1: Uitgifte van een authenticatiemiddel aan een gebruiker

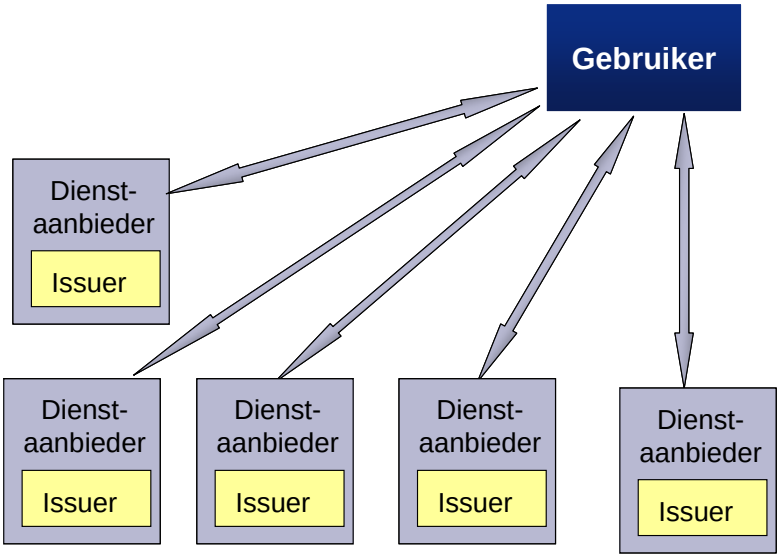
Omdat de dienstaanbieder zelf het authenticatiemiddel heeft uitgegeven, kan hij ook zelf de authenticatie van de gebruiker uitvoeren voordat die gebruiker een transactie/handeling mag uitvoeren (figuur 2).



Figuur 2: Transactie met authenticatie

Op deze manier heeft elke organisatie in Nederland die diensten via het internet aanbiedt, de authenticatie van zijn gebruikers geregeld. Iedere organisatie “roeit met de riemen die men heeft”.

Vanuit het perspectief van de gebruiker ziet het plaatje er helaas minder prettig uit (zie figuur 3). De huidige situatie heeft er namelijk in geresulteerd dat een gebruiker voor elke dienst die hij wil gebruiken een separaat authenticatiemiddel krijgt uitgereikt. Dit leidt ertoe dat gebruikers inmiddels vele wachtwoorden moeten onthouden en series pasjes hebben. De digitale sleutelbos is een feit.



Figuur 3: Authenticatiemiddelen van diverse dienstaanbieders

Overheidsorganisaties in Nederland zijn inmiddels gestart met het gezamenlijk gebruik van dezelfde authenticatiemiddelen (DigiD-wachtwoord, eenmalig wachtwoord via SMS). Alhoewel de overheid hiermee een bijdrage levert aan het beperken van de omvang van de digitale sleutelbos kan met echter stellen dat de overheid zich gedraagt als een grote private organisatie waarin bijvoorbeeld diverse divisies besluiten om van dezelfde authenticatiemiddelen gebruik te maken. De invloed hiervan op de situatie van de gebruiker is vooralsnog beperkt.

Het aantal communicatiemiddelen waarmee gebruikers via internet communiceren met dienstaanbieders groeit namelijk nog steeds. Voorbeelden hiervan zijn mobiele telefoons voor betalingen (zowel overboekingen als retail) en set-top-boxen. Hierdoor blijft het aantal authenticatiemiddelen dat een gebruiker nodig heeft ook groeien, onder meer in de vorm van SMS-authenticatie en smartcards. Ook de komst van de OV-chipkaart en de zorgpas breidt het aantal authenticatiemiddelen uit.

Een grote digitale sleutelbos is om diverse redenen ongewenst:

- Gebruikers hebben zoveel authenticatiemiddelen dat dit tot een onoverzichtelijke situatie en een sterke vermindering van gebruiksgemak leidt. Het gebruik van diensten zou daar ook onder kunnen leiden.

- Door de veelheid van authenticatiemiddelen (veelal wachtwoorden) zullen de meeste gebruikers er niet aan ontkomen om deze op te schrijven teneinde ze te kunnen onthouden. Ook de kwaliteit van elk authenticatiemiddel is voor de gebruiker onduidelijk. Bovendien leidt de veelheid ertoe dat de gemiddelde gebruiker zich hierin ook niet zal verdiepen. Dit alles leidt tot vermindering van kwaliteit in de authenticatie en ook tot een stijgende kans op identiteitsfraude.

Vanuit het perspectief van de individuele dienstaanbieder lijken er op dit moment geen issues te zijn. Immers, de benodigde authenticatie kan plaatsvinden. Echter, bij nadere beschouwing blijkt dat:

- diverse dienstaanbieders aangeven dat de kosten van het uitgeven en beheren van authenticatiemiddelen hoger zijn dan gewenst doordat elke dienstaanbieder een eigen infrastructuur daarvoor moet inrichten, onderhouden en beheren;

- diverse dienstaanbieders in de kosten een belemmering zien om authenticatie in te voeren dan wel om over te gaan tot het inzetten van sterke(re) authenticatiemiddelen. Dit blijkt onder meer door verzoeken aan bestaande issuers (zoals overheid en banken) om de door hen uitgegeven authenticatiemiddelen te mogen gebruiken.

Ook vanuit het perspectief van de overheid leidt de huidige situatie tot ongewenste effecten. De toenemende identiteitsfraude is een bron van zorg die ondermeer vanuit de overheid de nodige aandacht dient te krijgen.

Deze issues worden breed onderkend. Er zijn al vele onderzoeken uitgevoerd, overleggen gevoerd en allerlei initiatieven gestart, zoals de invoering van het DigiD-wachtwoord en Digid als authenticatie serviceprovider voor overheidsorganisaties. Ook binnen grote organisaties zien we een tendens om het aantal authenticatiemiddelen dat intern wordt gebruikt en aan klanten wordt uitgegeven, omlaag te brengen.

Dit blijven echter eiland-oplossingen: elke dienstaanbieder probeert voor zichzelf en “zijn” gebruiker de situatie te verbeteren. De geschetste issues in deze paragraaf worden hiermee niet opgelost. De gebruiker blijft met een groeiende digitale sleutelbos zitten en de dienstaanbieders blijven geconfronteerd worden met onnodig hoge kosten.

Uiteindelijk zijn de gebruikers (burgers en organisaties) het kind van de rekening. De kosten van alle infrastructuren worden namelijk uiteindelijk op de gebruikers afgewenteld. Lastenverhoging is het resultaat, waar lastenverlichting geboden is.

In het volgende hoofdstuk wordt ingegaan op de kenmerken van een “ideale” situatie, waarin de geschetste issues wel zijn opgelost.

4 Kenmerken ideale situatie

Niet alleen in Nederland, maar ook in het buitenland, is onderkend dat de situatie rond authenticatie slimmer kan dan elke dienstaanbieder zijn eigen authenticatiemiddel te laten uitgeven. Binnen Europa zien we voorbeelden daarvan in ondermeer Oostenrijk, Denemarken, Zweden, Finland, Estland, Italië en Malta. Daar is een oplossing voor de problematiek gezocht in samenwerking tussen overheid en bedrijfsleven.

Mede op grond van de inzichten die in het buitenland zijn verkregen en de uitgevoerde verkenning zijn een aantal kenmerken van de “ideale” situatie rond authenticatie onderkend, namelijk:

- De gebruiker kan zelf bepalen welke omvang zijn digitale sleutelbos heeft doordat dienstaanbieders bestaande authenticatiemiddelen, registratie- en uitgifteprocessen zo breed mogelijk hergebruiken. Dit zorgt er tevens voor dat nieuwe dienstaanbieders geen eigen authenticatiemiddelen hoeven uit te geven en dus niet met de noodzaak tot forse investeringen in de inrichting, het onderhoud en het beheer van een eigen infrastructuur worden “bestraft” als zij identiteitsfraude willen tegengaan. Tevens kan bij technologische ontwikkelingen snel kritieke massa aan gebruikers worden gecreëerd.

- De kwaliteit van authenticatiemiddelen is duidelijk, zowel voor dienstaanbieders als gebruikers.

- De overheid zorgt in de elektronische wereld voor authenticatie-middelen die zijn uitgegeven op basis van de authentieke registers. De overheid kan zo een fundament leggen voor onder meer private sterke authenticatiemiddelen waarmee identiteitsfraude tegengegaan kan worden. Hiermee ontstaat een parallel met het gebruik van het paspoort in de fysieke wereld dat zijn basis vindt in de GBA.

- De manier waarop en de middelen waarmee in Nederland wordt voorzien in authenticatie sluiten aan op de ontwikkelingen in internationaal verband. Zowel dienstaanbieders, gebruikers als issuers werken in toenemende mate op internationale schaal. Internet kent immers geen grenzen.

Het volgende hoofdstuk schetst op welke vlakken overheid en bedrijfsleven standaardisatie en samenwerking kunnen inzetten om de huidige situatie om te buigen naar een situatie die aan bovenstaande kenmerken voldoet.

5 Mogelijkheden tot standaardisatie en samenwerking

Bij het oplossen van de problematiek zoals geschetst in hoofdstuk 3 en om stappen te zetten richting de “ideale” situatie rond authenticatie kan standaardisatie van diverse aspecten een belangrijke bijdrage leveren. Om tot die standaardisatie te komen zullen overheid en bedrijfsleven nauw moeten samenwerken teneinde de gebruiker (burgers èn organisaties) te verlossen van de groeiende digitale sleutelbos. De paragrafen 5.1, 5.2 en 5.3 beschrijven welke initiatieven worden voorgesteld. Bij al deze initiatieven dient te worden meegenomen dat een hechte aansluiting op de internationale situatie dient te worden bereikt. Hiermee wordt voorkomen dat de resultaten van de initiatieven alleen bruikbaar zijn in de Nederlandse omgeving.

Aanvullend valt te overwegen om in samenwerking tussen overheid en bedrijfsleven te komen tot een initiatief inzake de authenticatieproblematiek dat een wezenlijke stap voorwaarts kan betekenen. Een voorstel hiertoe is opgenomen als paragraaf 5.4.

5.1 Terminologie

Het voeren van de discussie over en het bepalen van beleid betreffende authenticatie valt of staat met de helderheid van de communicatie over dit onderwerp. Alle betrokken partijen dienen daarom eenzelfde terminologisch kader te gebruiken. Het verdient aanbeveling om dit kader in overleg tussen overheid en bedrijfsleven vast te stellen.

Een kanttekening verdient de aanduiding “DigiD”. Deze term behoeft ook verheldering. Immers, momenteel wordt dezelfde term gebruik als aanduiding van:

- het authenticatiemiddel dat door de overheid wordt uitgegeven (het DigiD-wachtwoord);
- het technisch platform dat voor de dienstaanbieders in de overheid de authenticatie verzorgt (DigiD als authenticatie service provider);
- de organisatie die de voorgaande twee voorzieningen verzorgt.

Hierdoor ontstaat onnodig verwarring en het verdient aanbeveling terminologisch onderscheid tussen voornoemde drie aspecten te creëren.

5.2 Kwaliteitsklassen authenticatiemiddelen

Om duidelijkheid te scheppen in de kwaliteit van een authenticatiemiddel verdient het aanbeveling kwaliteitsklassen vast te stellen die een aanduiding geven van de kracht van authenticatiemiddelen. Tevens dient te worden bepaald aan welke criteria authenticatiemiddelen dienen te voldoen teneinde tot een bepaalde klasse te worden “toegelaten” en welke organisatie die toetsing uitvoert.

Naast die voorbereidende stappen dienen vervolgens authenticatiemiddelen volgens een uniform proces te worden “ingeschaald”.

Om de beoogde duidelijkheid te verkrijgen dient ook te worden voorzien in een heldere communicatie naar dienstaanbieders, gebruikers en issuers over de kwaliteitsaspecten en -klassen.

5.3 Anker

Een belangrijk aspect bij de uitgifte van authenticatiemiddelen is de registratie van de gebruiker waarbij de koppeling tussen het authenticatiemiddel en de identiteit plaatsvindt. De overheid kan hierin een belangrijke taak op zich nemen. Door de uitgifte van authenticatiemiddelen die zijn gebaseerd op de authentieke registers ontstaat een goede, eenduidige basis waarop private partijen de uitgifteprocessen voor hun eigen authenticatiemiddelen kunnen baseren. Met deze “standaard” kunnen private organisaties zodoende hun eigen registratie- en uitgifteprocessen standaardiseren. Dit leidt tot kostenverlaging en verhoogt, door de toegenomen eenduidigheid, het gemak voor de gebruiker.

Indien het voorgaande daarin al niet voorziet, zou de overheid overigens kunnen overwegen om in elk van de klassen van authenticatiemiddelen (zie paragraaf 5.2) te zorgen voor de uitgifte van tenminste één authenticatiemiddel. Zie echter in deze ook paragraaf 5.4.

5.4 Authenticatie Serviceprovider

Een belangrijke stap voorwaarts kan worden gedaan indien de noodzaak wordt weggenomen dat een dienstaanbieder zelf een authenticatiemiddel uitgeeft en in plaats daarvan gebruik kan maken van een authenticatiemiddel dat al door een andere organisatie is uitgegeven. Daarbij zou een dienstaanbieder eigenlijk alleen maar (moeten) hoeven aan te geven welke kwaliteit van authenticatie gewenst is. Dit kan worden bereikt door het creëren van een zogenaamde “authenticatie serviceprovider”. Voor een gedetailleerde uitleg van dit concept verwijzen we naar bijlage C.

Een dergelijke organisatie is technisch vergelijkbaar met het huidige DigiD-platform maar met de volgende verschillen:

- verzorgt authenticatie voor marktpartijen én de overheid;
- biedt in principe de mogelijkheid om alle authenticatiemiddelen uit de markt te gebruiken indien ze tot een bepaalde kwaliteitsklasse zijn toegelaten op basis van overeengekomen classificatieregels.

Dit betekent onder andere het volgende:

- een dienstaanbieder kan de authenticatie van “zijn” gebruiker laten verzorgen door die authenticatie serviceprovider en niet langer de kosten hoeft aan te gaan van het uitgeven en beheren van eigen authenticatiemiddelen. Dienstaanbieders kunnen zo “roeien met de riemen van een ander”;

- het hergebruik van authenticatiemiddelen wordt mogelijk, waardoor de issuers van dergelijke middelen kosten kunnen dekken uit het gebruik ervan door andere organisaties dan hun eigen organisatie;

- de gebruiker bepaalt zelf welk authenticatiemiddel hij wil gebruiken voor het laten verifiëren van zijn identiteit en hij hoeft slechts over een digitale sleutelbos van beperkte omvang te beschikken;[1]

- door een strikte scheiding tussen de dienstaanbieder, de issuer en de authenticatie service-provider houdt de gebruiker zelf zeggenschap over de toegang tot zijn gegevens door derden;

- de overheid kan in deze situatie beter dan momenteel voorzien in de rol van toezichthouder, bijvoorbeeld ter zake van privacy. Immers, het aantal authenticatiemiddelen en daarbij betrokken partijen zal aanzienlijk kleiner zijn dan heden ten dage;

- lastenverlichting kan worden bereikt.

Teneinde te zorgen voor een werkbare situatie vraagt de realisatie van een (of meer) authenticatie serviceprovider(s) dat zowel dienstaanbieders als issuers via gestandaardiseerde koppelvlakken met de authenticatie serviceprovider kunnen communiceren. Hierdoor worden onder meer concurrentiemogelijkheden en transparantie geborgd.

Daarnaast dienen gebruikers en dienstaanbieders voldoende vertrouwen te hebben in de authenticatie serviceprovider (onder meer vanuit privacy oogpunt) waardoor afdoend toezicht van de authenticatie serviceprovider(s) gewenst is. Het lijkt dan ook wenselijk een entiteit in het leven te roepen die dit toezicht uitoefent.

Om dit concept te realiseren kan met een kleine groep dienstaanbieders en issuers worden gestart (“coalition of the willing”) met de uitwerking en realisatie. Daarbij dient ervoor te worden gezorgd dat de invulling geen belemmering oplevert voor de doorgroei naar integraal gebruik. Als blijkt dat het concept van de authenticatie serviceprovider werkt, zullen in toenemende mate dienstaanbieders ervan gebruik gaan maken (en hun eventueel eerder uitgegeven authenticatiemiddelen intrekken) en zullen issuers van authenticatiemiddelen vragen om ook hun authenticatiemiddel te laten accepteren.

[1] Het is niet te verwachten dat het aantal authenticatiemiddelen tot één beperkt zal kunnen blijven. Immers, sommige organisaties zullen hun authenticatiemiddel willen gebruiken om hun naamsbekendheid te verhogen. Wel zal het ontstaan van een authenticatie serviceprovider organisaties ertoe brengen om de kosten van het uitgeven van een eigen authenticatiemiddel en de voordelen van de zichtbaarheid die ermee wordt bereikt, te heroverwegen.

Naast het hiervoor geschetst initiatief kan de overheid zelf een belangrijke bijdrage aan deze ontwikkeling leveren door:

- het DigiD-technisch platform ook authenticatiemiddelen te laten accepteren die niet zijn uitgegeven door de overheid. Hierdoor kan de gebruiker voor zijn communicatie met de overheid gebruikmaken van authenticatiemiddelen die hij al in zijn bezit heeft;

- het DigiD-technisch platform ook aan te bieden aan dienstaanbieders die geen overheidsorganisatie zijn.

Dit initiatief kan de Nederlandse positie rond authenticatie internationaal aanzienlijk verbeteren. Voor een concept als hiervoor geschetst is in het buitenland merkbare interesse.

6 Randvoorwaarden

In de afgelopen jaren zijn al vele pogingen ondernomen om tot oplossing van de problematiek rond authenticatie in Nederland te komen. Telkens zijn die pogingen gestrand op onder andere gebrek aan daadkracht of vertrouwen. De onderhavige verkenning is een aanzet tot een nieuwe poging. De lessen uit het verleden leren ons dat het alleen zinvol is om die poging te wagen als aan onderstaande randvoorwaarden wordt voldaan:

- er dient een duidelijk aangewezen regisseur te zijn die de zorgdraagt dat de integrale problematiek tot een oplossing wordt gebracht;
- er dient duidelijk te zijn wie de verantwoordelijkheid heeft voor realisatie van gestelde doelen;
- overheid en bedrijfsleven zullen gezamenlijk de standaarden zoals aangeduid in paragrafen 5.1 en 5.2 moeten bepalen teneinde voldoende breed draagvlak te bereiken;
- voor het realiseren van het concept van een authenticatie serviceprovider dienen er van meet af aan voldoende partijen aan de “coalition of the willing” mee te doen;
- binnen de samenwerking die worden aangegaan dienen de betrokken partijen voldoende vertrouwen in elkaar te hebben;
- er dient een goede aansluiting te zijn met internationale ontwikkelingen.

Als aan deze randvoorwaarden niet kan worden voldaan, lijkt het niet zinvol om nog langer te trachten te komen tot een wezenlijke samenwerking tussen overheid en bedrijfsleven op het vlak van authenticatie. Vanuit andere landen in Europa zullen dan uiteindelijk wel initiatieven komen waarop Nederland kan/moet aanhaken.

7 Slotwoord

Dit rapport geeft, gegeven het verkennende karakter, slechts schetsen. Het beoogt niet een volledig uitgewerkt pad naar een oplossing van de aangeduide problematiek te geven.

Tijdens onze werkzaamheden is gebleken dat alle betrokkenen ervan blijk geven de problematiek te herkennen en te erkennen. Ondanks vele initiatieven is het echter nog steeds niet gelukt om tot een structurele oplossing te komen.

De oplossingsrichting die dit rapport schetst kan een dergelijke oplossing bieden. Door als overheid en bedrijfsleven krachtig en eendrachtig de handen ineen te slaan kan Nederland veel bereiken op het vlak van authenticatie. Gebruikers (zowel burgers als organisaties) en dienstaanbieders kunnen dan met aanzienlijk meer gebruiksgemak de voordelen van elektronische communicatie plukken.

“Door de riemen te delen, kunnen we samen meer kracht zetten.”

Tot nadere toelichting zijn wij gaarne bereid.

Ir. A. van Zanten CISA
Partner
KPMG Information Risk Management

A Geïnterviewde personen

Naam	Organisatie
Dhr. G.B.J. Hartsink	ABN AMRO
Dhr. S. Luitjens en Dhr. E. Hardam	GBO.Overheid
Dhr. drs. C. Franke	Centrum voor Werk en Inkomen
Dhr. T. Masseur	Thuiswinkel.org
Dhr. dr. P.W.J. de Graaf	VNO NCW
Dhr. W.C. Westerhof en Dhr. drs. F.J.H. Visser	Rabobank
Dhr. dr. H.J.M. van Zon en Dhr. T. Meesters	Ministerie van Binnenlandse Zaken
Dhr. drs. M.J.P. Stoelinga	Vereniging van Kamers van Koophandel

B Terminologie

In de verkenning zijn diverse begrippen gebruikt. In deze bijlage bij het rapport zijn voor de belangrijkste begrippen definities vermeld. In nagenoeg alle gevallen bestaan er voor de begrippen meerdere gangbare definities. Bij de keuze van de definities voor dit rapport is zoveel mogelijk gebruikgemaakt van bronnen die worden gehanteerd door (Europese) overheden. In sommige gevallen betreft het een vertaling uit het Engels.

B.1 Context van het gebruik: Objecten

Entiteit – "Een entiteit is elke natuurlijke persoon, rechtspersoon of object (bijvoorbeeld een computer) die kan worden gekarakteriseerd door de interpretatie van zijn of haar *attributen.*[2]**"**

Identiteit – "De identiteit is het bezit van een entiteit en is de volledige maar dynamische set van alle *attributen* behorende bij een entiteit die het mogelijk maakt de ene entiteit van de andere te onderscheiden. Elke entiteit heeft maar één identiteit.[3]**"**

De identiteit bestaat uit attributen die niet noodzakelijk onderling uniek hoeven te zijn. Een combinatie van attributen is, ondanks mogelijke ambiguïteit, nuttig wanneer wordt getracht entiteiten van elkaar te onderscheiden. Hoe meer zekerheid benodigd is, des te meer en sterker onderscheidende attributen er moeten worden geëvalueerd.

Attribuut – "Een attribuut is een afzonderlijke, meetbare, fysieke of abstract benoembare eigenschap behorende bij een entiteit.[4]**"**

Een attribuut heeft een type en een waarde, het is een stukje informatie van een entiteit. Een set van attributen hoeft een entiteit niet persé te onderscheiden van de andere entiteit, het aantal attributen en het onderscheidende vermogen dragen hier wel aan bij.

Bevoegdheid (authority) – "De bevoegdheid (authority) van een identiteit reflecteert het recht om een bepaalde gedefinieerde actie uit te voeren of een gedefinieerde dienst of bron te gebruiken."

Identificatiemiddel – "Een identificatiemiddel is een set van attributen dat een entiteit gebruikt om zijn identiteit weer te geven binnen een bepaald proces."

Authenticatiemiddel – "Een authenticatiemiddel is een set van attributen, dat is aangeleverd door een entiteit, waarvan de authenticiteit door een bepaald proces wordt onderzocht."

In de context van identificatie en authenticatie worden de termen identificatiemiddel en authenticatiemiddel door veel mensen als synoniem gebruikt. Hoewel beide termen technisch gezien hetzelfde attribuut beschrijven is er een verschil in het gebruik van het middel. Een

[2] Modinis, Study on Identity Management in eGovernment (2005)
[3] Modinis, Study on Identity Management in eGovernment (2005)
[4] Modinis, Study on Identity Management in eGovernment (2005)

identificatiemiddel wordt gebruikt om een identiteit te *claimen;* een authenticatiemiddel wordt gebruikt om een geclaimde identiteit te *controleren.*

B.2 Context van het gebruik: processen

Creatie van een identiteit – "Een identiteit wordt gematerialiseerd door een set van attributen van een entiteit vast te leggen en te koppelen aan deze identiteit. De totale set van attributen vormt de identiteit."

Identificatie – "Identificatie is het gebruiken van attributen van een entiteit om af te leiden wie de entiteit is.[5]"

Authenticatie – "Authenticatie is de controle van de geclaimde identiteit van een entiteit en de set van zijn geclaimde attributen.[6]"

Binnen het authenticatieproces controleert men (een set van) attributen om met een bepaalde mate van zekerheid aan te geven of een geclaimde identiteit gelijk is aan de werkelijke identiteit van een entiteit. De controle kan bestaan uit het verifiëren van de set van waargenomen of aangeboden attributen (zoals een wachtwoord, token, biometrie, telefoonnummer, etc.).

Autoriseren – "Het verlenen van een bevoegdheid tot het verrichten van handelingen (zoals inzien, aanpassen of bewerken) op informatie of middelen.[7]"

Dit proces bestaat uit het definiëren van de bevoegdheden van een entiteit waardoor een entiteit gemachtigd wordt om een gedefinieerde actie uit te voeren of een gedefinieerde dienst of bron te gebruiken.

Interoperabiliteit – "De mogelijkheid dat verschillende (geautomatiseerde) systemen met elkaar samen kunnen werken.[8]"

In het kader van identificatie en authenticatie: "Van interoperabiliteit is sprake wanneer een dienstaanbieder buiten het technische en juridische 'veld' staat van de partij die de identiteit van een entiteit heeft vastgelegd en dat de aangeboden identiteit door vertrouwde derden bij deze partij geverifieerd kan worden."

Er is van interoperabiliteit sprake in het geval dat de volgende voorwaarden van toepassing zijn:

1 de identiteit kan worden gelezen en geïnterpreteerd door de dienstaanbieder (technische voorwaarde);

[5] Modinis, Study on Identity Management in eGovernment (2005)
[6] Modinis, Study on Identity Management in eGovernment (2005)
[7] PKIoverheid (2005)
[8] PKIoverheid (2005)

2 de dienstaanbieder geeft toestemming dat de entiteit de gevraagde activiteiten uitvoert of van de gevraagde diensten of bronnen gebruikmaakt.

B.3 Bronnen

Voor dit onderzoek is gezocht naar een algemeen geaccepteerde definities. Als bronnen zijn vooral de terminologie binnen de Nederlandse PKIoverheid en het tussenresultaat van een onderzoek voor de Europese Commissie naar “Identity Management” gebruikt, i.c.:

1 Modinis, “Study on Identity Management in eGovernment” for the European Commission, november 2005;

2 PKIoverheid, Plan van Eisen deel 4, http://www.pkioverheid.nl/uploads/media/PvE_deel4_v1_0.pdf, 2005.

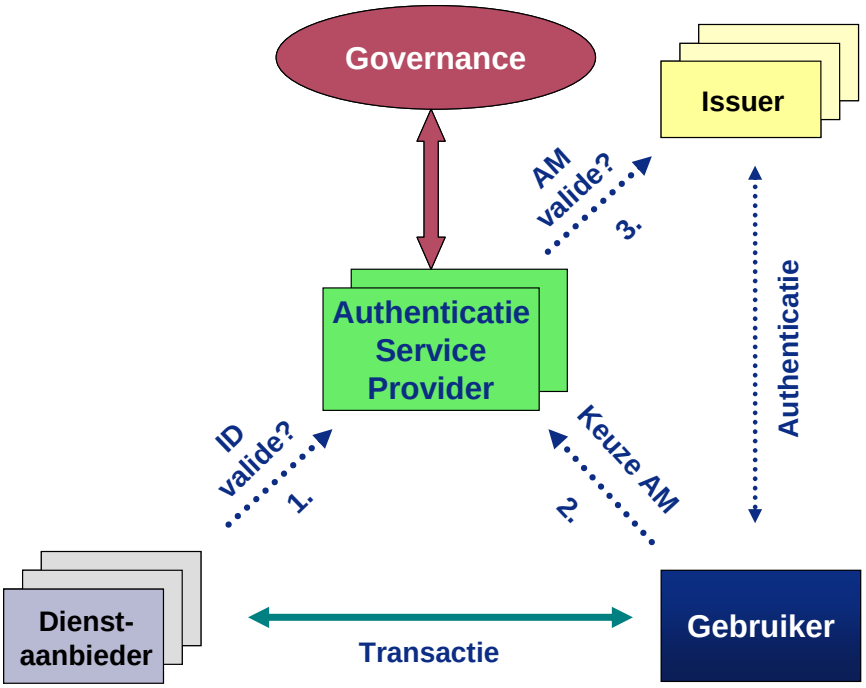
C Authenticatie Serviceprovider

Indien de noodzaak wordt weggenomen dat een dienstaanbieder zelf een authenticatiemiddel uitgeeft en in plaats daarvan gebruik kan maken van een authenticatiemiddel dat al door een andere organisatie is uitgegeven kan een belangrijke stap voorwaarts kan worden gezet in het oplossen van de problematiek rond authenticatie. Dit kan worden bereikt door het creëren van een zogenaamde “authenticatie serviceprovider”.

De authenticatie serviceprovider biedt een infrastructuur waarmee de identiteit van gebruikers gevalideerd kan worden met behulp van verschillende authenticatiemiddelen, mogelijk uitgegeven door derden. Hiermee is de authenticatie serviceprovider technisch vergelijkbaar met het DigiD-platform, maar dan ook beschikbaar voor private partijen.

C.1 Processen

Het authenticatie serviceprovider-model is weergegeven in figuur C1.



Figuur C1: Authenticatie serviceprovider-model

Naast de authenticatie serviceprovider zelf is in dit model nog een “nieuwe” partij geïntroduceerd: de issuer van authenticatiemiddelen. Deze rol werd voorheen uitgevoerd door de dienstaanbieder zelf, maar in het nieuwe model kan een issuer zowel een derde partij zijn als de dienstaanbieder zelf.

Het model werkt in grote lijnen als volgt. Als een gebruiker en een dienstaanbieder een transactie willen uitvoeren, stelt de dienstaanbieder vast of authenticatie daarbij gewenst is en, zo ja, met welke mate van zekerheid die authenticatie moet plaatsvinden. Daarna treedt het model in werking.

Stap 1 – Dienstaanbieder doet een aanvraag voor het valideren van een identiteit tegen een bepaald kwaliteitsniveau.

De dienstaanbieder legt contact met de authenticatie serviceprovider en biedt de authenticatievraag aan. Daarbij geeft de dienstaanbieder aan welke gebruiker het betreft en met welke mate van zekerheid de authenticatie moet worden uitgevoerd. Let wel, de dienstaanbieder bemoeit zich niet met het authenticatiemiddel dat daarbij moet worden gebruikt. Alleen de mate van gewenste zekerheid wordt door de dienstaanbieder bepaald.

Stap 2 – Gebruiker kiest een authenticatiemiddel om zijn identiteit te bewijzen.

De authenticatie serviceprovider neemt vervolgens contact op met de gebruiker om te vragen welk authenticatiemiddel de gebruiker wil benutten. Daarbij geeft de authenticatie serviceprovider aan welke mate van zekerheid daarbij dient te worden bereikt. De gebruiker kiest vervolgens uit de hem ter beschikking staande authenticatiemiddelen het middel dat hij bij deze transactie wil gebruiken.

Praktisch gezien zal de gebruiker overigens vooraf aan de authenticatie serviceprovider hebben gemeld over welke authenticatiemiddelen hij beschikt.

Stap 3 – Issuer valideert de identiteit op basis van het gekozen authenticatiemiddel.

In deze stap vindt de daadwerkelijke authenticatie van de gebruiker plaats. Aan de hand van keuze van de gebruiker bepaalt de authenticatie serviceprovider door welke issuer het te gebruiken authenticatiemiddel is uitgegeven. Aan die issuer richt de authenticatie service provider een verzoek om tot validatie van de identiteit van de desbetreffende gebruiker over te gaan.

De issuer neemt daartoe contact op met de gebruiker en voert de validatie uit, bijvoorbeeld door een wachtwoord aan de gebruiker te vragen of door te controleren of de gebruiker over een uitgegeven pas beschikt.

Het resultaat van die validatie koppelt de issuer terug aan de authenticatie serviceprovider, die dit op zijn beurt terugmeldt aan de dienstaanbieder. Indien dat resultaat positief is, zullen de dienstaanbieder en gebruiker hun transactie uitvoeren.

C.2 Standaardisatie

Om het uiteengezette model een succes te laten worden zijn de volgende standaardisaties noodzakelijk:

- de te onderscheiden maten van zekerheid (“kwaliteitsniveau’s”) van authenticatiemiddelen zullen moeten zijn vastgesteld;

- er dienen voor elk kwaliteitsniveau heldere criteria te zijn gedefinieerd voor het toelaten van authenticatiemiddelen tot dat kwaliteitsniveau;

- er dienen afspraken te zijn gemaakt over de manier waarop dienstaanbieder, authenticatie serviceprovider en issuer weten van welke gebruiker de identiteit moet worden gevalideerd;

- De manier waarop berichten tussen dienstaanbieder, authenticatie serviceprovider, issuer en gebruiker worden ingericht dient te zijn gestandaardiseerd om interoperabiliteit en concurrentie mogelijk te maken.

C.3 Voordelen

Dit model heeft de volgende voordelen:

- Voor de dienstaanbieder:

  - Bij het uitvoeren van hun risicoanalyse om te bepalen met welke mate van zekerheid de authenticatie moet worden uitgevoerd, kunnen dienstaanbieders gebruikmaken van de classificatie van de authenticatiemiddelen.

  - Dienstaanbieders kunnen van alle authenticatiemiddelen uit de markt gebruikmaken. Dienstaanbieders hoeven dus geen eigen authenticatiemiddelen uit te geven en kunnen dus hun diensten aanbieden zonder eerst een infrastructuur voor authenticatie op te hoeven zetten.

  - Dienstaanbieders kunnen zware investeringen op deze manier vermijden en hoeven alleen een bedrag per authenticatie te betalen aan de authenticatie serviceprovider.[9]

- Voor de gebruiker:

  - Gebruikers kunnen authenticatiemiddelen, indien ze tot een bepaalde kwaliteitsklasse zijn toegelaten, bij meerdere dienstaanbieders gebruiken, zodat hun digitale sleutelbos beperkt kan blijven.

  - De gebruiker bepaalt per transactie zelf welk authenticatiemiddel hij wil gebruiken voor het laten verifiëren van zijn identiteit bij het aangaan van een transactie met een dienstaanbieder.

[9] Dit is uiteraard afhankelijk van het commerciële betalingssysteem dat een dergelijke authenticatie serviceprovider zal inrichten.

- Door het hanteren van de classificatie van authenticatiemiddelen is het voor een gebruiker duidelijk(er) welke kwaliteit elk authenticatiemiddel heeft.

- Voor de overheid:

  - Het aantal authenticatiemiddelen neemt (wellicht op den duur) af omdat de noodzaak om “eigen” authenticatiemiddelen voor dienstaanbieders vervalt. Bovendien zijn authenticatiemiddelen ingeschaald in kwaliteitsklassen en is de kwaliteit van die middelen ook aan de gebruiker duidelijk. Hiermee wordt een belangrijke bijdrage aan de bestrijding van identiteitsfraude geleverd.

  - Door het hergebruik van authenticatiemiddelen zal de overheid zelf ook minder kosten hoeven te maken voor het uitgeven van authenticatiemiddelen. Een deel van de burgers en bedrijven zal immers gebruikmaken van authenticatiemiddelen van private partijen bij de communicatie met de overheid. Dit zorgt voor een kostenbesparing bij de overheid.

  - Daarnaast zal de Nederlandse samenleving als geheel minder kosten behoeven te maken voor het inrichten, onderhouden, beheren en gebruiken van authenticatiemiddelen, waardoor lastenverlichting wordt bereikt.

- Voor issuers:

  - Hergebruik van authenticatiemiddelen wordt mogelijk, waardoor de issuers van dergelijke middelen kosten kunnen dekken uit het gebruik ervan door andere organisaties dan hun eigen organisatie.

C.4 Kanttekeningen

Bij het model van de authenticatie serviceprovider zijn wel enkele kanttekeningen te maken.

- In het kader van deze verkenning is het niet doenlijk om dit model volledig uit te werken. Hetgeen in de voorgaande paragrafen is beschreven dient dan ook als een schets te worden beschouwd.

- De partijen in het model zullen moeten kunnen vaststellen van welke gebruiker de identiteit moet worden gevalideerd. Daarbij is het van belang een zodanige oplossing te kiezen dat de privacy van de gebruiker niet wordt geschaad. Alhoewel de authenticatie serviceprovider kan vaststellen met welke dienstaanbieder een gebruiker communiceert en van welk authenticatiemiddel de gebruiker daarbij gebruikmaakt, ontvangt de authenticatie serviceprovider geen informatie over de inhoud van de communicatie tussen gebruiker en dienstaanbieder (de “transactie”).

- Het voorgaande punt leidt er wel toe dat de authenticatie serviceprovider aan toezicht onderworpen dient te zijn. Immers, ook de wetenschap met welke dienstaanbieders een

gebruiker communiceert is gevoelig van aard. Onafhankelijk toezicht dient ervoor te zorgen dat dienstaanbieders en gebruikers voldoende vertrouwen in het model hebben en houden.

- De standaarden die nodig zijn om het model te laten werken dienen te worden opgesteld en onderhouden door een entiteit die zelf geen authenticatie serviceprovider is teneinde te voorkomen dat een machtspositie wordt afgedwongen. De toezichthouder uit het vorige punt zou hierin (en in het toezicht op het naleven van de standaarden) een belangrijke rol kunnen spelen.

- Er is geen principiële reden waarom niet meerdere authenticatie serviceproviders naast elkaar zouden kunnen bestaan. Of dit ook werkelijkheid wordt zal waarschijnlijk vooral door commerciële factoren worden bepaald. Het model leent zich er echter uitstekend voor om ook in andere landen toe te passen. In dat geval zou een netwerk van authenticatie serviceproviders kunnen zorgen voor (internationale) concurrentie en standaardisatie. Nederland kan hierin het voortouw nemen.