Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 299

BRIEF VAN DE MINISTERS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES EN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 december 2013

De Nederlandse overheid en het bedrijfsleven bieden hun diensten steeds vaker op digitale wijze aan. In het regeerakkoord is de doelstelling opgenomen dat burgers en bedrijven in 2017 digitaal zaken met de overheid moeten kunnen doen. Van belang daarbij is een veilige en betrouwbare toegang door burgers en bedrijven tot deze elektronische dienstverlening. De identiteit en bevoegdheid van burgers en bedrijven moet met een voldoende mate van zekerheid vastgesteld kunnen worden. Er is een breed gedragen gevoel van urgentie: het toenemende gebruik en de noodzaak tot voorkoming van misbruik vraagt om een elektronische identiteitsvaststelling die meer betrouwbaar en toekomstbestendig is. Nieuwe technologische en economische ontwikkelingen bieden kansen en vragen tegelijk om continue alertheid op veiligheidsrisico's. Een toekomstbestendigde betrouwbare identiteitsvaststelling is een essentiële voorwaarde.

Tot nu toe hebben publieke en private organisaties hun eigen oplossingen bedacht voor online identificatie. Deze oplossingen zijn onderling niet of beperkt uitwisselbaar en in een aantal gevallen niet meer toereikend, zoals bij transacties waarbij privacygevoelige informatie wordt uitgewisseld. Het investeren in nieuwe voorzieningen met een hoger betrouwbaarheidsniveau is kostbaar voor deze organisaties. Daarom streven we naar een stelsel met publiek en private partijen om kosten te spreiden. Bovendien moeten kwetsbaarheden en afhankelijkheden van een enkele oplossing worden voorkomen (lees: Diginotar).
De Ministeries van BZK en EZ, enkele grote uitvoeringsorganisaties en medeoverheden hebben daarom in 2012[1] een strategische verkenning uitgevoerd naar de mogelijkheden voor een publiek-privaat stelsel voor

[1] «eID Stelsel NL», *Strategische verkenning en voorstel voor vervolg,* Ministerie van BZK, oktober 2012.

kst-26643-299
ISSN 0921 - 7371
's-Gravenhage 2013

elektronische identificatie[2] (het eID Stelsel). Beoogd onderdeel van dat stelsel wordt de invoering van een publiek uitgegeven eID middel met een hoog betrouwbaarheidsniveau (DigiD-kaart). De uitgangspunten van de strategische verkenning zijn dit jaar getoetst bij een brede groep publieke en private organisaties zoals de gemeentelijke overheden, de grotere uitvoeringsorganisaties verenigd in de Manifestgroep, juridische dienstverleners (onder andere advocatuur, notariaat), leveranciers van authenticatiediensten, de thuiswinkelbranche en het bank- en verzekeringswezen. Er is draagvlak om publiek-privaat samen te werken aan de totstandkoming van het eID Stelsel met daarin de DigiD-kaart als één van de authenticatiemiddelen.

Met het eID Stelsel wordt tevens een bijdrage geleverd aan de bestrijding van cybercrime en identiteitsfraude omdat bij gebruik van middelen met een hoger betrouwbaarheidsniveau met grotere zekerheid kan worden vastgesteld dat degene die handelt ook werkelijk degene is die hij zegt te zijn. Ook moet het stelsel bijdragen aan een betere naleving van leeftijdsverificatie alvorens bepaalde diensten of producten worden verleend of verstrekt.

Met deze brief informeren wij u met name over de invoering van het eID Stelsel, de plek daarbinnen van de voorgenomen DigiD-kaart en een aantal belangrijke aspecten zoals privacy, toezicht, publiek-private samenwerking en ontwikkelingen binnen Europa.
Samen met de Minister van Economische Zaken wordt met deze brief invulling gegeven aan de toezegging om u voor het kerstreces hierover te informeren.

Huidige situatie: publiek en privaat gescheiden

In Nederland worden via verschillende sporen elektronische identificatiediensten aangeboden. Aan de overheidszijde is er onder andere voor natuurlijke personen DigiD, bedrijven kunnen gebruik maken van eHerkenning. In de private sectoren werken organisaties eveneens met diverse authenticatievoorzieningen: denk aan bankpassen en middelen om toegang te krijgen tot de dienstverlening van webwinkels.

De huidige scheidslijnen tussen de privaat en publiek georganiseerde vertrouwensdienstverlening leveren een aantal onwenselijkheden en risico's op. Zo zijn er onnodige administratieve lasten voor burgers en bedrijven. Voor het verkrijgen van toegang tot publieke elektronische diensten, moeten burgers en bedrijven andere authenticatiemiddelen gebruiken dan voor de toegang tot private elektronische diensten. Een risico is dat bij uitval van een voorziening niet overgeschakeld kan worden naar een back-up. Hierdoor kan de continuïteit van de dienstverlening niet in alle gevallen gegarandeerd worden.

Publieke en private organisaties geven in het kader van fraudepreventie en privacy-bescherming aan bij bepaalde transacties pas verder te willen digitaliseren als mensen en organisaties op een hoger betrouwbaarheidsniveau digitaal kunnen aantonen dat ze daadwerkelijk zijn wie ze zeggen te zijn. Private organisaties lopen zo minder risico op niet-inbare facturen en oplopende betalingstermijnen die voor extra kosten zorgen. Overheidsorganisaties kunnen de effecten van identiteitsfraude bij het innen van heffingen of het uitkeren van subsidies en andere financiële tegemoetkomingen beperken. Ook is er behoefte aan voorzieningen voor betere

[2] In deze brief wordt gesproken over identificatie en authenticatie. Bij identificatie geeft iemand aan wie hij/zij is, bij authenticatie wordt vastgesteld of deze persoon ook daadwerkelijk is wie die zegt dat die is.

naleving van wettelijke leeftijdseisen die aan (online) levering van bepaalde producten en diensten zijn verbonden[3].

Het eID Stelsel

Het eID Stelsel is een publiek privaat stelsel, waarbinnen burgers, consumenten en ondernemers zowel publieke als private authenticatie-middelen gebruiken, waarmee ze veilig online zaken kunnen doen met de overheid en het bedrijfsleven.
Het eID Stelsel ondersteunt de volgende functionaliteiten:

1. Vaststellen van de identiteit van een partij (authenticatie);
2. Bewijzen dat je bevoegd bent om bepaalde diensten en producten af te nemen (autorisatie);
3. Verrichten van (rechts)handelingen namens anderen (op basis van machtiging of wettelijke vertegenwoordiging);
4. Bevestigen van een wilsuiting of instemmen met de inhoud van een transactie (ondertekenen).

Binnen het eID Stelsel worden diverse bestaande en nieuwe, publieke en private middelen met verschillende betrouwbaarheidsniveaus voor online identificatie ondergebracht. Dit wordt een multi-middelenstrategie genoemd. Het stelsel biedt de gebruiker de gelegenheid om de omvang van zijn of haar digitale sleutelbos (eID middelen) zelf te bepalen als mede keuzevrijheid bij het gebruik van het middel. Tegelijkertijd worden de elektronische dienstaanbieders door het stelsel ontzorgd omdat het stelsel zorgdraagt voor authenticatie van het middel, en vaststelt of de gebruiker bevoegd is namens een ander te handelen (op basis van een machtiging of wettelijke vertegenwoordiging). Ook wordt hiermee een terugvaloptie gecreëerd: bij uitval van één middel kan de gebruiker overstappen op gebruik van een ander middel.
In de bijlage is de opzet van het eID Stelsel nader uitgewerkt. Het eID Stelsel bouwt voort op het Afsprakenstelsel eHerkenning. eHerkenning migreert in 2014 naar het eID Stelsel. Dienstverleners kunnen blijven aansluiten op eHerkenning. Aansluiten op eHerkenning blijft dus toekomstvast.

Publiek-privaat kader

Een belangrijk uitgangspunt van het stelsel, is dat binnen het stelsel zowel publieke als private middelen opgenomen kunnen worden.
De overweging hierbij is of een publieke invulling van een dienst noodzakelijk is en het algemeen belang dient. Uitgangspunt voor voorzieningen in het stelsel is «privaat waar het kan, publiek waar het moet». In de bijlage is dit concreet uitgewerkt.

Waarborging privacy

De zorgvuldige omgang met persoons- en organisatiegebonden gegevens is van essentieel belang voor het vertrouwen van mensen en organisaties in het stelsel en de beschikbare eID middelen daarbinnen. Ieder ontwerp moet rekening houden met de mogelijkheid van een misbruik- of beveiligingsincident, en moet tevens de impact van een dergelijk incident zo veel mogelijk beperken. Dataminimalisatie en zelfbeschikking zijn hierbij belangrijke uitgangspunten. Degenen die betrokken zijn bij de afhandeling van een online transactie krijgen alleen toegang tot die

[3] Beantwoording Kamervragen omtrent:
1. Naleving leeftijdsgrenzen bij verkoop van leeftijdsgebonden producten d.d. 22 augustus 2012.
2. Bericht dat online alcoholhoudende drank kopen kinderspel is d.d. 15 juli 2013.

informatie die strikt noodzakelijk is voor het uitvoeren van hun taak. De gebruiker geeft vooraf toestemming voor de uitwisseling van informatie (tenzij op grond van wettelijke bepalingen toestemming niet aan de orde is).

Op het stelsel wordt een privacy-impactanalyse uitgevoerd om de privacy-risico's volledig in kaart te brengen en de maatregelen zo uit te werken dat deze afdoende zijn.

Toezichtfunctie

Een gedragen normenkader en adequaat toezicht moeten een robuust stelsel borgen en moeten falen tijdig detecteren, zodat snel maatregelen getroffen kunnen worden. De organisaties die willen toetreden tot het eID Stelsel en dienstaanbieders, ondergaan een audit bij toetreding, die daarna periodiek wordt herhaald. Het toezicht op (de deelnemers in) het stelsel en de daarvoor aan te wijzen toezichthouder zullen wettelijk verankerd worden. Bij de inrichting van het toezicht wordt rekening gehouden met de aard van de deelnemende organisaties binnen het stelsel en zal gebruik gemaakt worden van ervaringen met bestaande toezichtarrangementen op dit terrein, zoals in het kader van eHerkenning, PKIoverheid en op grond van de Telecommunicatiewet (certificaat-diensten).

Het voornemen van het kabinet is om in 2015 een werkend eID Stelsel te hebben inclusief een governancemodel.

De DigiD-kaart

Het kabinet is uitdrukkelijk van mening dat er voluit ruimte moet zijn voor inzet van private eID-voorzieningen, ook voor natuurlijke personen. Dat is zeer gewenst in het kader van de beschreven multi-middelenstrategie. In de lopende oriënterende besprekingen met private partijen wordt hierop dan ook ingezet. De huidige marktmiddelen bieden wel al oplossingen, maar zijn op dit moment nog niet breed uitgerold. Er kan niet gegarandeerd worden dat er tijdig (uiterlijk eind 2017) voldoende private middelen op een hoog beveiligingsniveau (in Europese termen: STORK[4] 4 niveau) voor burgers beschikbaar zullen zijn.
Tevens acht het kabinet het gewenst – in lijn met het WRR-advies[5] – dat burgers de mogelijkheid hebben om een publiek middel aan te schaffen – een DigiD-kaart – waarmee ze zaken kunnen doen met de overheid.
Om deze redenen onderzoekt het kabinet de mogelijkheden voor een publiek middel, zijnde de DigiD-kaart. Europese aanbestedingsregels worden hierbij in acht genomen, evenals de regels die gelden voor zover de overheid met het aanbieden van de kaart een economische activiteit verricht. Op dit moment wordt de precieze vormgeving van deze kaart, inclusief de benodigde financiële middelen uitgewerkt. Zodra daar helderheid over is, wordt de Kamer nader geïnformeerd.

---

[4] STORK is een Europees raamwerk voor het vaststellen van de betrouwbaarheid van elektronische authenticatie van personen, oplopend van niveau 1 (laag) tot 4 (hoog). Zie: Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, Een handreiking voor overheidsorganisaties», Forum Standaardisatie. Link: http://www.logius.nl/fileadmin/logius/product/Samenwerkende_Catalogi/HR_Betrouwbaarheidsniveaus_WEB.pdf.

[5] WRR-Webpublicatie NR. 47 «Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit» d.d. 2010-11-22.

Ontwikkelingen in Europa

Momenteel wordt een concept Verordening elektronische identiteiten en vertrouwensdiensten[6] besproken tussen de lidstaten van de Europese Unie. Deze verordening gaat onder andere de wederzijdse erkenning van identificatiemiddelen tussen de lidstaten regelen. Hierdoor wordt grensoverschrijdende elektronische overheidsdienstverlening aan burgers en ondernemers vergemakkelijkt.
De verordening betekent dat Nederland middelen uit andere lidstaten, die vergelijkbaar zijn met de DigiD-kaart, moet kunnen accepteren. Omgekeerd moeten andere lidstaten middelen uit het Nederlandse eID Stelsel accepteren als burgers of ondernemers digitale diensten in die lidstaten willen afnemen. Bij de ontwikkeling van het eID Stelsel wordt rekening gehouden met de verwachte eisen die gesteld worden op grond van de Europese Verordening.

Ten slotte

Voor de totstandkoming van het eID Stelsel en de uitwerking van de DigiD-kaart is het programma eID ingericht, onder aansturing vanuit een stuurgroep waarin diverse departementen zijn vertegenwoordigd. Het programma werkt nauw samen met de VNG en NVVB. Gedurende de looptijd van het programma is er een tijdelijke governance voor het eID Stelsel waarin publieke en private partijen deelnemen. Na afloop van het programma komt er een definitieve governance voor het eID Stelsel waarin de publiek-private samenwerking op langere termijn wordt geborgd. De definitieve besluitvorming over de inrichting van het eID Stelsel en de introductie van de DigiD-kaart kan pas plaatsvinden als de hiermee samenhangende uitgaven en ontvangsten volledig in kaart zijn gebracht en alle uitgaven zijn gedekt. De Tweede Kamer zal hier op een later tijdstip nader over geïnformeerd worden.
De Ministers van BZK en EZ dragen gezamenlijk de verantwoordelijkheid voor het eID Stelsel; de Minister van BZK is specifiek verantwoordelijk voor de DigiD-kaart.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk

De Minister van Economische Zaken,
H.G.J. Kamp

[6] Kamerstuk 22 112, FL.

Bijlage:

Opzet eID Stelsel

Om uitwisselbaarheid te borgen worden binnen het stelsel standaarden gedefinieerd, eisen en normen vastgelegd zoals beveiligingsniveaus en worden de voorwaarden afgesproken waaronder partijen mogen deelnemen. Hierdoor wordt het volgende mogelijk:

1. Er komt één eID Stelsel voor authenticatie- en bevoegdheidsdiensten, te gebruiken bij elektronische transacties door natuurlijke en niet-natuurlijke personen waardoor:
   a. Dezelfde standaarden gelden voor het burger- en bedrijvendomein;
   b. Verschillende typen gebruikers bediend worden, ook de minder en niet digitaal vaardigen;
   c. De privacy van mensen en organisaties gewaarborgd blijft;
   d. Waar mogelijk gebruik gemaakt wordt van bestaande en bewezen oplossingen en open standaarden;
   e. Een toekomstvaste en robuuste open publiek-private infrastructuur voor authenticatie- en bevoegdheidsdiensten ontstaat waarbij binnenlandse en buitenlandse organisaties vrijwillig kunnen toetreden en
   f. Private en publieke organisaties niet individueel toegangsvoorzieningen in stand hoeven te houden, maar gebruik kunnen maken van gestandaardiseerde oplossingen binnen het stelsel.
2. Het eID Stelsel beschrijft de werking van de volgende elektronische vertrouwensdiensten: authenticatie, het vaststellen van bevoegdheden om voor een ander te handelen (machtiging en wettelijke vertegenwoordiging), het leveren van attributen (zoals beroepsbevoegdheid of voldoen aan een leeftijdsgrens), en ondertekenen.
3. Binnen het stelsel wordt gewerkt met een beperkt aantal betrouwbaarheidsniveaus conform het STORK-raamwerk[7] waaraan elektronische identificatie voor een bepaalde dienst moet voldoen.
4. De organisatie die digitaal toegang wil verlenen tot haar dienstverlening classificeert de dienst op een bepaald betrouwbaarheidsniveau.
5. De gebruiker van de dienst kan vervolgens de keuze maken met welk eID middel hij zijn identiteit op het gevraagde betrouwbaarheidsniveau aantoont. Hiertoe kan hij de beschikking hebben over een publiek of een privaat authenticatiemiddel dat in het stelsel is ondergebracht. Voor bedrijfsgebonden authenticatiemiddelen van rechtspersonen zijn er alleen private middelen beschikbaar.
6. De middelen onder het stelsel zijn bruikbaar voor de toegang tot zowel publieke als private elektronische diensten.
7. In de toekomst kunnen de in het stelsel ondergebrachte middelen ook in het buitenland gebruikt worden.
8. De Ministers van BZK en EZ zijn systeemverantwoordelijk voor het afsprakenstelsel. Dit houdt in dat de Ministers:
   a. Eindverantwoordelijkheid dragen voor het eID Stelsel en (nieuwe) versies van stelselafspraken goedkeuren.
   b. Toezicht uitoefenen op (delen van) het afsprakenstelsel en de deelnemers.

Publiek-privaat kader

Een belangrijk uitgangspunt van het stelsel, is dat binnen het stelsel zowel publieke als private middelen opgenomen kunnen worden.

---

[7] STORK is een Europees raamwerk voor het vaststellen van de betrouwbaarheid van elektronische authenticatie van personen, oplopend van niveau 1 (laag) tot 4 (hoog). Zie: Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, Een handreiking voor overheidsorganisaties», Forum Standaardisatie. Link: http://www.logius.nl/fileadmin/logius/product/Samenwerkende_Catalogi/HR_Betrouwbaarheidsniveaus_WEB.pdf.

De overweging hierbij is of een publieke invulling van een dienst noodzakelijk is en het algemeen belang dient. Uitgangspunt voor voorzieningen in het stelsel is «privaat waar het kan, publiek waar het moet». Of er een noodzaak is voor het aanbieden van een publieke voorziening, is onderzocht voor de volgende voorzieningen in het eID Stelsel:

• Authenticatiemiddel (sleutel)
De sleutel is het middel waarmee de persoon inlogt bij een digitale dienst. Het authenticatiemiddel kan voor natuurlijke personen zowel publiek als privaat worden aangeboden, voor alle STORK betrouwbaarheidsniveaus[8]. De authenticatie van (medewerkers van) rechtspersonen wordt uitsluitend privaat aangeboden, zoals nu al het geval is binnen eHerkenning.

• eID Makelaar (ontzorgt een dienstaanbieder)
Via de makelaar is het mogelijk in te loggen bij een publieke of private organisatie (het «slot»). Een eID Makelaar verzamelt alle informatie (wie de persoon is, wat de persoon mag en dergelijke) voor een dienstaanbieder om een persoon toegang te kunnen verlenen. Deze functie wordt privaat uitgevoerd.

• Machtigingenregister
Hierin wordt op een betrouwbare wijze geregistreerd dat een persoon een andere persoon heeft gemachtigd namens hem/haar diensten af te nemen bij een dienstverlener. Het machtigingenregister voor natuurlijke personen kan zowel publiek als privaat worden aangeboden. Het machtigingenregister voor rechtspersonen wordt – mits aan bepaalde voorwaarden wordt voldaan – uitsluitend privaat aangeboden.

• Burgerservicenummer en koppelregister
Een eID-middel in het kader van het stelsel bevat een uniek identificerend pseudoniem. Bij gebruik van een publiek eID-middel (zoals de DigiD-kaart) in het private domein wordt geen BSN uitgewisseld, maar een pseudoniem dat per dienstaanbieder uniek is. Bij gebruik van de DigiD-kaart of een privaat eID-middel (bijvoorbeeld een bankpas) in het publieke domein wordt het pseudoniem vertaald in een BSN. Dit wordt in een door de overheid beheerd koppelregister bij gehouden, zoals nu ook in het huidige DigiD.
In dit register worden ook private authenticatiemiddelen gekoppeld aan het BSN. Vanwege de verwerking van het BSN is het in stand houden van deze voorziening een exclusieve publieke taak.

[8] Er zijn 4 betrouwbaarheidsniveaus binnen STORK.