Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

# 26 643 Informatie- en communicatietechnologie (ICT)

**Nr. 371**

## BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 november 2015

In de brief van 30 juni[1] heb ik u geïnformeerd over de stand van zaken rond Idensys (voorheen eID Stelsel).[2] Naar aanleiding van mijn toezegging informeer ik u, mede namens de Minister van Economische Zaken, over de uitwerking van de pilotcriteria.

### Inleiding

In het Regeerakkoord is de doelstelling opgenomen dat burgers en bedrijven in 2017 digitaal zaken met de overheid moeten kunnen doen. In dit kader wordt Idensys ontwikkeld als standaard voor online toegang tot dienstverlening van overheid en bedrijven. De standaard bestaat uit afspraken en voorzieningen. Zowel publieke als private authenticatiemiddelen kunnen deel uitmaken van Idensys. Hiermee wordt uitvoering gegeven aan de gewenste multimiddelenstrategie én wordt het risico op een *single point of failure* gereduceerd. Om de standaard te kunnen beproeven zullen er pilots worden uitgevoerd.

### Pilots met Idensys en het publieke authenticatiemiddel

Zoals eerder aan uw Kamer gemeld[3] worden twee typen pilots voorbereid: pilots met private authenticatiemiddelen binnen Idensys en pilots met publieke authenticatiemiddelen. Hieronder licht ik beide pilots nader toe. Een pilot ter versterking van DigiD en een pilot met het bankenmiddel zal ik aan het einde van deze brief nader toelichten.

---

[1] Tweede Kamerbrief Pilotvoorwaarden en pilotcriteria eID Stelsel, Kamerstuk 26 643 nr. 363.
[2] Sinds de Kamerbrief van 30 juni 2015, wordt het eID Stelsel aangeduid met Idensys, klik hier voor de Kamerbrief.
[3] Brief Voortgang eID van 9 februari 2015 Kamerstuk 26 643, nr. 349.

kst-26643-371
ISSN 0921 - 7371
's-Gravenhage 2015

### 1. Pilots met private authenticatiemiddelen (Idensys-pilots)

In deze pilots wordt het gebruik van private middelen binnen Idensys getest. Een groep gebruikers krijgt tijdens deze pilots toegang tot enkele digitale diensten van publieke dienstaanbieders. Verschillende middelenleveranciers hebben zich aangemeld om toe te treden tot Idensys en meer dan 15 overheidsdienstverleners (onder andere de Belastingdienst, SVB, zorgaanbieders, zorgverzekeraars en vijf gemeenten) hebben zich aangemeld voor pilots. Deze pilots maken onder strikte voorwaarden gebruik van het BSN-koppelregister.[4] De pilots zullen starten in december 2015.

### 2. Pilots met publieke authenticatiemiddelen

In deze pilots wordt getest of wettelijke identiteitsdocumenten geschikt zijn om als authenticatiemiddel te functioneren zodat deze middelen op termijn kunnen gaan voldoen aan de eisen van Idensys. Er worden pilots uitgevoerd waarbij aan het identiteitsdocument een «applet» (klein stukje software) voor authenticatie wordt toegevoegd. De gemeente Den Haag voert een pilot uit met de Nederlandse Identiteitskaart en de gemeente Eindhoven met een specimen van het rijbewijs. Deze pilots zullen gefaseerd starten vanaf december 2015 en doorlopen tot juli 2016. Op 22 september 2015 is het convenant voor de samenwerking in de pilot met de gemeente Den Haag getekend. Een belangrijk verschil met de pilots met de private middelen in Idensys is dat de pilots met publieke authenticatiemiddelen gebruik maken van de systemen van DigiD.

*Voorwaarden voor deelname aan Idensys*

Voor pilotdeelnemers gelden voorwaarden waaraan voldaan dient te worden bij aanvang van de Idensys-pilots. Zo moeten private partijen die middelen willen uitgeven onder het merk Idensys voldoen aan technische, organisatorische en juridische eisen die zijn vastgelegd in het Afsprakenstelsel Elektronische Toegangdiensten.[5]
De Minister van EZ is verantwoordelijk voor het toezicht op het Afsprakenstelsel Elektronische Toegangsdiensten. Hij laat toetsen of alle deelnemende partijen voldoen aan de afspraken.

## *Evaluatie van de pilots met Idensys en de pilots met publieke authenticatiemiddelen*

### 1. Evaluatiecommissie

Conform de toezegging in mijn brief van juni[6] richt ik een evaluatiecommissie in, die de uitvoering van het evaluatieonderzoek voor de pilots bij overheidsdienstverleners met private authenticatiemiddelen en de pilots publieke authenticatiemiddelen begeleidt.
De evaluatiecommissie brengt een advies uit aan de Ministers van BZK en EZ over waardering van de pilots, waarna het kabinet medio 2016 een standpunt over de uitrol van Idensys en de publieke authenticatiemiddelen zal voorbereiden. Het evaluatieonderzoek wordt uitgevoerd door externe onderzoeksbureaus. In het onderzoek wordt in ieder geval ingegaan op:

---

[4] Deze voorziening legt bij uitgifte van een privaat authenticatiemiddel de koppeling tussen dat middel en het burgerservicenummer van de gebruiker.
[5] Dit afsprakenstelsel wordt formeel aangeduid als Afsprakenstelsel Elektronische Toegangsdiensten. Zie ook de brief aan de Tweede Kamer van 30 juni 2014, waarnaar wordt verwezen in voetnoot 3.
[6] Kamerstuk 26 643, nr. 363.

- Feitelijk gebruik van het middel in de pilots;
- Technische werking van Idensys en het publiek authenticatiemiddel;
- Privacy en beveiliging van Idensys en het publiek authenticatiemiddel;
- Ervaringen van burgers, dienstaanbieders en leveranciers.

De evaluatiecommissie begeleidt de onderzoeksbureaus bij het uitvoeren van de onderzoeken. De evaluatiecommissie zal onder het voorzitterschap staan van drs. P.W.A. Veld. Het instellingsbesluit met de samenstelling van de commissie wordt gepubliceerd in de Staatscourant.
Bij de samenstelling van de commissie zijn de relevante invalshoeken, te weten gebruikersperspectief, dienstverlening, privacybescherming en techniek in acht genomen. De commissie zal medio november 2015 worden ingesteld en wordt na afronding van de werkzaamheden (naar verwachting: medio 2016) opgeheven.

**2. Evaluatie onderzoeken**

De evaluatieonderzoeken worden uitgevoerd door onafhankelijke onderzoeksbureaus. Zij maken gebruik van de volgende bronnen:
- Desk research, waarbij zij de volgende rapporten gebruiken: auditrapportages van toezicht, rapportages van dienstaanbieders, Service Level Agreement rapportages en rapportages over het gebruik van het publieke middel.
- Kwantitatief onderzoek, waarbij zowel feitelijke gegevens over bijvoorbeeld het gebruik, als subjectieve informatie als ervaringen en meningen van burgers en dienstverleners worden verzameld.
- Kwalitatief onderzoek, waarbij met interviews en focusgroepen de ervaringen en opvattingen van de betrokkenen in kaart worden gebracht.

De evaluatieonderzoeken worden uitgevoerd aan de hand van vooraf geformuleerde onderzoeksvragen. De onderzoeksrapportages geven naar verwachting een representatief beeld van de pilots, op basis waarvan het kabinet een afweging kan maken en een standpunt kan voorbereiden.

Om de pilot(resultaten) te kunnen beoordelen wordt gebruik gemaakt van evaluatiecriteria. Deze geven de meetlat aan, waartegen de uitkomsten van de verschillende onderzoeken worden afgezet om te komen tot een gefundeerd advies.

***Evaluatiecriteria***

De onderstaande evaluatiecriteria gelden voor de Idensys-pilots en de pilots met publieke authenticatiemiddelen.

**1. Betrouwbaarheid en veiligheid**

Er wordt gekeken naar:
- Incidenten die hebben plaatsgevonden;
- Hebben de procedures in geval van incidenten naar behoren gewerkt;
- Welke aanvullende technische en procedurele maatregelen kunnen worden getroffen;
- Is het toezicht op de veiligheid en betrouwbaarheid effectief uitgevoerd. Welke aanpassingen zijn wenselijk en/of nodig?

Bij de uitvoering van de pilots wordt met een hoog betrouwbaarheidsniveau gewerkt. Alle authenticatiemiddelen hebben een hoger betrouwbaarheidsniveau van identiteitsvaststelling dan thans met DigiD beschikbaar is.
De uitvoering van de pilots voldoet aan de eisen die gesteld zijn ten aanzien van veiligheid en betrouwbaarheid. Het gaat om eisen die gesteld

zijn en voortkomen uit het afsprakenstelsel (Idensys-pilots) en het gaat om eisen ten aanzien van het vier-ogenprincipe en logging van mutaties.

**2. Privacy**

Voor de pilots zijn Privacy Impact Analyses (PIA) uitgevoerd, waarbij getoetst is aan feitelijke en technische nationale en Europese juridische vereisten betreffende privacy.[7]

Uit de PIA op het introductieplateau van Idensys is gebleken dat de privacymaatregelen voor de pilotfase adequaat zijn, maar dat voor een eventuele structurele fase mitigerende maatregelen noodzakelijk zijn.[8]

Parallel aan de pilots is daarom gestart met de uitwerking van de gewenste aanvullende privacy maatregelen die voor een eventuele brede uitrol van Idensys noodzakelijk zijn. De ervaringen uit de pilots worden hierbij meegenomen. Pas als Idensys met akkoord van uw Kamer breder kan worden uitgerold, wordt geïnvesteerd in de aanvullende privacy maatregelen die nodig zijn bij grootschalig gebruik. Deze stapsgewijze aanpak is in lijn met het advies van de Commissie Elias.

Er is ook een PIA uitgevoerd voor de pilot met het publieke authenticatiemiddel. De PIA geeft aan dat er technische en procedurele maatregelen zijn getroffen om de privacy van burgers te borgen. Daar waar aandachtspunten naar voren kwamen, zijn mitigerende maatregelen toegepast.

**3. Gebruikersvriendelijkheid en toegankelijkheid:**

Er wordt gekeken naar:
- In welke mate de gebruikers om kunnen gaan met de aangeboden authenticatiemiddelen;
- In welke mate de inlogprocedures helder en begrijpelijk zijn voor de gebruikers;
- In welke mate de gebruikers door willen gaan met de digitale dienstverlening met gebruik van deze inlogprocedures, ook voor andere diensten.

Zowel het uitgifteproces, het inloggen en ondersteuning bij en het oplossen van eventuele problemen die gebruikers ervaren worden beoordeeld op gebruikersvriendelijkheid en toegankelijkheid.

Daarnaast worden ook de ervaringen bij dienstaanbieders en leveranciers van authenticatiemiddelen beoordeeld: is de wijze van aansluiting voor hen bruikbaar? Willen de dienstverleners ook hun andere diensten op deze manier ontsluiten?
En willen de leveranciers van de authenticatiediensten verder gaan met deze dienstverlening?

**Advies over de organisatie van de pilots**

In de aanloop naar de pilots heb ik kritisch laten kijken naar de manier waarop de pilots georganiseerd zijn. De planning is aangescherpt. De governance is passend gemaakt. Ook is er meer samenhang tussen de pilots aangebracht. Daarnaast is, conform de rijksbrede afspraken, rekening gehouden met de aanbevelingen van de CIO BZK.

---

[7] Een privacy Impact Assessment (PIA) is een hulpmiddel bij de ontwikkeling van beleid, wetgeving en bouw van IT-systemen. Hiermee kunnen privacyrisico's op een gestructureerde en heldere wijze in kaart worden gebracht.

[8] In de bijlage bij deze brief vindt u de privacymaatregelen die voor de pilotfase zijn genomen.

## Overige Pilots

Naast de pilots met Idensys en pilots met de publieke authenticatiemiddelen vinden er pilots plaats ter versterking van DigiD en is er een pilot met het bankenmiddel. Deze twee pilots dragen bij aan de verdere digitalisering van de overheid. Deze pilots zullen apart worden geëvalueerd omdat merendeels andere partijen betrokken zijn. Hierbij zullen zoveel mogelijk dezelfde criteria worden gehanteerd. Uiteraard kan het zijn dat de specifieke onderzoeksvragen anders zijn vanwege de andere invulling van de pilots.

*Pilots ter versterking van DigiD*

In het kader van de versterkingsagenda DigiD[9] wordt een pilot uitgevoerd door enkele grote uitvoeringsorganisaties met het toepassen van een extra controle na het inloggen met DigiD. Die extra controle vindt plaats door het uitlezen van gegevens op de al aanwezige chip van een wettelijk identiteitsdocument, zoals de Nederlandse identiteitskaart en het rijbewijs. Daarmee wordt het mogelijk authenticaties met een hoog betrouwbaarheidsniveau uit te voeren. Deze toepassing dient ter versterking van het huidige DigiD en wordt daarom in die context geëvalueerd.

*Pilot met het bankenmiddel*

In het kader van elektronische dienstverlening wordt verkend of het mogelijk is om via de banken toegang te krijgen tot publieke dienstverlening. Er zal daarom aan het einde van het jaar gestart worden met een pilot bij de Belastingdienst. Aangezien banken zowel internationaal als nationaal aan andere regels zijn gebonden en een bestaande elektronische infrastructuur hebben, kunnen zij nog niet aansluiten op Idensys.

*Samenhang*

Idensys staat centraal, we werken naar één Stelsel, waarbij zowel de publieke als de private authenticatiemiddelen aan dezelfde eisen gaan voldoen van veiligheid en betrouwbaarheid, DigiD migreert en met de banken wordt bezien hoe één samenhangend stelsel kan ontstaan met Idensys en de bankmiddelen samen. Dit laatste binnen de ruimte die banken en hun toezichthouder hebben en de mogelijkheden die Idensys biedt.

## Tot slot: Hoe nu verder?

U hebt voor het Algemeen Overleg van 25 november aanstaande mijn eerdergenoemde brief van 30 juni 2015 geagendeerd. In de onderhavige brief heb ik de opzet, de voorwaarden en de criteria voor de evaluatie verder geconcretiseerd.

Voordat er sprake zal zijn van een grootschalige uitrol, zullen de benodigde waarborgen die een structurele inproductiename vraagt, zoals privacy by design, fraudebestrijding, beveiliging en extra benodigde functionaliteiten worden uitgewerkt, zodat een robuust afsprakenstelsel verzekerd is. Over de contouren hiervan zal ik u medio 2016 inlichten, zodat u deze bij uw afweging kunt betrekken.

[9] Kamerbrief Kosten Versterking DigiD en voortgang oplossen onvolkomenheden Beveiligingsnorm DigiD van 24 februari 2015 (Kamerstuk 26 643, nr. 352).

Als uw Kamer er prijs op stelt, kan voorafgaand aan het Algemeen Overleg van 25 november 2015 een technische briefing worden georganiseerd.

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

**BIJLAGE I:** **privacymaatregelen**

Privacy is een van de belangrijkste elementen bij de authenticatie van burgers. Daarom geef ik u bij deze nader inzicht in de maatregelen die binnen Idensys worden genomen om de privacy te borgen.

In de versie van Idensys gedurende de pilotperiode is een aantal privacy maatregelen opgenomen. Hieronder zal worden aangegeven welke dat zijn.
De privacy maatregelen zijn deels al opgenomen in het voorgestelde afsprakenstelsel. Op de voorgestelde versie is een Privacy Impact Analyse (PIA) uitgevoerd door Mazars. Dat heeft geleid tot aanvullende maatregelen die deels in de versie van Idensys tijdens de pilots worden meegenomen en deels behelst het maatregelen die na de pilots opgepakt moeten worden.
Hieronder wordt eerst ingegaan op de belangrijkste privacy maatregelen in Idensys tijdens de pilotperiode en daarna worden de maatregelen benoemd die uit de PIA zijn gekomen voor de eventuele fase erna.

**Privacy in Idensys tijdens de pilotperiode**

Privacy in Idensys valt uiteen in vier onderdelen:

1. Privacy beleid
2. Privacy-analyse(PIA)
3. Privacy maatregelen
4. Controle bij toetreding en op de naleving

Controle op de naleving vindt periodiek plaats en bij iedere fundamentele wijziging van het afsprakenstelsel wordt er opnieuw een PIA uitgevoerd als onderdeel van de stelselrisicoanalyse.

Privacy beleid

Standaard onderdeel van het afsprakenstelsel is het hebben van privacy beleid door de deelnemers. Doel van het privacy beleid is een eenduidige implementatie en controle van de naleving van de privacy wet- en regelgeving. Dit beleid is kaderstellend voor het Afsprakenstelsel. Voor het Introductieplateau is er een PIA gedaan door Mazars.
Specifiek voor het Introductieplateau worden in Idensys op verschillende onderdelen van het afsprakenstelsel privacy maatregelen opgenomen:
- Juridisch Kader (opnemen verplichting tot naleving van het privacybeleid),
- Het Informatiebeveiligingsbeleid (opnemen/verwijzing naar het privacybeleid),
- De Stelselrisicoanalyse (opnemen overzicht van geïdentificeerde privacy risico's uit de PIA),
- Het Gemeenschappelijk Normenkader (opnemen/verwijzing naar het privacybeleid),
- Het Normenkader Betrouwbaarheidsniveaus,
- Het Stelselnormenkader.

Privacy maatregelen

- Een unieke identiteit per organisatie
- Vooraf toestemming vragen en geven bij verstrekken van informatie
- Geen meekijkers onderweg (versleuteling)
- Persoonsgegevens worden zo kort mogelijk bewaard
- Gebruiker heeft recht op inzage
- Een BSN wordt enkel verstrekt indien nodig en toegestaan

- Dienstaanbieders sluiten aan onder voorwaarden
- Chinese muur tussen dienstverlening pilots Idensys en business as usual
- Ook de privacy maatregelen vallen onder het toezicht van de toezichthouder.