Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten: elektronische identificatie

J.J. Linnemann[1]

1. Inleiding

Twee jaar geleden, op 17 september 2014, trad Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG in werking.[2] Deze verordening beoogt het vertrouwen in elektronische transacties te vergroten en wordt ook wel aangeduid als de eidasverordening (hierna: de Verordening).[3] De Verordening voorziet in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden. Daarnaast ziet de Verordening op het verhogen van de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne en Europese markt.[4]

De Verordening regelt twee hoofdonderwerpen. Allereerst verplicht de Verordening openbare instanties in een lidstaat onder voorwaarden een elektronisch identificatiemiddel te erkennen dat is uitgegeven in een andere lidstaat. Concreet houdt dit in dat burgers zich in een andere lidstaat moeten kunnen identificeren met een elektronisch identificatiemiddel dat in hun eigen lidstaat is uitgegeven en vice versa. Deze wederzijdse verplichting geldt vanaf 29 september 2018.[5]

Daarnaast reguleert de Verordening zogenaamde vertrouwensdiensten. Onder vertrouwensdiensten verstaat de Verordening diensten met betrekking tot elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en diensten voor websitecertificaten. Voor dergelijke diensten voorziet de Verordening in een wetgevingskader. Deze bepalingen zijn sinds 1 juli 2016 van toepassing.[6] Op diezelfde dag werd Richtlijn 1999/93/EG ingetrokken. In een eerder artikel is dit onderdeel van de Verordening besproken.[7] Daarbij is ook aandacht besteed aan de Uitvoeringswet van EU-verordening elektronische identiteiten en vertrouwensdiensten (hierna: de Uitvoeringswet). Het desbetreffende wetsvoorstel moest bij het afsluiten van het vorige artikel in dit tweeluik nog worden ingediend. Dat is inmiddels gebeurd. De behandeling in de Tweede Kamer was ten tijde van het schrijven van dit artikel bijna afgerond, maar vast staat dat de inwerkingtreding van de Uitvoeringswet te laat komt. Sinds 1 juli 2016 is een groot aantal bepalingen van de Verordening namelijk rechtstreeks van toepassing. Op die datum hadden met de Verordening strijdige bepalingen en bepalingen die hetzelfde regelen als de Verordening uit onder meer het Burgerlijk Wetboek geschrapt moeten zijn[8]. Dat gebeurt echter pas door inwerkingtreding van de Uitvoeringswet.

In dit artikel zal worden ingegaan op het deel van de Verordening dat ziet op elektronische identifica-

1. Joost Linnemann is advocaat te Amsterdam. De auteur is dank verschuldigd aan Gianna Hendriks voor haar nuttige bijdrage aan dit artikel.
2. *PbEG* L 257, 28 augustus 2014, p. 73114.
3. De afkorting eidas stamt uit de tijd dat in de Engelse naam van de Verordening nog werd gesproken over *assurance services*. Uiteindelijk is in plaats daarvan voor de term *trust services* gekozen, maar desondanks wordt de afkorting eidas nog vrij algemeen gebruikt.
4. Overweging 2 Verordening.
5. Op grond van art. 52, lid 2, onder c van de Verordening, is de verplichting tot erkenning van toepassing vanaf drie jaar na de datum van toepassing van de in art. 8, lid 3, en art. 12, lid 8, van de Verordening bedoelde uitvoeringshandelingen. De desbetreffende uitvoeringsverordeningen traden in werking op 29 september 2015.
6. Art. 2 Verordening.
7. J.J. Linnemann, 'Uitvoering van de verordening elektronische identificatie en vertrouwensdiensten', *IR* 2015, nr. 5/6, p. 176.
8. Arrest van het Hof van de Europese Gemeenschap van 7 februari 1973, C-39/72, ECLI:EU:C:1973:13, Slachtpremies.

tiemiddelen. Allereerst zal worden besproken wat de Verordening over dit onderwerp regelt, daarna de effecten van de Verordening voor het nationale recht kort worden belicht, en zal worden stilgestaan bij de praktische uitvoering van de Verordening.

2. Elektronische identificatie in de Verordening

2.1. Definities

De Dienstenrichtlijn verplichtte lidstaten tot het opzetten van zogenaamde 'één- loketten' zodat alle voor het verrichten van een dienst vereiste procedures en formaliteiten (zoals een vergunningaanvraag) eenvoudig, op afstand en met elektronische middelen kunnen worden afgewikkeld. Veel onlinediensten die via dergelijke loketten toegankelijk zijn, vergen elektronische identificatie, authenticatie en een elektronische handtekening.
In de fysieke wereld worden ter identificatie van personen identiteitsbewijzen gebruikt, zoals paspoort, identiteitskaart of rijbewijs. Deze documenten bevatten niet alleen identificerende gegevens, maar ook echtheidskenmerken zoals een speciaal bewerkte foto, zegel of hologram. Hierdoor weet degene die het identiteitsdocument controleert met wie hij te maken heeft, dat het document echt is en dat de gegevens op het document authentiek zijn. Online gaat dit natuurlijk anders. Elektronische identificatie is een proces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt om een uniek persoon aan te duiden.[9]
Hoofdstuk 2 (artikelen 6 tot en met 12) van de Verordening ziet op elektronische identificatie.
Elektronische identificatie wordt in de Verordening gedefinieerd als het proces van het gebruiken van persoonsidentificatiegegevens in elektronische vorm die op unieke wijze een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, aanduiden.[10]
Een elektronisch communicatiemiddel wordt gedefinieerd als een materiële en/of immateriële eenheid die gebruikt wordt voor authenticatie[11] bij een onlinedienst.[12]
In paragraaf 2.2 zullen de wederzijds erkende elektronische identificatiemiddelen, die het gebruik van buitenlandse (overheids)diensten gemakkelijker moeten maken, worden besproken. In paragraaf 2.3 zal worden stilgestaan bij de betrouwbaarheidsniveaus voor toegang tot onlinediensten.

9. Art. 3, onderdeel 1, Verordening.
10. Art. 3, onder 1, Verordening.
11. Authenticatie is een elektronisch proces dat de bevestiging van de elektronische identificatie van een natuurlijke persoon of rechtspersoon, of van de oorsprong en integriteit van gegevens in elektronische vorm mogelijk maakt, dit blijkt uit art. 3, onder 5, Verordening.
12. Art. 3, onder 2, Verordening.

2.2. Wederzijds erkenning van elektronische identificatiemiddelen

2.2.1. Doel en reikwijdte

Doel van de wederzijdse erkenning van elektronische identificatiemiddelen is het faciliteren van grensoverschrijdende diensten op de interne markt. Daarnaast zal de wederzijdse erkenning bedrijven in staat stellen grensoverschrijdend activiteiten te ondernemen zonder daarbij veel belemmeringen te ondervinden in hun contacten met overheidsinstanties.[13] De bedoeling is dat de Verordening bijdraagt aan transparantie, toegankelijkheid en geloofwaardigheid van elektronische identificatiediensten. Wederzijdse erkenning maakt het bijvoorbeeld om met behulp van een elektronisch identificatiemiddel in een andere lidstaat online belastingaangifte te doen, of om online in te schrijven bij een buitenlandse universiteit.
De wederzijdse erkenning van elektronische identificatiemiddelen houdt in dat als voor een bepaalde onlinedienst die wordt aangeboden door een openbare instantie in lidstaat A, een elektronisch identificatiemiddel nodig is, een elektronisch identificatiemiddel dat is uitgegeven in lidstaat B, dient te worden erkend.[14] De wederzijdse erkenning is niet onvoorwaardelijk. Allereerst moet het elektronisch identificatiemiddel zijn uitgegeven op grond van een stelsel voor elektronische identificatie dat is opgenomen in de lijst die de Commissie heeft bekendgemaakt.[15] Ten tweede moet het betrouwbaarheidsniveau van het elektronisch identificatiemiddel gelijk of hoger zijn aan het betrouwbaarheidsniveau dat de bevoegde openbare instantie als voorwaarde stelt voor onlinetoegang tot die dienst in eigen land. Ten derde moet de openbare instantie in kwestie het betrouwbaarheidsniveau substantieel of hoog gebruiken voor toegang tot de onlinedienst (zie hiervoor paragraaf 2.3 van dit artikel).
De Verordening laat Nederland overigens geen ruimte om zelf te bepalen of een elektronisch identificatiemiddel van een andere lidstaat aan de Europese eisen voldoet. Dit stuk voor stuk beoordelen van elektronische identiteiten van individuele lidstaten zou leiden tot een onwenselijke situatie. Het zou betekenen dat lidstaten elkaar zouden mogen toetsen; met alle nadelige gevolgen van dien.[16]
De Verordening gaat over de verplichte erkenning door openbare instanties van bepaalde in andere lidstaten uitgegeven elektronische identificatiemiddelen. Uiteraard staat het private marktpartijen in een lidstaat (zoals webwinkels of verzekeraars) vrij om toegang tot hun diensten open te stellen aan burgers of ondernemingen uit andere lidstaten, waarbij die burgers of ondernemingen gebruik maken van elektronische identificatie-

13. Overweging 9 Verordening.
14. Art. 6 Verordening.
15. Art. 9 Verordening.
16. *Kamerstukken II* 2015/16, 34 413, nr. 6, p. 7.

middelen die in hun eigen land zijn uitgegeven. Zo kan een Poolse webwinkel een Nederlandse klant toegang verlenen op basis van een in Nederland uitgegeven elektronisch identificatiemiddel. Omgekeerd kan een Nederlandse verzekeraar een Poolse burger toegang verlenen op basis van een in Polen uitgegeven elektronisch identificatiemiddel. De Verordening verplicht daar echter niet toe.

2.3. Betrouwbaarheidsniveaus

Het is van belang om in het kader van wederzijdse erkenning stil te staan bij het onderscheid in betrouwbaarheidsniveaus voor toegang tot onlinediensten. Het betrouwbaarheidsniveau geeft de mate van vertrouwen weer die in een elektronisch identificatiemiddel kan worden gesteld voor het vaststellen van de identiteit van een persoon. Zodoende dient het betrouwbaarheidsniveau zekerheid te geven dat iemand ook daadwerkelijk degene is die hij beweert te zijn.[17] Aan de hand van betrouwbaarheidsniveaus kunnen lidstaten en private partijen hun elektronische identificatiemiddelen inrichten.

De Verordening onderscheidt de betrouwbaarheidsniveaus laag, substantieel en hoog[18], maar bepaalt daarover zelf niet veel meer dan dat het gaat om identificatiemiddelen die respectievelijk een beperkte mate, een substantiële mate, of een hoge mate van vertrouwen bieden in iemands opgegeven of beweerde identiteit. De op grond van art. 8 lid 3 vastgestelde Uitvoeringsverordening betrouwbaarheidsniveaus beschrijft in detail de minimale technische specificaties en procedures van de verschillende betrouwbaarheidsniveaus.[19] Om het noodzakelijke vertrouwen tot stand te brengen, moet een voldoende hoog betrouwbaarheidsniveau worden gewaarborgd.[20] In het kader van dit artikel zijn met name de betrouwbaarheidsniveaus substantieel en hoog van belang. Substantieel en hoog zijn de minimumniveaus die openbare instanties uit andere lidstaten dienen te erkennen wanneer een gebruiker zich identificeert.[21] Overigens staat het lidstaten vrij ook lagere niveaus te erkennen, zij zijn daartoe alleen niet verplicht.[22]

Het betrouwbaarheidsniveau wordt bepaald met gebruikmaking van de specificaties en procedures die in de bijlage bij de Uitvoeringsverordening zijn vastgelegd. Aan de hand van die specificaties en procedures wordt de betrouwbaarheid en kwaliteit van bepaald van vier elementen, te weten inschrijving, beheer van elektronische identificatiemiddelen, authenticatie, en beheer en organisatie.[23]

2.3.1. Inschrijving

Allereerst wordt gekeken naar de inschrijving. De daarvoor gelden specificaties en procedures hebben betrekking op (i) de aanvraag en registratie van de inschrijving, (ii) het bewijs en de verificatie van de identiteit van de natuurlijk persoon of rechtspersoon aan wie het elektronische identificatiemiddel moet worden afgegeven, en (iii) de koppeling tussen de elektronische identificatiemiddelen van de desbetreffende natuurlijke persoon of rechtspersoon.

Ten aanzien van de inschrijving geldt voor het betrouwbaarheidsniveau substantieel bijvoorbeeld de eis dat (i) is geverifieerd dat de persoon in het bezit is van een bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt (zeg maar: een geldig identiteitsbewijs), en (ii) het bewijs is gecontroleerd op de echtheid ervan, en (iii) er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is.

Voor betrouwbaarheidsniveau hoog geldt dan als aanvullende eis dat een identiteitsbewijs voorzien is van een foto of biometrische gegevens en dat de opgegeven identiteit wordt geverifieerd door vergelijking van een of meer fysieke kenmerken van de persoon met een gezaghebbende bron (zoals met gegevens in de persoonsregistratie van de desbetreffende lidstaat). Het verschil is in dit geval dat bij niveau substantieel de foto op een identiteitsbewijs door een ambtenaar wordt gecontroleerd op gelijkenis met de aanvrager (is degene die voor mij staat ook degene op de foto?), terwijl bij niveau hoog ook wordt gecontroleerd aan de hand van gegevens in bijvoorbeeld een basisadministratie van de overheid.

2.3.2. Beheer van elektronische identificatiemiddelen

Naast de inschrijving wordt gekeken naar het beheer van elektronische identificatiemiddelen. Om dit element te beoordelen kijkt men naar (i) de kenmerken en het ontwerp van elektronische identificatiemiddelen, (ii) de uitgifte, uitreiking en activering van elektronische identificatiemiddelen, (iii) de schorsing, herroeping en reactivering van

17. Overweging 16 Verordening.
18. Art. f1 Uitvoeringsverordening betrouwbaarheidsniveaus.
19. Uitvoeringsverordening 2015/1502 van de Europese Commissie tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig art. 8, lid 3, van de Verordening (EU) nr. 910/2014 (*PbEU* 2015, L 235/7), (hierna: Uitvoeringsverordening betrouwbaarheidsniveaus).
20. Overweging 6 Uitvoeringsverordening betrouwbaarheidsniveaus.
21. MvT Uitvoeringswet p. 9.
22. Art. 6 lid 2 Verordening.
23. Inschrijving, beheer van elektronische identificatiemiddelen, authenticatie en beheer & organisatie zoals bedoeld in punt 2.1 t/m 2.4 van de bijlage bij de Uitvoeringsverordening betrouwbaarheidsniveaus.

elektronische identificatiemiddelen en (iv) de verlenging en vervanging van elektronische identificatiemiddelen.
Bij het ontwerp van het elektronische identificatiemiddel gaat het bijvoorbeeld om de vraag hoeveel authenticatiefactoren moeten worden gebruikt. De Uitvoeringsverordening onderscheidt drie authenticatiefactoren: een op bezit gebaseerde authenticatiefactor (bijvoorbeeld een pasje), een op kennis gebaseerde authenticatiefactor (bijvoorbeeld een wachtwoord of pincode, of een combinatie van gebruikersnaam en wachtwoord), en een inherente authenticatiefactor (bijvoorbeeld een vingerafdruk).
Voor betrouwbaarheidsniveau laag kan worden volstaan met één authenticatiefactor (bijvoorbeeld een combinatie van gebruikersnaam en wachtwoord, of een pasje). Voor de hogere betrouwbaarheidsniveaus zijn ten minste twee authenticatiefactoren vereist (bijvoorbeeld een pasje dat alleen in combinatie met een pincode kan worden gebruikt).

2.3.3. Authenticatie

Het derde element waarnaar wordt gekeken bij het bepalen van het betrouwbaarheidsniveau is authenticatie. Authenticatie is de controle van iemands identiteit online, het gaat dus om het daadwerkelijk online gebruik van het identificatiemiddel.
Hierbij geldt bijvoorbeeld dat voor de betrouwbaarheidsniveaus substantieel en hoog gebruik moet worden gemaakt van zogenaamde dynamische authenticatie. Hierbij wordt bij elk gebruik van het identificatiemiddel een unieke code gegenereerd (bijvoorbeeld door een token zoals dat door banken wordt gebruikt ter beveiliging van de ebanking omgeving). Aldus wordt vastgesteld dat de gebruiker op het moment van gebruik daadwerkelijk in bezit is van het token. Je zou denken dat dit ook zonder dynamische authenticatie zou kunnen worden vastgesteld, en wel door gebruik van een inherente authenticatiefactor, maar daar denkt de Europese wetgever dus anders over.

2.3.4. Beheer en organisatie

Het laatste element waarnaar wordt gekeken bij het bepalen van het betrouwbaarheidsniveau is beheer en organisatie. Dit element moet worden onderscheiden van het beheer van de identificatiemiddelen zelf (zie daarvoor paragraaf 2.3.2). Bij het element beheer en organisatie gaat het om de inrichting van de dienstverlening op het gebied van elektronische identificatie. Daarbij kan bijvoorbeeld worden gedacht aan informatiebeveiliging, administratie en technische controles.
Opvallend bij dit element is dat de verschillen tussen de betrouwbaarheidsniveaus relatief klein zijn. Ze zijn er wel, bijvoorbeeld bij de verplichte periodiek audits. Voor betrouwbaarheidsniveau laag geldt dat de audits intern mogen zijn, terwijl ze voor betrouwbaarheidsniveau hoog extern moeten zijn.

3. Praktische uitwerking

De Verordening heeft rechtstreekse werking. Dit betekent niet dat de wetgevende werkzaamheden zijn voltooid met de inwerkingtreding. Om de Verordening in te passen in het Nederlandse recht is een uitvoeringswet vereist. Deze Uitvoeringswet omvat wijzigingen van de Telecomwet, Algemene wet bestuursrecht, het Burgerlijk Wetboek en de Wet bescherming persoonsgegevens. Het uitgangspunt van de rechtstreekse werking van de Verordening en minimumomzetting wordt door middel van het wetsvoorstel gerespecteerd.[24] Het in dit artikel besproken deel van de Verordening over elektronische identificatie vereist alleen feitelijke uitvoering, en dan vooral de ontwikkeling van een landelijk koppelpunt dat grensoverschrijdende elektronische identificatie mogelijk moet maken. De wetswijzigingen die het gevolge zullen zijn van de Uitvoeringswet vloeien voort uit het deel van de Verordening dat betrekking heeft op vertrouwensdiensten.

3.1. eIDAS-koppelpunt

Om grensoverschrijdend gebruik van elektronische identificatiemiddelen mogelijk te maken, is in elke lidstaat een technische voorziening nodig. Die voorziening moet berichten over elektronische identiteiten die in een lidstaat zijn verstrekt kunnen versturen en berichten kunnen ontvangen over elektronische identiteiten die zijn verstrekt in andere lidstaten. De desbetreffende voorziening in een lidstaat voorziet openbare instanties in die lidstaat van persoonsidentificatiegegevens van burgers en bedrijven uit andere lidstaten, die die gegevens gebruiken voor onlinedienstverlening aan deze groep. Andersom kan de voorziening in een lidstaat persoonsidentificatiegegevens van burgers en bedrijven uit die lidstaat naar openbare instanties in andere lidstaten sturen, waar deze burgers en bedrijven onlinediensten willen afnemen.
Het Nederlandse koppelpunt (het eIDAS-koppelpunt of koppelpunt) wordt aangesloten op de nationale infrastructuur elektronische identiteiten, het eID-stelsel. Het koppelpunt stelt Nederlandse openbare instanties in staat om vast te stellen of het een elektronisch identificatiemiddel betreft dat is gemeld bij de Europese Commissie, over welk betrouwbaarheidsniveau dat middel beschikt en levert de authenticatie van de persoon, zodat de openbare instantie kan bepalen of toegang tot de onlinedienst wordt verleend. Door middel van aansluiting van het koppelpunt op de bestaande Nederlandse identiteitsinfrastructuur kan het internationale berichtenverkeer via een reeds bestaande

24. *Kamerstukken II* 2015/16, 34 413, nr. 7, p. 3.

beveiligde verbinding plaatsvinden en worden onnodige inspanningen en kosten bij openbare instanties vermeden, zo blijkt uit de Memorie van Toelichting.

Bij de totstandkoming van het eIDAS-koppelpunt is gegevensbescherming is een belangrijk aandachtspunt. Er is een zogenaamde Privacy Impact Assessment (PIA) uitgevoerd.[25] Hierover heeft de Autoriteit Persoonsgegevens geoordeeld. De Autoriteit persoonsgegevens heeft wat betreft het eIDAS-koppelpunt onder meer gewezen op het feit dat de ontwikkeling van het eIDAS-koppelpunt complex is en dat het grondrecht voor bescherming van de persoonlijke levenssfeer voldoende gewaarborgd moet zijn.[26] Onder de Wbp zijn de overheidsinstanties verantwoordelijke voor de persoonsgegevens die zij in het kader van hun diensten verwerken en doorgeven via het koppelpunt. De Minister van Economische Zaken blijft voorlopig verantwoordelijke in de zin van de Wbp voor het eIDAS-koppelpunt.[27]

Het uitgangspunt is dat het koppelpunt versleutelde berichten met persoonsgegevens naar openbare instanties routeert en dat de beheerder van het koppelpunt de gegevens niet zal mogen decoderen of opslaan. De berichten die via het koppelpunt lopen dienen ter unieke aanduiding van de gebruiker in elk geval de voor- en achternaam, geboortedatum en een unieke identifier te bevatten. Vooralsnog zullen door het eIDAS-koppelpunt geen bijzondere persoonsgegevens in de zin van art. 16 Wbp worden verwerkt. Echter kan het, afhankelijk van de dienst met het oog waarop authenticatie plaatsvindt, nuttig zijn dat andere gegevens over gebruikers vanuit het stelsel voor identificatie via een bericht worden geleverd. De Verordening bevat hierover geen regeling, maar sluit de mogelijkheid ook niet uit. Er dient er daarom van te worden uitgegaan dat ook berichten met bijzondere persoonsgegevens het koppelpunt zullen passeren. Hierover heeft het koppelpunt geen controle.[28]

3.2. Nederlandse multimiddelenaanpak

Hierboven werd al aangegeven dat eIDAS-knoop gekoppeld zal worden aan het eID-stelsel.

Het kabinet treft op dit moment voorbereidingen om te komen tot dit nieuwe stelsel voor digitale identificatie en authenticatie. Op dit moment gebruiken burgers vooral DigiD om zaken met de overheid digitaal te regelen. Het is inmiddels echter tien jaar geleden dat DigiD werd ingevoerd. In de huidige tijdsgeest van explosief groeiende digitalisering, dienen burgers meer ruimte te krijgen om een inlogmiddel te gebruiken dat zij vertrouwen en dat past bij de eigen gebruiksvoorkeur. In de pilots is geëxperimenteerd met het inloggen op het zogenaamde BSN-domein.[29]

Er lopen verschillende pilots met DigiD - waarvan de merknaam behouden zal blijven - om DigiD te verbeteren en het betrouwbaarheidsniveau te versterken. Uit meerdere onderzoeken blijkt dat de naamsbekendheid van DigiD zeer groot is en dat het merk groot vertrouwen geniet.[30] Het doel is dus om het grote volume en bereik van DigiD te behouden maar dan op betrouwbaarheidsniveau substantieel. De politiek heeft zich uitgesproken over een multimiddelenstrategie. Dit wil zeggen dat het kabinet mensen de vrijheid gaat geven om zelf uit meerdere, door de overheid erkende, inlogmiddelen te kiezen en daarbij de beschikking geven over ook hoger beveiligde middelen dan tot nu toe.

De toelating van alle publieke en private inlogmiddelen voor het BSN-domein zal onder één publiekrechtelijk regime komen en bij wet[31] worden eisen gesteld waaraan inlogmiddelen voor gebruik in het publieke domein moeten voldoen, alsook waaraan hierbij betrokken partijen moeten voldoen. Het kabinet heeft gekozen voor een stapsgewijze uitrol.

> Stap 1: Continuering huidige dienstverlening
> Stap 2: Aansluiten nieuwe organisaties op basis van eerste uniforme toelatingseisen
> Stap 3: Structurele uitrol multimiddelenaanpak

In stap 1 wordt de dienstverlening uit de pilotfase (met uitzondering van het publieke middel) doorgezet. Dat betekent dat de hoogwaardige authenticatiemiddelen, onder de huidige pilotcondities, beschikbaar blijven voor gebruikers. In deze stap zal het aantal gebruikers worden uitgebreid tot het maximaal aantal gebruikers voor de pilot. In de pilot kunnen Nederlandse boeren met eHerkenning[32] inloggen bij het Belgische departement Landbouw en Visserij. Andersom kunnen ongeveer driehonderd Belgische 'grensboeren' digitaal zakendoen met RVO.nl met hun eigen, Belgische inlogmiddel.[33] In de gemeente Rotterdam kan men via Idensys bij de kredietbank inloggen door het maken van een selfie, waarbij een automatische check plaatsvindt met biometrische gegevens op een identiteitsbewijs. Daarnaast kan men ervoor kiezen om een ge-

25. J.H.J. Terstegge, J.A.G. Versmissen & T.N. Tran, Privacy Impact Assessment: eIDAS-koppelpunt versie 1.0, 31 juli 2015.
26. *Kamerstukken II* 2015/16, 34 413, nr. 6, p. 13.
27. J.H.J. Terstegge, J.A.G. Versmissen & T.N. Tran, Privacy Impact Assessment: eIDAS-koppelpunt versie 1.0, 31 juli 2015, p. 5.
28. J.H.J. Terstegge, J.A.G. Versmissen & T.N. Tran, Privacy Impact Assessment: eIDAS-koppelpunt versie 1.0, 31 juli 2015, p. 12.
29. BSN-domein of publiek domein: dienstverlening door overheden en andere instanties die gerechtigd zijn het BSN te gebruiken, zo blijkt uit de brief van minister Blok van 25 augustus 2016.
30. 95% kent DigiD en 77% vertrouwt DigiD, zo blijkt uit *Kamerstukken II* 2015/16, 26 643, Bijlage I bij Impuls eID, p. 3.
31. De momenteel in voorbereiding zijnde Wet Generieke Digitale Infrastructuur, zie hiervoor *Kamerstukken II* 2015/16, 26 643, nr. 373.
32. In de pilotfase wordt gebruik gemaakt van eHerkenning voor bedrijven en Idensys voor consumenten.
33. Eherkenning.nl (zoek op: nieuwsberichten, idensys en eherkenning zetten stappen voor Europees gebruik), geraadpleegd op 7 september 2016.

bruikersnaam en wachtwoord in combinatie met een mobiele code te gebruiken. Pilotgebruikers zijn vrij in het kiezen van een methode.[34]

In stap 2 is er ruimte voor nieuwe organisaties die zich graag willen aansluiten. Deze fase zal plaatsvinden in het derde kwartaal van 2017. In deze fase zullen er extra waarborgen zijn op het gebied van privacy- en informatiebeveiliging. Dit gebeurt in elk geval door *privacy by design* in te bouwen in het BSN-koppelregister (hierna: BSNk). Het BSNk kan dan niet meer zien waar een gebruiker naar toe gaat. Daarnaast wordt er passende misbruik- en fraudebestrijding toegepast.

In stap 3 zal de multimiddelenaanpak breed worden uitgerold. Dit houdt in dat burgers kunnen kiezen uit verschillende inlogmiddelen en dat ze deze kunnen gebruiken bij publieke organisaties. Eind 2018 zou het mogelijk moeten zijn om alle organisaties in het BSN-domein aangesloten te hebben op de tot het BSN-domein toegelaten authenticatiediensten. In de loop van 2018 is *privacy by design* bij alle partijen verplicht volledig doorgevoerd, waarmee de privacy en veiligheid van de gebruiker maximaal geborgd is. Noodzakelijke toepassingen in deze fase zijn onder meer het digitaal ondertekenen van stukken en het machtigen van iemand om zaken te doen (voor de minder 'digivaardigen').[35]

De Impuls eID dient erin te resulteren dat per uiterlijk oktober 2018 in beginsel alle dienstverleners in het BSN-domein in staat zijn om grootschalig alle door de minister van Binnenlandse Zaken en Koninkrijksrelaties toegelaten inlogmiddelen in hun digitale dienstverlening te accepteren. Het kabinet kiest bij het uitwerken van de planning voor het gaandeweg realiseren van dit resultaat in de diverse geledingen van de publieke dienstverlening, met de Zorg en de Belastingdienst als eerste prioriteiten (de zogenaamde 'voorlopers').

De merknaam DigiD zal in gebruik blijven, maar voortaan zal hij wel dienen als paraplu van meerdere publieke inlogmanieren. Het cruciale belang van veiligheid en vertrouwen in digitale identiteitsvaststelling en de kansen tot het beter benutten van technische ontwikkelingen spelen op de achtergrond een grote rol. Het behouden van de naam DigiD maakt het daarnaast makkelijker om in de toekomst – met oog voor betere dienstverlening en kostenbesparing - op minder ingrijpende wijze inlogmanieren te blijven vernieuwen.[36]

Zoals gezegd – en dat volgt ook uit de hiervoor beschreven tijdlijn is het eID-stelsel nog in ontwikkeling. Inmiddels heeft de Algemene Rekenkamer de stelselvernieuwing onderzocht en daarover gerapporteerd.[37] Volgens de Rekenkamer is op nog niet is voldaan aan een aantal onderzochte randvoorwaarden:

- De verantwoordelijkheden voor het eID-stelsel zijn niet eenduidig belegd en de governancestructuur is ingewikkeld.
- Op wezenlijke onderdelen van het eID-stelsel moeten nog besluiten worden genomen of uitgewerkt.
- Een actuele integrale business case en alternatievenafweging ontbreken vooralsnog.
- Een integrale visie op de inrichting van het toezicht voor het eID-stelsel ontbreekt.

Al met al moet er dus het nodige gebeuren om het eIDstelsel tot stand te brengen. Omdat, zoals gezegd, het eIDstelsel zal worden aangesloten op het eIDASkoppelpunt, is het voor de feitelijke uitvoering van de Verordening van groot belang dat een en ander goed en tijdig wordt afgerond.

4. Conclusie

Overheidsdiensten worden tegenwoordig meer en meer digitaal aangeboden. De Verordening biedt een kader om ook grensoverschrijdend gebruik van die diensten mogelijk te maken waarbij burgers en bedrijven gebruik maken van in hun 'eigen' lidstaat uitgegeven identificatiemiddelen.

In Nederland zijn vooral feitelijke uitvoeringshandelingen nodig om te voldoen aan de eisen van het desbetreffende deel van de Verordening. Het gaat dan vooral om het inrichten van het eIDAS-koppelpunt. Dat koppelpunt zal worden aangesloten op het nieuwe eIDstelsel. De in dat kader voorgestane multimiddelenaanpak zal het voor gebruikers makkelijker maken om in te loggen op (overheids) diensten. Ook hebben gebruikers straks de vrijheid om zelf uit meerdere, door de overheid erkende, inlogmiddelen te kiezen, ook met hogere betrouwbaarheidsniveaus.

34. Idensys.nl (zoek op: verhalen uit de praktijk, gemeente Rotterdam), geraadpleegd op 7 september 2016.
35. *Kamerstukken II* 2015/16, 26 643, Bijlage II bij Impuls eID, p. 1-6.
36. Brief van minister Blok 25 augustus 2016.
37. Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel), Rapport Algemene Rekenkamer, Den Haag, September 2016.