Een handreiking voor overheidsorganisaties

Betrouwbaarheidsniveaus voor digitale dienstverlening

Forum Standaardisatie

Forum Standaardisatie
Forum Standaardisatie is ingesteld om de digitale samenwerking (interoperabiliteit) tussen overheden onderling en tussen overheid, bedrijfsleven en publiek te bevorderen. Interoperabiliteit zorgt ervoor dat verschillende systemen beter op elkaar aansluiten en dat gegevens uitgewisseld en/of hergebruikt kunnen worden. Het gebruik van open standaarden speelt hierbij een belangrijke rol.

Het Forum Standaardisatie adviseert op basis van onderzoek het Nationaal Beraad Digitale Overheid, dat op haar beurt aanbevelingen doet aan de Ministeriële Commissie Digitale Overheid over beleid op het gebied van interoperabiliteit en open standaarden. Het Forum is tot stand gekomen op initiatief van het ministerie van Economische Zaken. Bureau Forum Standaardisatie, het secretariaat van Forum Standaardisatie, is ondergebracht bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Voor meer informatie kijk op **www.forumstandaardisatie.nl**.

Voorwoord

Thema van het overheidsbrede Digiprogramma 2016-2017 is 'De mens centraal'.
Als Digicommissaris heb ik gemerkt dat het niet altijd meevalt om dat thema in de praktijk leidend te laten zijn bij de keuzes die gemaakt moeten worden. Burgers en bedrijven zijn gebaat bij een eenduidige, herkenbare overheid, die veilige en betrouwbare dienstverlening biedt zonder onnodige kosten en administratieve lasten. Een overheid dus, die in vergelijkbare gevallen dezelfde keuzes maakt. Omdat er zoveel verschillende overheden en overheidsorganisaties zijn, is het geen vanzelfsprekendheid dat die keuzes in vergelijkbare gevallen leiden tot dezelfde dienstverlening.

Deze Handreiking Betrouwbaarheidsniveaus helpt overheidsorganisaties om de juiste keuzes te maken bij het digitaliseren van de dienstverlening. De handreiking koppelt eigenschappen van de dienst aan genormeerde Europese betrouwbaarheidsniveaus en houdt daarbij rekening met bijvoorbeeld machtigen, retourstromen van informatie en machine-to-machine berichtenverkeer. Het is als het ware een gereedschapskist voor overheidsdienstverleners, waarmee zaken als Single Sign On over overheidsorganisaties heen, grensoverschrijdende dienstverlening, elektronische handtekeningen, zegels en tijdstempels makkelijker te regelen zijn.

De standaardisatie, die mogelijk wordt gemaakt door de Handreiking, maakt de overheid transparanter en eenduidiger. De mens centraal! Bovendien worden overheidsorganisaties ondersteund in hun digitaliseringsproces en hoeven zij niet meer hun eigen individuele (risico)afweging op te stellen om te bepalen welk betrouwbaarheidsniveau bij hun dienstverlening passend is. Dat is efficiënt!

Aanbieders van authenticatiemiddelen doen er goed aan om hun aanbod zo snel mogelijk op eenzelfde wijze te categoriseren, zodat overheidsdienstverleners die digitale diensten aanbieden makkelijk de link kunnen leggen tussen hun behoefte en het beschikbare aanbod van middelen.

Ik beveel deze nieuwe Handreiking Betrouwbaarheidsniveaus warm in uw aandacht aan. Om toepassing van de handreiking te bevorderen, zal ik er voor zorgen dat deze Handreiking – via de regieraden en het Nationaal Beraad-overheids – breed wordt verspreid.

Bas Eenhoorn
Digicommissaris


MADE IN
ENGLAND

Inhoudsopgave

Voorwoord **3**

1 Inleiding **7**
1.1 E-overheid: zorgvuldig het betrouwbaarheidsniveau kiezen 7
1.2 'One size fits all' bestaat niet 8
1.3 Maak een risicoanalyse met deze handreiking 8
1.4 Hoe is deze handreiking tot stand gekomen? 10
1.5 Leeswijzer 11

2 Afbakening en context **13**
2.1 Afbakening 13
2.2 Welke trends en ontwikkelingen spelen er nu? 13

3 Uitgangspunten **19**
3.1 Vereenvoudigde risicoanalyse 19
3.2 eIDAS-verordening als basis 21
3.3 eIDAS: drie betrouwbaarheidsniveaus 22

4 Inschaling van diensten **27**
4.1 Classificatiemodel en criteria 27
4.2 Referentiescenario 38
4.3 Correctiefactoren 39
4.4 Voorbeelden van diensten en betrouwbaarheidsniveaus 41

5 Machtigingen **43**
5.1 Waar gaat het eigenlijk over? 43
5.2 Wat betekenen machtigingen voor een individuele dienst? 44
5.3 Wat betekent machtiging in de praktijk? 44
5.4 Overige aandachtspunten: misbruik en fraude 44

6 Applicatie-applicatieverkeer **47**
6.1 Waar gaat het eigenlijk over? 47
6.2 Manieren van beveiliging 47
6.3 Wat betekent dit voor toepassing van het classificatiemodel? 48

7 Retourstromen **49**
7.1 Waar gaat het eigenlijk over? 49
7.2 Wat betekent dit voor een individuele dienst? 49
7.3 Wat betekent dit voor toepassing van het classificatiemodel? 51

8 Eenmalig inloggen 55
8.1 Waar gaat het eigenlijk over? 55
8.2 Perspectief van de individuele dienst 55
8.3 Wat betekent dit voor toepassing van het classificatiemodel? 56
8.4 Overige aandachtspunten 56

9 Ondertekening 59
9.1 Inleiding 59
9.2 Ondertekenen en de elektronische handtekening, waar hebben we het eigenlijk over? 59
9.3 Welke elektronische handtekeningen heeft u als dienstaanbieder nodig? 64
9.4 Overige vragen over elektronische handtekeningen 67

Bijlagen
1 Relevante Wet- en regelgeving 73
2 Voorbeelden van invulling van de wettelijke kaders en vertaling van papieren naar elektronische situatie 89
3 Begrippenkader 92

1 Inleiding

Waarom deze handreiking?

1.1 E-overheid: zorgvuldig het betrouwbaarheidsniveau kiezen

Alle overheidsdiensten digitaal

De overheid zet grootschalig in op digitale dienstverlening aan burgers en bedrijven. Alle diensten van de overheid moeten in 2017 digitaal beschikbaar zijn. Het streven is zo administratieve lastenverlichting, een betere dienstverlening en een efficiëntere overheid te realiseren.

Verplichtingen voor overheidsorganisaties

Deze doelstelling schept verplichtingen voor u als overheidsorganisatie. U heeft te maken met de Algemene wet bestuursrecht (Awb). Die vereist dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' verloopt. Daarnaast is er het Besluit voorschrift informatiebeveiliging rijksdienst (VIR). Dit stelt dat rijksoverheden de betrouwbaarheidseisen voor digitale diensten moeten vaststellen aan de hand van een risicoafweging en er op moeten toezien dat er passende maatregelen worden getroffen om aan die betrouwbaarheids-eisen te voldoen. In de Awb en het Besluit VIR staan de eisen aan die maatregelen niet concreet gedefinieerd. Het Rijk en andere overheden hebben daarom zogenoemde normen vastgesteld: het Rijk heeft de BIR (Baseline Informatiebeveiliging Rijk), provincies hebben de IBI (Interprovinciale Baseline Informatiebeveiliging) en gemeenten hebben de BIG (Baseline Informatiebeveiliging Gemeenten).

Keuze maken in betrouwbaarheidsniveaus

In de Awb en het Besluit VIR staan de eisen zoals gezegd niet concreet gedefinieerd. Maar er is wel behoefte aan helderheid nu e-diensten steeds meer worden gebruikt. Zo is het belangrijk dat overheidsorganisaties in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid vereisen (en borgen) voor hun digitale diensten. Belangrijk is ook dat hun keuzes helder en transparant zijn. Dat draagt bij aan een transparante, toegankelijke, geloofwaardige en zorgvuldig opererende overheid en aan de rechtszekerheid van burgers en bedrijven.

Handreiking op basis van eIDAS

Met deze handreiking helpen we u een heldere en transparante keuze te maken voor het betrouwbaarheidsniveau van uw digitale dienst. We doen dit op basis van de eIDAS-verordening voor digitale identificatie- en vertrouwensdiensten, die van kracht is sinds 1 juli 2016. Daarnaast nemen we de bijbehorende uitvoeringsbesluiten en de nationale wet- en regelgeving mee.

1.2 ‘One size fits all’ bestaat niet

Geen hoog of laag niveau

Er zijn veel verschillende digitale overheidsdiensten. Het is niet mogelijk om voor al die diensten één uniforme oplossing vast te stellen voor identificatie, authenticatie en autorisatie. Zo is een standaardoplossing met een zeer hoog betrouwbaarheidsniveau in veel gevallen te duur of simpelweg niet nodig. Bovendien beperk je daarmee het gebruik van e-diensten. Maar een standaardoplossing met een laag betrouwbaarheidsniveau werkt ook niet. Die kan namelijk aanzienlijke veiligheidsrisico’s met zich mee brengen.

Algemeen inzetbare oplossingen

Burgers en bedrijven zullen met verschillende betrouwbaarheidsniveaus te maken krijgen bij verschillende diensten. Om te voorkomen dat gebruikers daardoor te maken krijgen met een grote, onhandige, digitale ‘sleutelbos’, werkt de rijksoverheid aan algemeen inzetbare oplossingen. Voorbeelden daarvan zijn DigiD, PKIoverheid, eHerkenning en Idensys). Hoewel gebruikers dus wel met de keuze van een niveau van een authenticatie-middel of -middelen worden geconfronteerd, wordt zodoende een digitale sleutelbos vermeden.

1.3 Maak een risicoanalyse met deze handreiking

Handreiking helpt keuze maken

Welk betrouwbaarheidsniveau gebruik je in welke situatie? Die vraag is voor u als uitvoerder van publieke diensten niet gemakkelijk te beantwoorden. Daarom hebben we deze handreiking opgesteld. Het helpt u om een eenduidige, efficiënte en bewuste keuze te maken voor de betrouwbaarheidsniveaus van digitale overheidsdiensten.

Vereenvoudigde risicoanalyse met classificatiemodel

Deze handreiking bevat een ‘classificatiemodel’. Hiermee maakt u een vereenvoudigde risicoanalyse van uw digitale dienst. Op basis van verschillende (wettelijke) criteria maakt het classificatiemodel een algemene koppeling tussen (soorten) diensten en betrouwbaarheidsniveaus. Met deze handreiking kunt ook zien wanneer een hoger of lager betrouwbaarheidsniveau nodig zou kunnen zijn. We verwijzen in de handreiking niet naar specifieke authenticatiemiddelen.

Beredeneerde keuzes maken

Met het classificatiemodel kunnen architecten, informatiebeveiligers, juristen en bestuurders een beredeneerde keuze maken voor het juiste betrouwbaarheidsniveau voor uw e-diensten.

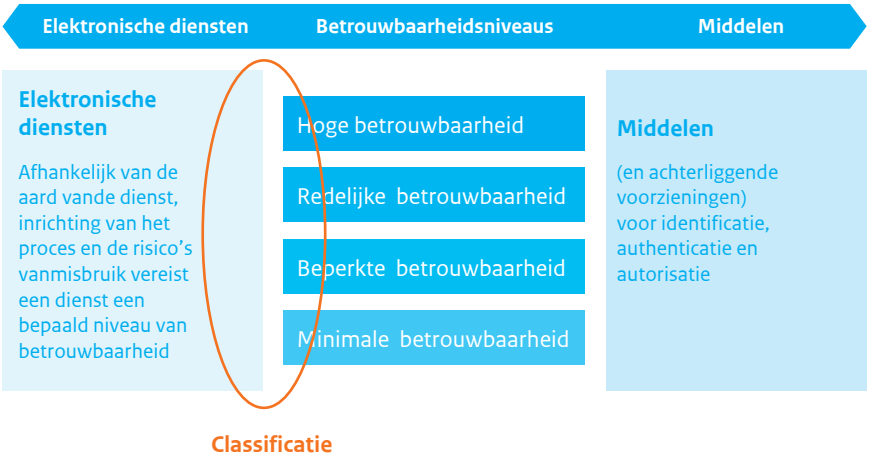
Risicoanalyse niet voor elke dienst geschikt

Let op: in deze handreiking gaat het om een generieke benadering. In de meeste gevallen leidt die tot een adequate keuze, maar uitzonderingen zijn mogelijk. Misschien wijkt de aard van uw dienst of de omstandigheden zo af van het classificatiemodel, dat u toch een volwaardige risico- en impactanalyse moet uitvoeren.

Maak uw keuze kenbaar in een regeling

Het is overigens wenselijk dat u het betrouwbaarheidsniveau voor uw diensten bekendmaakt in een regeling. Denk aan beleidsregels of algemeen bindende voorschriften, afhankelijk van de context. In de toelichting daarbij onderbouwt u uw keuze zodat die ook voor gebruikers van de dienst helder is.

Figuur 1. *De analyse van de risico's in de elektronische dienst bepaalt de* ***gewenste*** *betrouwbaarheid van (met name) authenticatie en dat bepaalt de sterkte van het gebruikte middel. Dat is de reikwijdte van deze handreiking. eIDAS geeft aan de andere kant voor de middelen een kader, de* ***aangeboden*** *betrouwbaarheid (zie 3.2).*



1.4 Hoe is deze handreiking tot stand gekomen?

Handreiking vanaf 2011

Verschillende overheidsorganisaties en bedrijven werkten gezamenlijk aan deze handreiking, gefaciliteerd door Forum Standaardisatie. Daarbij was een van de doelen duidelijk te krijgen welk betrouwbaarheidsniveau voor welke (soorten) diensten passend is. Standaarden die een specifieke oplossing met een specifiek betrouwbaarheidsniveau beschrijven krijgen hiermee ook een duidelijk afgebakend toepassingsgebied.

Het College Standaardisatie heeft in het najaar van 2011 ingestemd met de eerste versie van deze handreiking. Die is daarop breed verspreid onder overheidsorganisaties, met een advies over hoe zij de handreiking kunnen verankeren in hun uitvoeringsbeleid rond digitale dienstverlening.

Handreiking continu in ontwikkeling

De handreiking is geen statisch product. Sinds de eerste versie wordt de ontwikkeling van e-dienstverlening en van identificatie- en authenticatie-middelen gevolgd. Bovendien zijn ervaringen van overheidsorganisaties met de handreiking uiterst welkom. Die worden meegenomen in volgende versies. Forum Standaardisatie en Logius blijven het beheer en de door-ontwikkeling ondersteunen. Dit sluit aan bij de beheerverantwoordelijkheid die Logius heeft voor verschillende identificatie- en authenticatiemiddelen en -standaarden, zoals DigiD (Machtigen), PKIoverheid en eHerkenning.

Community houdt handreiking up-to-date

De partijen die betrokken zijn geweest bij de eerste versie van de handreiking vormen de basis voor een ‘community’ van gebruikers. De community helpt Forum Standaardisatie om de handreiking te onderhouden en verder te ontwikkelen. Zo is de handreiking in de tweede en derde versies inhoudelijk uitgebreid met onderwerpen zoals machtigen, eenmalig inloggen, elektronisch waarmerken en ondertekenen.

Wijzigingen in versie 4

In de huidige versie 4 staat de overgang naar de eIDAS-verordening centraal. Verder is hoofdstuk 9 over ondertekenen aangepast aan recente ontwikkelingen. Daarin zijn eerdere normatieve elementen voor ondertekenoplossingen geschrapt. Generieke oplossingen zoals eHerkenning en Idensys bieden daar handvatten voor. Ook de bijlagen over wet- en regelgeving zijn geactualiseerd.

Niet voor private dienstverleners

Bij versie 4 hebben we overwogen om ons ook te richten op private aanbieders van digitale diensten. Hier hebben we uiteindelijk niet voor gekozen, omdat de juridische grondslag voor hen wezenlijk anders is. Handelt u als overheidsorganisatie zelf privaatrechtelijk? Bijvoorbeeld door de exploitatie van sportaccommodaties? Dan bevelen we deze handreiking toch aan. Zo behandelt u deze digitale diensten hetzelfde als uw publiekrechtelijke digitale diensten.

1.5 Leeswijzer

Hoofdstuk 2-4: de kern

Hoofdstuk 2 beschrijft de afbakening en context voor deze handreiking. Waar gaat deze wel en niet over? Hoofdstuk 3 bevat de uitgangspunten voor de uitwerking van het classificatiemodel. In hoofdstuk 4 lichten we onze methodiek nader toe. Hier vindt u het daadwerkelijke classificatiemodel om uw diensten op het vereiste betrouwbaarheidsniveau in te schalen. Deze drie hoofdstukken vormen de kern van de handreiking.

Hoofdstuk 5-9: specifieke diensten

In de hoofdstukken 5 tot en met 9 leest u over specifieke vormen van communicatie of dienstverlening. We gaan in op: machtigingen, applicatie-applicatieverkeer, retourstromen, eenmalig inloggen en ondertekenen.

Bijlagen: wetten, voorbeelden en definities

Bijlage 1 beschrijft het wettelijke kader voor inschaling van diensten op het vereiste betrouwbaarheidsniveau. In bijlage 2 vindt u voorbeelden van de manier waarop wettelijke vereisten en formuleringen zich vertalen naar de digitale praktijk. In bijlage 3 hebben we een lijst met veel gebruikte begrippen opgenomen.

2 Afbakening en context

Waar gaat deze handreiking over?

De betrouwbaarheid van de digitale dienstverlening van de overheid is een groot en complex domein. Immers, de taken van verschillende delen van de overheid verschillen essentieel van elkaar. We kunnen dit domein onmogelijk geheel binnen één handreiking behandelen. In dit hoofdstuk maken we duidelijk waarop we ons wel richten. Binnen deze 'afbakening' gaan we ook kort in op relevante trends en ontwikkelingen. Definities van begrippen, zoals het 'betrouwbaarheidsniveau', vindt u in bijlage 2.

2.1 Afbakening

2.1.1 Om welke diensten gaat het?

In deze handreiking gaan we in op diensten en processen van de overheid aan burgers en bedrijven. Het gaat grofweg om diensten waarbij:

1. een burger of bedrijf voor zichzelf via internet een dienst afneemt en ook zelf de benodigde handelingen uitvoert. Hij bezoekt bijvoorbeeld een website en voert daar een transactie uit of verzendt een e-mail;
2. iemand zelf de benodigde handelingen uitvoert namens een andere (natuurlijke of niet-natuurlijke) persoon ('machtiging');
3. geautomatiseerde systemen met elkaar communiceren zonder directe menselijke tussenkomst.

2.1.2 Alleen voor individuele diensten

Met deze handreiking helpen we vast te stellen wat het vereiste betrouwbaarheidsniveau is voor één bepaalde dienst. Natuurlijk kunt u meer diensten aanbieden. Daarvoor komt u wellicht conform de risicoanalyse in deze handreiking uit op verschillende betrouwbaarheidsniveaus. Het toepassen van risicomitigerende maatregelen in uw dienst kan aanknopingspunten bieden om het aantal betrouwbaarheidsniveaus voor uw organisatie te beperken (langs de dimensie van risicoverlagende aspecten zoals benoemd in hoofdstuk 4).

2.2 Welke trends en ontwikkelingen spelen er nu?

Welke actuele ontwikkelingen en trends zijn relevant voor het betrouwbaarheidsniveau waarop diensten worden aangeboden? We onderscheiden er zes, die hieronder worden toegelicht.

2.2.1 Uitbesteding en externe vertrouwensdiensten

Met deze handreiking gaan we ervan uit dat u een individuele dienst aanbiedt en ook zelf inricht en beheert. Trend is echter dat steeds meer overheidsdienstaanbieders hun digitale vertrouwensdiensten geheel of gedeeltelijk uitbesteden. In dat geval ligt bijvoorbeeld de inrichting of het

beheer van de vertrouwensdiensten bij een externe partij. U als dienstaanbieder stelt daaraan duidelijke eisen. U moet ook goed controle kunnen houden over de dienstverlening van deze externe partij.

Bij uitbesteding blijft u altijd verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, integriteit en vertrouwelijkheid) van uw dienst. U moet dus zelf het vereiste betrouwbaarheidsniveau voor uw dienst vaststellen. Daarnaast moet u strenge eisen stellen aan de betrouwbaarheid en kwaliteit van uw externe leveranciers en hun authenticatieoplossingen. Ook de verantwoording en het toezicht moet u goed regelen. Het maakt daarbij in principe niet uit of u gebruik maakt van een marktpartij of van gemeenschappelijke voorzieningen van de overheid.

Relevantie voor deze handreiking

In deze handreiking geven wij geen toelichting over hoe u kwaliteit en betrouwbaarheid kunt borgen bij een uitbesteding, daarvoor verwijzen wij naar VIR, BIR, IBI, BIG en bijvoorbeeld de richtlijnen die het NCSC opstelt.

2.2.2 Europese verordeningen en NEN-normen

Twee nieuwe Europese verordeningen zijn relevant voor betrouwbaarheidsniveaus. Allereerst is er eIDAS. Dit komt in hoofdstuk 3 verder aan de orde. Daarnaast is er de *Algemene Verordening Gegevensbescherming (AVG)*. Vanaf 25 mei 2018 treedt de AVG formeel in werking. Dan moeten alle overheidsdienstverleners hieraan voldoen.

Algemene Verordening Gegevensbescherming (AVG)

De AVG omvat aangescherpte regels voor bescherming van (bijzondere) persoonsgegevens. Worden die niet nageleefd, dan kunnen hoge boetes volgen. De AVG verschilt van de huidige Nederlandse privacywetgeving volgens de Wet bescherming persoonsgegevens (Wbp). Enkele belangrijke verschillen op een rij:

- De verplichtingen in de AVG zijn op veel punten gedetailleerder uitgewerkt. Ook staat beschreven hoe u aan de norm moet voldoen.
- Er wordt een accent gelegd op verantwoording. Verwerkt u persoonsgegevens, dan moet u het verwerkingsproces niet alleen beschrijven, maar ook zo inrichten dat u kunt aantonen dat u voldoet aan de wet.
- Naast een adequate beveiliging moet u ervoor zorgen dat u ‘privacy impact assessments’ verricht en ‘privacy by design’ toepast. Dit alles hoort u te documenteren.
- U moet veel meer aandacht besteden aan hoe u betrokkenen informeert over de verwerking van hun persoonsgegevens. Ook om te voldoen aan het inzage- en correctierecht zult u processen moeten inrichten.

NEN-normen

Daarnaast zijn er de Nederlandse NEN-normen over authenticatie waar naar verwezen wordt in wet- en regelgeving. Ze zijn een voorbeeld van hoe in specifieke sectoren normen van invloed zijn op het benodigde betrouwbaarheidsniveau. Zo gaat het in de NEN 7510 bijvoorbeeld om de Wet gebruik burgerservicenummer in de zorg (Wbsn-z). Deze norm noemt tweefactorauthenticatie[1] om toegang te krijgen tot een medisch informatiesysteem: 'Informatiesystemen die patiëntgegevens verwerken, behoren authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken.'

2.2.3 Overheden verwerken steeds meer bijzondere persoonsgegevens (met of zonder beroepsgeheim)

Een trend is dat steeds meer bijzondere persoonsgegevens worden verwerkt door (decentrale) overheden. Ook verwerken overheden meer gegevens die door een beroepsgeheim worden beschermd (zie kader).

Voorbeeld: decentralisatie zorg en welzijn

Verschillende vormen van zorg en welzijn zijn gedecentraliseerd naar gemeentelijke diensten. Daardoor verwerken gemeenten inmiddels steeds meer gezondheidsgegevens en andere bijzondere gegevens. Ze krijgen bovendien vaker dan voorheen te maken met informatie die onder het medisch beroepsgeheim valt.

Een ander voorbeeld is de gegevensverwerking voor de jeugdzorg door gemeenten. Voor jeugdzorgaanbieders geldt een dossierverplichting. Die is vergelijkbaar met de dossierverplichting in de Wet Geneeskundige BehandelingsOvereenkomst (WGBO) voor zorgaanbieders in een behandelrelatie. Daarbij is ook sprake van medisch beroepsgeheim. Dit gaat over alles wat de zorgverlener van de patiënt weet of bijhoudt in het medisch dossier. Gemeenten moeten daarnaast gegevens verwerken rond de toegang en de afrekening van jeugdzorg.

Relevantie voor deze handreiking

Voor deze handreiking is deze trend relevant. Het laat zien dat de behoefte aan hogere betrouwbaarheidsniveaus toeneemt.

[1] Tweefactorauthenticatie betekent dat je alleen toegang krijgt met iets wat je weet (een wachtwoord of code) samen met iets wat je hebt (een pasje of token).

2.2.4 Overheden verwerken steeds meer gegevens digitaal

Overheden verwerken steeds meer gegevens digitaal. Ook als het gaat om de interactie met burgers en bedrijven. Programma's als Digitaal 2017 versterken deze trend. In die trend zien we dat (vrijwel) alle dienstverlening van de overheid digitaal wordt aangeleverd, nu vaak nog naast de 'klassieke' vorm van dienstverlening (aan de balie, schriftelijk). Digitaal wordt bovendien steeds meer het *voorkeurskanaal* van de overheid. De verwachting is dat digitaal daar bovenop steeds vaker als enige mogelijkheid wordt aangeboden, zoals bij de aangifte Inkomstenbelasting en bij aanbestedingen. Die laatste beweging zal door de wetgever steeds van dienst tot dienst overwogen worden.

Relevantie voor deze handreiking

De Nationale Ombudsman stelde in het rapport 'Het verdwijnen van de blauwe envelop' (5 april 2016) dat 'mensen die moeite hebben met de digitalisering hierbij adequate ondersteuning moeten kunnen krijgen'. Dit vraagt, naast enige terughoudendheid met het verplicht stellen van het digitale kanaal, vooral ook om een goede voorziening voor de machtiging van burgers aan medeburgers en organisaties. Denk aan organisaties die als intermediair optreden. Inmiddels is Logius bezig om een burger-organisatiemachtiging te realiseren in DigiD Machtigen.

2.2.5 Dienstaanbieders 'in het BSN-domein' maken gebruik van vertrouwensdiensten uit de markt

Dienstaanbieders in het BSN-domein maken steeds meer gebruik van authenticatiemiddelen en vertrouwensdiensten uit de markt. Dus ook voor de authenticatie van burgers en niet meer uitsluitend voor organisaties. Vooralsnog betreft dit vooral eHerkenning en de proeven in het BSN-domein met iDIN (inloggen met de bankpas bij de Belastingdienst) en Idensys.

Uiteraard speelt ook hier dat de dienstaanbieder uiteindelijk verantwoordelijk is en blijft voor de algehele betrouwbaarheid van zijn dienst en de toegepaste authenticatieoplossing.

Relevantie voor deze handreiking

Deze trend is geen aanleiding om de scope van deze handreiking aan te passen. Het is een trend die reeds was voorzien bij de eerste opzet van deze Handreiking.

2.2.6 Authentieke gegevens uit basisregistraties worden verplicht gebruikt

Authentieke gegevens uit basisregistraties moeten verplicht worden gebruikt door alle organisaties met een publiekrechtelijke taak. Als dit plaatsvindt vraagt de betrokken organisatie die gegevens dan niet meer uit bij burger of bedrijf. Het gaat om gegevens uit bijvoorbeeld de Basisregistratie Personen (*BRP*), het Handelsregister (*HR*), de Basisregistratie Adressen en Gebouwen (*BAG*), de Basisregistratie Kadaster (*BRK*), de Basisregistratie Voertuigen (BRV, ook Kentekenregister), de Basisregistratie Inkomen (*BRI*) en de Basisregistratie Waardering Onroerende Zaken (*WOZ*). Hierdoor neemt het belang van een voldoende hoog betrouwbaarheidsniveau toe voor de toegang tot de basisregistraties.

Relevantie voor deze handreiking

Voor de handreiking is deze trend relevant, omdat daardoor vaker een hoger betrouwbaarheidsniveau vereist is. We maken daarbij onderscheid tussen twee situaties. Je kunt allereerst slechts raadplegen, in welk geval de geraadpleegde gegevens en de hierover verstuurde berichten vooral heel betrouwbaar moeten zijn. Maar een tweede casus is dat de basisregistratie wordt gebruikt èn er een wijziging in die basisregistratie wordt aangebracht. In dat geval is het van belang dat de gebruiker met hoge betrouwbaarheid is geauthenticeerd.

3 Uitgangspunten

Vereenvoudigde risicoanalyse op basis van eIDAS

In dit hoofdstuk beschrijven we de uitgangspunten van de handreiking. Dat zijn:

- De kern van de handreiking is een vereenvoudigde, makkelijk hanteerbare risicoanalyse.
- De handreiking hanteert de eIDAS-betrouwbaarheidsniveaus.
- De handreiking hanteert de eIDAS-vertrouwensdiensten (zie hoofdstuk 9 en delen van hoofdstuk 7).

Dankzij deze benadering kunt u betrekkelijk eenvoudig een globale inschatting maken van de risico's van uw specifieke dienst. Zo bepaalt u snel het vereiste betrouwbaarheidsniveau.

3.1 Vereenvoudigde risicoanalyse

In verschillende landen gebeurt het inschalen van betrouwbaarheidsniveaus op basis van risicoanalyses.[2] Ook de Verenigde Staten hebben deze benadering gekozen. De Office of Management and Budget heeft hiervoor in 2006 de EAuthentication Guidance for Federal Agencies[3] vastgesteld. Daarin is sprake van een gedetailleerde risicoanalyse, wat te maken heeft met de aansprakelijkheidscultuur in de Verenigde Staten.

Systematiek op basis van objectieve criteria

In Nederland schiet een dergelijke kostbare, tijdrovende en versnipperde benadering zijn doel voorbij. We gaan liever uit van de kenmerken van processen en diensten als basis voor het vaststellen van het gewenste betrouwbaarheidsniveau. We hebben in deze handreiking gezocht naar een systematiek om risico's generiek in te schatten. We maakten een inschatting van de te beschermen waarde aan de hand van een aantal objectieve (of objectiveerbare) criteria en belangen. Denk daarbij aan wettelijke eisen, de aard van de gegevens die uitgewisseld worden (persoonsgegevens of niet) en het economisch of maatschappelijk belang van een dienst. Vervolgens schatten we de mogelijke schade in als authenticatie niet op de juiste wijze zou plaatsvinden.

[2] Zie bijvoorbeeld in Spanje: MAGERIT, Methodology for Information System Risk Analysis and Management; Ministerio de Administraciones Públicas, June 2006, *http://rminv.enisa.europa.eu/methods/m_magerit.html*

[3] *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800632.pdf*

Aannames over (IT)-veiligheid

Verder namen we aan dat de desbetreffende diensten vanuit vergelijkbare online omgevingen worden geleverd en vergelijkbare kwetsbaarheden hebben. Voor het voorkomen van deze kwetsbaarheden is de Norm ICT-beveiligingsassessments DigiD[4] van belang en de richtlijnen van het Nationaal Cyber Security Centrum (NCSC) waarop deze zijn gebaseerd[5]. Verder gingen we ervan uit dat de diensten ten minste de norm voor DigiD implementeren.

Daarnaast hielden we rekening met het feit dat er ook 'off line' maatregelen genomen kunnen worden om de betrouwbaarheid van gegevens te verzekeren en de kans op verwisselde of vervalste identiteit te reduceren. Denk bijvoorbeeld aan terugkoppeling via een brief naar het woonadres of fysieke verschijning aan een loket.

Onze risicoanalyse voor betrouwbaarheidsniveaus kan gezien worden als een specifieke invulling van een deel van een bredere risicoanalyse voor informatiebeveiliging. Met onze benadering sluiten we bewust aan bij de voorschriften voor informatiebeveiliging in Nederland.

Lees meer over onze methodiek

Onze methodiek presenteren we in hoofdstuk 4. Doorloop deze vereenvoudigde risicoanalyse helemaal om het betrouwbaarheidsniveau dat u nodig heeft te bepalen. Wilt u een eerste indruk van het juiste betrouwbaarheidsniveau? Kijk dan naar de voorbeelden in paragraaf 4.4.

Nieuwe vormen van diensten

Digitale dienstverlening verandert continu. Zo zijn nieuwe vormen van diensten in opkomst, zoals:

- diensten via een app, zoals de Student App van DUO of de Aangifte IB App van de Belastingdienst;
- continue gegevensuitwisseling op basis van specifieke apparaten, al dan niet gekoppeld aan een vorm van een abonnement. Denk bijvoorbeeld aan smart meters, devices in auto's die voortdurend gegevens uitwisselen, toepassingen in de medische sfeer waar gebruikers op geregelde basis meetgegevens registreren, inzien en bewerken.

[4] Versie 1.0 d.d. 21 februari 2012 zie *www.logius.nl/ondersteuning/digid/beveiligingsassessments/*

[5] Waarvan huidige versie 2.0 is terwijl de Norm ICT-beveiligingsassessments DigiD nog gebaseerd is op versie 1.0.

Momenteel hebben deze ontwikkelingen nog niet geleid tot echt nieuwe soorten overheidsdiensten. De huidige generatie apps biedt vergelijkbare diensten als die via websites en portals geboden worden. Het is echter waarschijnlijk dat ook heel nieuwe toepassingen ontstaan en dat dit de beoordeling van betrouwbaarheidsniveaus verandert. Momenteel is het gebruik van deze toepassingen nog gering. Voor deze handreiking leidt deze ontwikkeling daarom op dit moment niet tot wijzigingen.

3.2 eIDAS-verordening als basis

Vanaf 1 juli 2016 is de Europese eIDAS-verordening van kracht. eIDAS legt criteria vast voor de betrouwbaarheidsniveaus van authenticatiemiddelen. Er zijn drie niveaus: laag, substantieel en hoog[6]. Met deze verordening is er een wettelijk kader om betrouwbaarheidsniveaus te bepalen voor digitale overheidsdiensten. In deze vierde versie van de handreiking nemen we eIDAS voor het eerst als basis[7]. Zie voor een verdere inleiding op de verordening bijlage 1.

De drie niveaus van eIDAS leggen we hieronder uit. De uitleg helpt u om deze handreiking toe te passen.

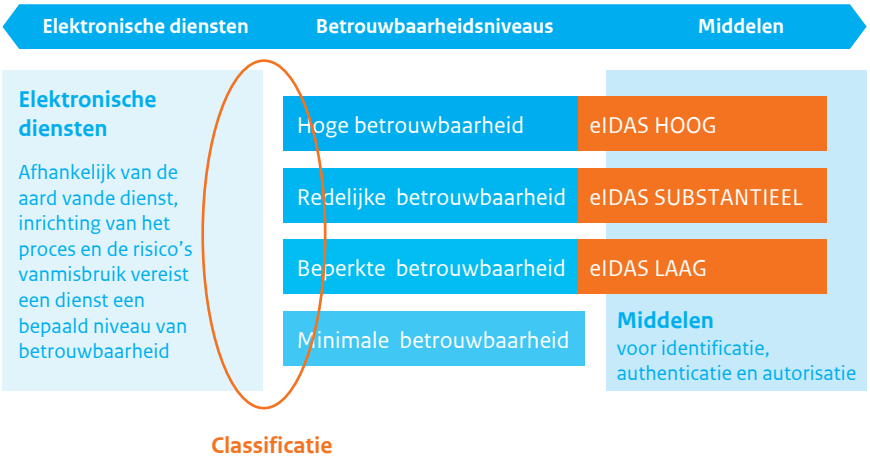
Alleen voor authenticatie

eIDAS richt zich alleen op de authenticatie van burgers en bedrijven en dan vooral als het gaat om webportalen. Voor andere zaken, zoals machtigingen en applicatieapplicatieverkeer, zijn er nauwelijks algemeen geaccepteerde standaarden voorhanden voor een indeling in betrouwbaarheidsniveaus. In deze handreiking geven we daar echter wel een nadere invulling aan.

[6] Tot en met versie 3 van deze handreiking was er nog geen sprake van een wettelijk kader. In plaats daarvan werd gebruikgemaakt van het STORK-classificatiemodel.

[7] We hanteren in deze handreiking eIDAS ook voor het nationale betrouwbaarheidsniveau van diensten, hoewel eIDAS strikt genomen slechts de grensoverschrijdende authenticatie regelt en de daarbij te erkennen authenticatiemiddelen.

Figuur 2. *De handreiking gaat over het classificeren van elektronische diensten om het gewenste betrouwbaarheidsniveau, met name van authenticatie, te bepalen.*



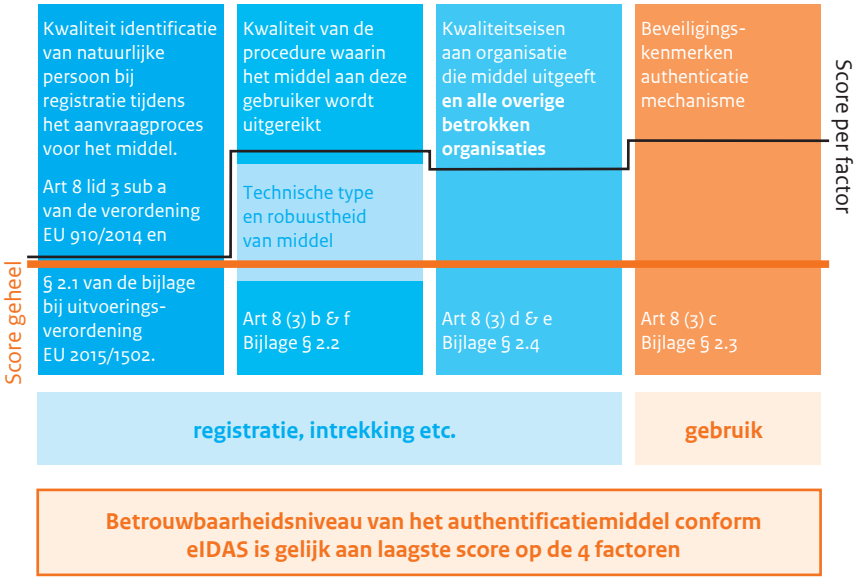
3.3 eIDAS: drie betrouwbaarheidsniveaus

Om het betrouwbaarheidsniveau te bepalen hanteert eIDAS minimumeisen per niveau. eIDAS stelt daarbij de volgende vragen:

- Hoe goed is de **identiteitsverificatie** van iemand die een middel aanvraagt?
- Hoe goed is de **procedure** waarin het middel aan een gebruiker
- wordt uitgereikt?
- Wat is de kwaliteit van de **organisaties** die betrokken zijn bij het uitreiken van het middel en de registratie?
- Wat zijn de **technische specificaties** van het authenticatiemiddel?
- Hoe werkt het **authenticatiemechanisme** waarmee de gebruiker zich bij een digitale dienst identificeert?

Deze factoren worden eerst los beoordeeld. Vervolgens wordt het uiteindelijke betrouwbaarheidsniveau van het authenticatiemiddel bepaald door de laagste score voor de individuele factoren. In onderstaande figuur is dit verbeeld.

Figuur 3. *eIDAS geeft vier factoren om een authenticatiemiddel op te scoren. De laagste score bepaalt het uiteindelijke niveau van het authenticatiemiddel.*



Aanvullende eisen

Naast de genoemde eisen stelt eIDAS ook eisen aan:
de minimale reeks van persoonsgegevens die voor de identificatie gebruikt moet worden;

- de gebruikersvoorwaarden;
- de vernieuwing van het middel;
- de informatiebeveiliging;
- (onafhankelijke) audits;
- de aansprakelijkheid.

Niveau 1: eIDAS laag

Voor eIDAS geldt als eerste minimumeis voor de **identiteitsverificatie** dat de identiteitsgegevens die de gebruiker opgeeft, gecontroleerd kunnen worden in een basisregistratie. In de Nederlandse situatie gaat het in de praktijk om de Basisregistratie Personen (BRP). De controle van deze basisregistratie moet daadwerkelijk worden uitgevoerd. Maar de gebruiker meldt zich niet fysiek in het registratieproces.

Een **middel** met éénfactorauthenticatie volstaat. Denk bijvoorbeeld aan een combinatie van een gebruikersnaam en wachtwoord of een unieke code die de gebruiker ontvangt van een vertrouwde partij.

De **doelstelling** van eIDAS laag is om het risico van misbruik of wijziging van de identiteit te verkleinen. Dit gebeurt door vast te stellen dat de gebruiker een uniek identificeerbare persoon is, iemand bij wie bij de overheid gecontroleerd heeft dat hij bestaat. Maar voor toepassing in digitale diensten geldt een beperkte mate van vertrouwen. Het is niet helemaal zeker dat de persoon die zich in de elektronische dienst meldt echt diegene is waar u als dienstverlener de identiteit van krijgt doorgegeven.

DigiD (basis) is een **voorbeeld** van een middel op het niveau eIDAS laag.

Lager dan eIDAS laag
Veel authenticatiemiddelen voldoen niet aan de eisen voor eIDAS laag. Het zijn niveau 1-middelen volgens STORK en ISO29015[8]. Een voorbeeld is een e-mail met daarin een verificatielink die de aanvrager slechts hoeft aan te klikken om het authenticatiemiddel in gebruik te nemen.

Niveau 2: eIDAS substantieel

Voor eIDAS substantieel zijn striktere methoden voor de **identiteitsverificatie** nodig. Als een gebruiker dit middel aanvraagt, moet daadwerkelijk vastgesteld worden dat hij een geldig, officieel document bezit met dezelfde identiteitsgegevens die gecontroleerd kunnen worden in een basisregistratie. Deze controle[9] mag worden uitbesteed of op afstand plaatsvinden. De controle moet een substantiële mate van vertrouwen bieden.

Als type **middel** is tweefactorauthenticatie vereist. Het middel moet zo ontworpen zijn dat het alleen onder controle van de gebruiker gebruikt kan worden. Het mag niet mogelijk zijn dat het per ongeluk of ongemerkt door een ander kan worden gebruikt.

Ten slotte geldt voor eIDAS substantieel een eis voor het **authenticatiemechanisme** zelf. Er moet sprake zijn van dynamische authenticatie: de (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik. Dit biedt extra bescherming tegen fraudeurs die gegevens willen stelen en hergebruiken. Een voorbeeld daarvan zijn onetimepasswordtokens.

[8] En ook als zodanig in vorige versies van de handreiking beschreven is.

[9] De precieze interpretatie van de eisen die aan deze controle gesteld worden is ongetwijfeld nog een onderwerp van nadere ontwikkeling en afstemming tussen de lidstaten.

Voorbeelden van middelen op het niveau van eIDAS substantieel zijn de tokens van banken (aannemende dat de identiteitsverificatie in het aanvraag- en uitfiteproces voldoende betrouwbaar was).

Niveau 3: eIDAS hoog

Voor eIDAS hoog moet de gebruiker bij de **identiteitsverificatie** in aanvulling op de eisen bij niveau substantieel ten minste eenmaal fysiek verschijnen.

Verder moet het **middel** goed beschermd zijn tegen misbruik door anderen. Denk bijvoorbeeld aan een cryptografisch token, dat echter ook nog een PIN-code vereist, voordat het gebruikt kan worden. Deze PIN-code biedt een extra bescherming tegen misbruik door derden.[10]

[10] De eisen zijn bijna net zo streng als die voor middelen voor gekwalificeerde elektronische handtekeningen. Anders dan bij het eerder gehanteerde STORK, is eIDAS hoog niet gelijkgesteld aan de gekwalificeerde elektronische handtekening c.q. de daarbij gehanteerde techniek.

4 Inschaling van diensten

Hoe kiest u het juiste betrouwbaarheidsniveau?

In hoofdstuk 3 hebben we uitgangspunten geformuleerd voor een classificatiemodel om e-overheidsdiensten in te schalen op de verschillende betrouwbaarheidsniveaus. In dit hoofdstuk komt dit model aan bod. U kunt het zien als een eenvoudige risicoanalyse. De keuze voor een betrouwbaarheidsniveau hangt af van een aantal criteria. Deze criteria hebben te maken met:

- de wettelijke eisen aan de dienst;
- de aard van de gegevens en de verwerking ervan;
- de potentiële schade bij misbruik van de gegevens.

Classificatiemodel in een tabel

Op pagina 29 hebben we de criteria overzichtelijk samengevat in een tabel. Dit is het classificatiemodel. Hiermee maakt u een eerste inschatting van het betrouwbaarheidsniveau. Lees vervolgens de toelichting op de criteria in dit hoofdstuk voor een nauwkeurigere beoordeling per criterium.

Analyse op basis van één scenario

In onze systematiek maken we geen inschatting van de kans op of de impact van een dreiging. In plaats daarvan gaan we uit van één scenario, het zogeheten referentiescenario. Hiervoor maken we aannames over bijvoorbeeld de kwaliteit van de ITbeveiliging en het achterliggende proces van de dienst.

Afwijking? Voer een volledige analyse uit

Het classificatiemodel kent een aantal correctiefactoren. Die zijn relevant wanneer de dreiging wezenlijk afwijkt van het referentiescenario en bijvoorbeeld lager of hoger is. Constateert u een hoger dreigingsniveau? Houd het dan niet bij deze vereenvoudigde risicoanalyse, maar voer een volledige risicoanalyse uit.

4.1 Classificatiemodel en criteria

In het classificatiemodel ziet u verschillende criteria. Ze zijn gekoppeld aan de betrouwbaarheidsniveaus. Bekijk vervolgens welke criteria van toepassing zijn op uw dienst. Sommige criteria scoren misschien laag, andere substantieel. De hoogste score bepaalt het gewenste betrouwbaarheidsniveau voor uw gehele dienst.

De volgende criteria zijn relevant om het betrouwbaarheidsniveau van uw dienst in te schalen:

1. Worden **persoonsgegevens** verwerkt (zie subparagraaf 4.1.1)? Zo ja:
   - wat is de aard van de te beschermen gegevens? Worden er ook bijzondere persoonsgegevens verwerkt? Wordt het burgerservicenummer (BSN) of bijvoorbeeld medische gegevens verwerkt?
   - wat zijn de relevante kenmerken van de verwerking zelf?
2. Wat zijn de **rechtsgevolgen** van het gebruik van uw dienst (zie subparagraaf 4.1.2)?
3. Worden er **basisregistratiegegevens** gewijzigd door uw dienst (zie subparagraaf 4.1.3)?
4. Hoe groot is het **economisch belang** bij uw dienst (zie subparagraaf 4.1.4)?
5. Hoe groot is het **publiek belang** bij uw dienst (zie subparagraaf 4.1.5)?

Wat als een middel van het juiste betrouwbaarheidsniveau niet algemeen beschikbaar is?

Met name bij elektronische dienstverlening aan burgers kan het voorkomen dat de doelgroep in kwestie nog niet in voldoende mate kan beschikken over een authenticatiemiddel met een voldoende betrouwbaarheidsniveau. De facto spreken we nu dan over het beschikbare betrouwbaarheidsniveau voor DigiD, op de iets langere termijn ook over de beschikbaarheid van andere tot het publieke domein toegelaten authenticatiemiddelen van private partijen.

In het geval dat het gewenste betrouwbaarheidsniveau nog niet (in voldoende mate) beschikbaar is, gelden de volgende vuistregels:

- Kies voor elektronische dienstverlening, waarbij u het eerstvolgende lagere betrouwbaarheidsniveau verplicht, dat wèl (in voldoende mate) beschikbaar is.
- Stimuleer in dit geval tevens het gebruik van een authenticatiemiddel van het gewenste betrouwbaarheidsniveau, indien burgers hier wel over kunnen beschikken maar dit nog niet gebruiken. Zo kan een doelgroep ook geleidelijk toegroeien naar het juiste betrouwbaarheidsniveau.
- Neem compenserende maatregelen, die het extra risico acceptabel maken, dat volgt uit de keuze van het lagere betrouwbaarheidsniveau.

Hieronder geven we eerst de tabel die aangeeft hoe de criteria leiden tot de keuze van een betrouwbaarheidsniveau. In de daarna volgende paragrafen behandelen we elk criterium afzonderlijk in detail. Let op, het betreft hier *indicaties* van een betrouwbaarheidsniveau dat van toepassing is in een standaard- of referentiescenario (zie paragraaf 4.2) In uw specifieke situatie kan er sprake zijn van correctiefactoren (zie paragraaf 4.3).

Criteria	Betrouwbaarheidsniveau (volgens eIDAS)
• Geen verwerking persoonsgegevens (klasse 0) • Geen BSN • Geen rechtsgevolg • Geen wijzigingen in basisregistratie • Economisch belang nihil • Publiek belang niet van toepassing	Geen eisen aan authenticatie
• Persoonsgegevens maximaal klasse 1 • BSN zelf verstrekt of impliciet in authenticatie • Mogelijk indirect rechtsgevolg • Alleen wijziging van niet risicovolle basisregistratiegegevens • Gering economisch belang • Publiek belang laag	Laag
• Persoonsgegevens maximaal klasse 2 • Verzwarende factor voor persoonsgegevens bovenop klasse 1 (aard verwerking) • BSN verwerkt in combinatie met aanvullende persoonsgegevens • Direct rechtsgevolg • Opgeven of wijzigen van basisregistratiegegevens die niet onder hoog vallen • Gemiddeld economisch belang • Gemiddeld publiek belang	Substantieel
• Persoonsgegevens klasse 3 • Verzwarende factor voor persoonsgegevens bovenop klasse 2 (aard verwerking) • BSN verwerkt in combinatie met aanvullende persoonsgegevens • Direct creëren, muteren of effectief beëindigen van (authentieke) basisregistratiegegevens • Groot economisch belang • Groot publiek belang	Hoog

4.1.1 Worden persoonsgegevens verwerkt met uw dienst?

Grofweg zijn er in deze handreiking twee scenario's denkbaar. Er worden gegevens verwerkt van bedrijven of instellingen. Of er worden (ook) persoonsgegevens verwerkt. Dit laatste is in veel gevallen aan de orde.

Persoonsgegevens vragen om beveiliging

Het verwerken van persoonsgegevens vraagt om een breed spectrum van beveiligingsmaatregelen. U moet er zeker van zijn dat alleen de bevoegde personen bij de persoonsgegevens kunnen, bijvoorbeeld door authenticatie 'aan de poort'.

Criteria voor risicoanalyse

Wat is het risico van een persoonsgegevensverwerking? Het belangrijkste criterium is de **aard van de persoonsgegevens**. Secundair gaat het om de

aard (wijze) van de verwerking. Zo staat het ook in de Richtsnoeren voor Beveiliging van Persoonsgegevens van de Autoriteit Persoonsgegevens (AP). De richtsnoeren zijn een nadere invulling van de beveiligingsverplichting in artikel 13 van de Wet bescherming persoonsgegevens (Wbp).

Hoe maken we het criterium persoonsgegevens toepasbaar?
Om uit de voeten te kunnen met het criterium 'aard van de persoonsgegevens' delen we persoonsgegevens in verschillende klassen in. Deze indeling is geïnspireerd op een publicatie uit 2001 van de Registratiekamer, de voorloper van de AP, over de beveiliging van persoonsgegevens (hierna: AV 23). De richtsnoeren van de AP vervangen AV 23. In de overwegingen in de richtsnoeren komen aspecten uit de AV 23 echter wel weer naar voren.

Nieuwe richtsnoeren
In de recente richtsnoeren is gekozen voor een methodiek die aansluit bij de gangbare praktijk van de informatiebeveiliging. Ze bieden u als verantwoordelijke de flexibiliteit om beveiligingsmaatregelen te treffen die in uw situatie het meest passend zijn. Dat maakt de richtsnoeren minder statisch dan het kader dat de AV 23 bood. Het gaat erom dat per geval alle omstandigheden een rol spelen. U moet ze uiteindelijk allemaal meenemen in uw risicoweging.

Consequentie voor deze handreiking
De AV 23 kent een bepaald risico toe aan de aard van gegevens bij verwerking van die gegevens. Eerdere versies van deze handreiking waren gerelateerd aan deze risico-indeling. Deze indeling blijft relevant, ook in de huidige richtsnoeren. Daarom wijken we in deze versie van de handreiking niet af van de risico-inschatting die samengaat met bepaalde gegevenssoorten. Tenzij er sprake is van een andere ontwikkeling of een verbeterd inzicht. We baseren ons op aanwijzingen in onderzoek van de AP en op de recente richtsnoeren.

Voor de goede orde: de indeling van persoonsgegevens in klassen is niet relevant voor het criterium 'aard van de verwerking' (zie pagina 34).

Verplichting: voldoe aan de Wet bescherming persoonsgegevens

Los van gegevenssoorten en hoe u die met deze handreiking inschaalt, bepaalt artikel 13 van de Wbp de noodzaak om een risicoanalyse op de informatiebeveiliging uit te voeren. U moet immers integraal aan de Wbp voldoen. Het gaat hier dus om de totale informatiebeveiliging, waarbij deze handreiking slechts een (vereenvoudigde) risicoanalyse biedt voor de authenticatie (als onderdeel van die informatiebeveiliging).

Zorg voor een passende beveiliging

De Wbp eist passende beveiligingsmaatregelen voor persoonsgegevens. Maar wat is 'passend'? In de richtsnoeren staat hoe de AP bij het onderzoeken en beoordelen van de beveiliging van persoonsgegevens de beveiligingsnormen uit de Wbp toepast. De richtsnoeren leggen daarmee een link tussen het juridisch domein en het domein van de informatiebeveiliging. Gebruik voor een passende beveiliging daarom de richtsnoeren samen met algemeen geaccepteerde beveiligingsstandaarden voor informatiebeveiliging, zoals de ISO/CIE 27001 en de ISO/CIE 27002.

AP: aanwijzingen voor het bepalen van het betrouwbaarheidsniveau

De AP geeft in de richtsnoeren concrete aanwijzingen over wat het juiste betrouwbaarheidsniveau is bij bepaalde soorten gegevensverwerking. Het gaat erom dat u weet wat de risico's (op een negatief effect op de persoonlijke levenssfeer) voor de betrokkene(n) zijn bij gegevensmisbruik. Vervolgens maakt u een vertaalslag van die risico's: welke betrouwbaarheidseisen moeten die risico's voorkomen? Voor deze vertaalslag moet u de gevolgen inzien van alle mogelijke vormen van verlies of onrechtmatige verwerking van persoonsgegevens. Denk bijvoorbeeld aan stigmatisering of uitsluiting, reputatieschade, schade aan de gezondheid of blootstelling aan (identiteits)fraude en inbreuk op de privacy.

Bepalend: aard van de gegevens en aard van de verwerking

Om de betrouwbaarheidseisen vast te stellen zijn de risico's voor één individuele betrokkene maatgevend. De schade die hij ondervindt door verlies of onrechtmatige verwerking van zijn persoonsgegevens, hangt af van de aard van de gegevens en de aard van de verwerking. Stel daarom voor de beoordeling van het betrouwbaarheidsniveau de volgende vragen:

1. Is er sprake van een passend beveiligingsniveau gezien de risico's rond **de aard van de te beschermen gegevens**?
2. Is er sprake van een passend beveiligingsniveau gezien de risico's rond **de (aard van de) verwerking**?

Hieronder gaan we dieper in op deze vragen.

Ad 1: Is er sprake van een passend beveiligingsniveau gezien de risico's rond de aard van de te beschermen gegevens?

De AP noemt in de richtsnoeren onder andere gegevens met een hoger en hoog risico: Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp.

1. Het gaat om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens in verband met een opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

- De Wbp vat begrippen zoals ‘gezondheid’ of ‘levensovertuiging’ ruim op. Zo vallen onder ‘gezondheidsgegeven’: ‘alle gegevens die de geestelijke of lichamelijke gezondheid van een persoon betreffen’. In de toelichting staat dat alleen al het gegeven dat iemand ziek is een gezondheidsgegeven is, hoewel dat gegeven op zichzelf nog niets zegt over de aard van de aandoening.

2. Gegevens over de financiële of economische situatie van de betrokkene.
3. (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over werkprestaties of relatieproblemen.
4. Gegevens die betrekking hebben op mensen uit kwetsbare groepen.
5. (Andere) gegevens die kunnen worden misbruikt voor (identiteits)fraude. Denk bijvoorbeeld aan biometrische gegevens, kopieën van identiteitsbewijzen en aan het BSN.

Apart criterium: verwerking van het BSN

Naast de verwerking van persoonsgegevens geldt de verwerking van het BSN als apart criterium. Het BSN is op grond van artikel 24 van de Wbp een wettelijk identificatienummer. Het mag alleen worden gebruikt voor doeleinden zoals in de wet staat. Dit komt omdat het BSN bij uitstek zorgt voor de koppeling van persoonsgegevens, zowel binnen als tussen organisaties.

BSN: welke betrouwbaarheidsniveaus horen hierbij?

Betrouwbaarheidsniveau: geen

- Het BSN wordt niet verwerkt.

Betrouwbaarheidsniveau: laag

- Het BSN wordt uitsluitend opgegeven door de gebruiker.
- Mogelijk wordt het teruggekoppeld (eventueel in combinatie met een beperkt aantal andere persoonsgegevens van maximaal klasse 1 (zie kader), bijvoorbeeld een naam, zodat u zeker bent over de juistheid van het opgegeven BSN).
- Hier valt ook de ‘impliciete’ opgave van het BSN onder en andere situaties waarbij de gebruiker het BSN uitwisselt met u, maar het BSN niet ziet. Dat gebeurt bijvoorbeeld bij DigiD of via het toekomstige BSN-koppelregister (zie kader).

Betrouwbaarheidsniveau: substantieel

- Het BSN wordt in samenhang met aanvullende persoonsgegevens verwerkt.

Wat is het BSN-koppelregister?
Het BSN-koppelregister [BSN-K] is een overheidsvoorziening om authenticatiemiddelen van private en publieke partijen te koppelen aan het BSN van de houder van het authenticatiemiddel. De identificatoren die hierbij worden verwerkt, uitgewisseld en mogelijk getoond, zijn pseudoniemen maar hebben bij publieke dienstverleners het BSN als basis. Het BSN is dan weliswaar 'onzichtbaar' voor de burgers die de dienst afnemen, maar het komt wel beschikbaar voor u als dienstverlener.

De systematiek van pseudonimisering door middel van het BSN-koppelregister voldoet aan alle relevante eisen voor de privacyvriendelijke gebruik van pseudoniemen. Het BSN-K valt verder buiten de scope van de elektronische dienstverlening en dus ook buiten de scope van deze handreiking.

Aard van persoonsgegevens: welke betrouwbaarheidsniveaus horen hierbij?

Betrouwbaarheidsniveau: geen
Klasse 0 persoonsgegevens:
- Er worden geen persoonsgegevens verwerkt.
- Het gaat om openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Denk bijvoorbeeld aan gegevens uit telefoonboeken, brochures en websites.

Betrouwbaarheidsniveau: laag
Klasse I persoonsgegevens (basis)
- Er is sprake van een beperkt aantal (niet-bijzondere) persoonsgegevens per individu.
- Er is sprake van één type vastlegging, bijvoorbeeld één lidmaatschap, arbeidsrelatie of klantrelatie.

Betrouwbaarheidsniveau: substantieel
Klasse II persoonsgegevens (verhoogd risico)
- Er worden bijzondere persoonsgegevens gebruikt (zoals genoemd in artikel 16 van de Wbp) of financieel-economische gegevens van de betrokkene.

Betrouwbaarheidsniveau: hoog
Klasse III persoonsgegevens (hoog risico)
- Er worden gegevens van opsporingsdiensten gebruikt, gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde, geheimhoudingsplicht op rust en gegevens die onder het beroepsgeheim vallen (zoals medische gegevens) in de zin van artikel 9, vierde lid, van de Wbp.

Ad 2: Is er sprake van een passend beveiligingsniveau gezien de risico's rond de (aard van de) verwerking?

Zoals aangegeven willen we nagaan of de aard van de verwerking leidt extra risico's, die ertoe leiden om een hoger betrouwbaarheidsniveau te vereisen. Analoog aan de AV23 bezien we de volgende factoren:

1. Verwerkt uw dienst een groot aantal gegevens per individu (meerdere vastleggingen, meerdere doelen), zodat verlies en onrechtmatige verwerking tot een bovenmatige inbreuk op de persoonlijke levenssfeer leidt? Het uitlekken van een compleet medisch dossier leidt over het algemeen bijvoorbeeld tot een grotere inbreuk dan het uitlekken van een herhaalrecept.
2. Doel of doelen waarvoor de persoonsgegevens worden verwerkt. Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter.
3. De mate waarin de gegevens bruikbaar zijn voor misbruik. Denk vooral aan de mogelijkheid van identiteitsfraude.

Als één van deze zaken aan de orde is voor gegevens tot klasse 2, dan kiezen we het betrouwbaarheidsniveau dat past bij de naasthogere klasse (zie de tabel).

4.1.2 Wat zijn de rechtsgevolgen van het gebruik van uw dienst?

Het gebruik van uw dienst kan rechtsgevolgen hebben. Hier is sprake van als uw dienst zijn grondslag vindt in wetgeving en leidt tot rechtshandelingen. Denk bijvoorbeeld aan een besluit dat vatbaar is voor bezwaar en beroep. Maar bij uw dienst kan ook slechts sprake zijn van feitelijk handelen. Denk aan het verstrekken van inlichtingen. In dat geval is uw dienst niet op rechtsgevolg gericht.

Er is nog een derde soort dienst. Die is gericht op feitelijk handelen, zoals het registreren van afvalcontainers op naam en adres. Maar dit kan vervolgens tot rechtsgevolg leiden: de gegevens gebruikt u mogelijk voor handhaving. In dat geval spreken we over indirect rechtsgevolg.

Rechtsgevolg: welke betrouwbaarheidsniveaus horen hierbij?

Betrouwbaarheidsniveau: geen
- Er is geen rechtsgevolg.

Betrouwbaarheidsniveau: laag
- Er is sprake van indirect rechtsgevolg.

Betrouwbaarheidsniveau: substantieel of hoog
- Er is sprake van rechtsgevolg.

4.1.3 Worden er basisregistratiegegevens gewijzigd door uw dienst?

Gegevens in een basisregistratie vormen een bijzondere categorie. Denk bijvoorbeeld aan gegevens uit de burgerlijke stand, geboorteregistratie en de gemeentelijke basisregistratie van het woonadres. Als deze gegevens worden verwerkt, kunnen de gevolgen groot zijn. Deze gegevens worden immers aan een grote groep afnemers verstrekt.

Onder basisregistratiegegevens vallen authentieke gegevens. Elke opname of mutatie daarvan moet met de grootste zekerheid en zorgvuldigheid gebeuren, want afnemers moeten deze authentieke gegevens zonder nadere controle overnemen en kunnen vertrouwen (het zogenoemde verplicht gebruik).

Over het algemeen past bij deze categorie het betrouwbaarheidsniveau hoog. Maar er is een uitzondering. Worden er gegevens verwerkt die bestemd zijn voor opname in een basisregistratie maar vindt daarop nog een aanvullende controle plaats door de instantie die verantwoordelijk is voor de basisregistratie? Dan geldt in bepaalde gevallen voor deze gegevensverwerking niveau substantieel. Dit is bijvoorbeeld voor veel processen van de Burgerlijke Stand het geval.

Basisregistratiegegevens: welke betrouwbaarheidsniveaus horen hierbij?

Betrouwbaarheidsniveau: substantieel
- Er worden authentieke of niet-authentieke gegevens opgegeven of wijzigingen hierop worden opgegeven om opgenomen te worden in basisregistraties. Op deze opgegeven mutaties vindt nog controle plaats.

Betrouwbaarheidsniveau: hoog
- Er worden authentieke gegevens gecreëerd, gewijzigd of functioneel beëindigd in basisregistraties.
- Er worden andere gegevens direct opgenomen of gewijzigd in basisregistraties, zonder verdere controle.

4.1.4 Hoe groot is het economisch belang bij uw dienst?

Is er sprake van economische belang bij uw dienst? Of kan er economische schade ontstaan bij een foutieve identificatie, identiteitsfraude of verkeerde verwerking van gegevens? Denk bijvoorbeeld aan financiële schade door misbruik of fraude, verlies van geld of economische positie, aansprakelijkheidsstelling, onbevoegden die toegang krijgen tot concurrentiegevoelige informatie (potentiële 'lost order') of koersgevoelige informatie die uitlekt.

Steeds zijn hierbij twee niveaus te beschouwen:

- De economische schade zoals die geleden wordt bij de individuele burger of het individuele bedrijf dat een elektronische dienst van een overheidsorganisatie afneemt. Op het individuele niveau dient u uit te gaan van de *potentiële* schade voor de bepaling van het gewenste niveau.
- De economische schade die op systeemniveau geleden wordt, dat wil zeggen de burgers of bedrijven gezamenlijk of de overheid in zijn totaal. Hierbij kan van ervaringscijfers worden uitgegaan.

Het hoogste van beide inschattingen is bepalend voor het te hanteren betrouwbaarheidsniveau.

Economisch belang: welke betrouwbaarheidsniveaus horen hierbij?

Betrouwbaarheidsniveau: geen

- Het economisch belang is nihil. U verwacht geen economische schade bij een foutieve identificatie of authenticatie.

Betrouwbaarheidsniveau: laag

- Het economisch belang is gering voor de betrokken persoon of organisatie. De gevolgen van een foutieve identificatie of authenticatie zijn vervelend, maar leiden niet tot gedwongen aanpassingen van activiteiten of welstandsniveau.
- Denk aan schade (veroorzaakt door de foutieve identificatie of authenticatie) kleiner dan 2 procent van de jaaromzet van de betrokken organisatie of minder dan 20 procent van het maandinkomen van de betrokken persoon.

Betrouwbaarheidsniveau: substantieel

- Het economisch belang is gemiddeld: het gaat over grotere belangen op individueel niveau of beperkte bedrijfsbelangen. Eventuele schade is goed te overzien en van tijdelijke invloed op de activiteiten van de organisatie of de persoon.
- Denk aan schade (veroorzaakt door de foutieve identificatie of authenticatie) ter grootte van 10 procent van de jaaromzet van de betrokken organisatie of een maandinkomen van betrokken persoon.

Betrouwbaarheidsniveau: hoog

- Het economisch belang is groot: het gaat over dusdanig grote belangen, dat het ongewijzigd voortbestaan van de organisatie of het doorleven op hetzelfde welstandsniveau voor de betrokken persoon ernstig bedreigd is.
- Denk aan schade (veroorzaakt door de foutieve identificatie, identiteitsfraude of authenticatie) ter grootte van de jaaromzet (of jaarbegroting) van betrokken organisatie of een jaarinkomen van de betrokken persoon.

4.1.5 Hoe groot is het publiek belang bij uw dienst?

Hiervoor stelden we het belang van de individuele burger of het individuele bedrijf centraal. Hier gaat het om het algemeen belang. Daarbij kunnen we onderscheid maken tussen enerzijds publicitaire en politieke onrust en anderzijds maatschappelijke ontwrichting.

Publiek belang: welke betrouwbaarheidsniveaus horen hierbij?

Bij het risico op publicitaire onrust (vanwege geschaad publiek vertrouwen in de dienstverlening)

Betrouwbaarheidsniveau: laag

- Er is sprake van klachten, er verschijnen berichten in de media.

Betrouwbaarheidsniveau: substantieel

- Er is bijvoorbeeld een interventie van de Nationale Ombudsman en er zijn Kamervragen.

Betrouwbaarheidsniveau: hoog

- De politiek verantwoordelijke komt in de problemen.

Bij risico op maatschappelijke ontwrichting

Betrouwbaarheidsniveau: laag

- Er zijn verstoringen die door één organisatie kunnen worden opgelost.

Betrouwbaarheidsniveau: substantieel

- Er zijn verstoringen die vragen om een gecoördineerd optreden van meerdere organisaties (vaak publiek en privaat).

Betrouwbaarheidsniveau: hoog

- Er is sprake van een noodtoestand. Er zijn bijvoorbeeld verstoringen die noodmaatregelen vereisen buiten de normale juridische en financiële kaders.

4.2 Referentiescenario

U kunt het classificatiemodel in deze handreiking goed gebruiken als de processen en de IT van uw dienst een gemiddelde kwetsbaarheid hebben. Maar wat is die gemiddelde kwetsbaarheid? De aannames hierover maken we hieronder expliciet. Ze vormen het referentiescenario.

Afwijkingen van het referentiescenario

Er zijn afwijkingen van het referentiescenario die veel voorkomen. We noemen dit correctiefactoren. Ze kunnen ertoe leiden dat u een ander betrouwbaarheidsniveau zou moeten kiezen of dat u een volledige risicoanalyse zou moeten uitvoeren.

Aannames voor het referentiescenario

Aannames over diensten en gebruikers

- U biedt een of meerdere interactieve, online diensten voor burgers, bedrijven of beide doelgroepen. Of het gaat om applicatie-applicatieverkeer en retourstromen.
- Burgers nemen uw dienst(en) af voor zichzelf of laten ze afnemen door gemachtigden. Werknemers nemen uw dienst(en) af voor de onderneming waarvoor ze werken.
- Het is duidelijk afgebakend welk soort regeling en welk type dienst u levert.

Aannames over IT-beveiliging en privacy

- U heeft werkende managementsystemen voor informatiebeveiliging en bescherming van persoonsgegevens.
- U heeft een geïmplementeerd en actueel IT-beveiligingsplan voor uw dienst. Dit plan is gebaseerd op gangbare normen, een specifieke risicoanalyse of beide.
- Specifiek voor uw dienst (en de eventuele regeling) is bekend welke persoons gegevens worden verwerkt. Ook is duidelijk om wat voor soort verwerkingsacties het gaat. (Zie hoofdstuk 4.1.1 voor persoonsgegevens en hoofdstuk 4.1.3 voor gegevensverwerking in het kader van een basisregistratie).

Aannames over het proces achter de regeling en dienst

- U neemt de geldende wettelijke vereisten voor uw dienst in acht.
- De gebruiker wordt voor de toegang tot uw dienst geauthenticeerd. In het navolgende proces gebruikt u die identiteit.
- U kunt aanvullende maatregelen treffen om de identiteit van de gebruiker te verifiëren, maar dat gaat niet verder dan backofficecontroles. U vraagt de gebruiker niet om extra zekerheid te geven over zijn identiteit.

- Biedt u een dienst aan die een besluit van een bestuursorgaan omvat? Dan wordt het besluit altijd bekendgemaakt aan de belanghebbende. Eventueel worden ook andere betrokkenen op de hoogte gesteld. Dit mag plaatsvinden via een ander kanaal dan die van uw dienst.

4.3 Correctiefactoren

Het referentiescenario, waarop we het classificatiemodel hebben gebaseerd, geeft niet onder alle omstandigheden een juiste uitkomst. Er zijn zowel risicoverlagende als risicoverhogende factoren.

Risicoverlagende factoren

Risicoverlagende factoren komen vooral voor als er extra processtappen zijn, waarin het risico verminderd wordt. Op basis hiervan kunt u voldoende reden hebben om een lager betrouwbaarheidsniveau te kiezen dan het classificatiemodel aangeeft.

Vijf situaties met risicoverlagende factoren

1. In het vervolgproces moet de belanghebbende zich fysiek melden en legitimeren (met een wettelijk indentiteitsdocument en BSN). Op die manier weet u zeker dat hij daadwerkelijk uw dienst in kwestie wil afnemen met de gegevens die hij heeft aangeleverd.
2. Er is een terugkoppeling van wijzigingen in gegevens of van (voorgenomen) besluiten via een ander kanaal dan het kanaal van uw dienst. NB Een ander kanaal kan daarin ook een ander elektronisch kanaal betreffen. Een transactie (of de uitkomst daarvan) op een overheidswebsite bevestigen via de Berichtenbox kwalificeert in dat geval dus. Uiteraard moet het andere kanaal van bereikbaarheidsgegevens gebruik maken, die los staan van de transactie in kwestie. Een transactie op een overheidswebsite bevestigen via een email terugkoppelen, waarvan het emailadres in die transactie wordt opgegeven, kwalificeert nadrukkelijk niet.
3. In het vervolgproces komen gegevens of documenten voor die, los van uw dienst, bewijzen dat de gebruiker echt betrokken is bij uw dienst en er toestemming voor heeft gegeven.
4. Er is sprake van voortdurende en actieve monitoring van uw dienst. Daarmee voorkomt u dat uw dienst in korte tijd heel vaak benaderd wordt door dezelfde gebruiker. Ook ziet u daarmee verdachte gebruikspatronen die op fraude duiden. Houdt u risico- of handhavingsprofielen bij, dan werkt dat ook risicoverlagend.
5. Is het economisch belang bepalend voor het betrouwbaarheidsniveau van uw dienst? En is er sprake van een financiële dienst? Dan werkt verificatie van de rekeninggegevens voor betalingen risicoverlagend.

Verbod verlagen betrouwbaarheidsniveau

Heeft uw dienst te maken met een risicoverlagende factor? Dan kunt u het betrouwbaarheidsniveau vaak met één stap verlagen. Maar dat kan niet als:

- wettelijke eisen het betrouwbaarheidsniveau bepalen (bijvoorbeeld vormeisen aan ondertekening);
- het betrouwbaarheidsniveau aanvankelijk op 1 stond. U kunt niet terug naar 0. Risicoverlagende factoren kunnen immers de *aard van de gegevens* niet veranderen. Er zullen altijd maatregelen nodig blijven om de betrouwbaarheid en vertrouwelijkheid van persoonsgegevens te garanderen.

Risicoverhogende factoren

Risicoverhogende factoren hangen samen met de context van uw dienst. Denk bijvoorbeeld aan politieke of bestuurlijke gevoeligheid of imago. In deze handreiking schrijven we dan geen hoger betrouwbaarheidsniveau voor, maar raden u aan een volledige risicoanalyse uit te voeren.

Vier situaties voor een volledige risicoanalyse

1. Aan uw dienst zit een groot politiek, bestuurlijk of imagorisico vast.
2. U kunt het risico moeilijk bepalen, omdat de directe gevolgen van een incident beperkt zijn. Tegelijkertijd is de potentiële vervolgschade groot.
3. Uw dienst loopt grote kans op grootschalig misbruik door georganiseerde criminaliteit. Dit doet zich vooral voor bij de combinatie van massale processen, beperkte controlemogelijkheden en als (grootschalig) misbruik veel gewin oplevert.
4. Uw dienst is een aantrekkelijk doelwit voor terreurorganisaties of buitenlandse inlichtingendiensten.

In veel gevallen komt het bovenstaande overeen met diensten waarbij ook de QuickScan BIR aangeeft een volledige risicoanalyse uit te voeren. Maar de bovenstaande lijst is doorslaggevend of u ook voor de bepaling van het betrouwbaarheidsniveau van authenticatie een volledige risicoanalyse moet uitvoeren.

4.4 Voorbeelden van diensten en betrouwbaarheidsniveaus

Welk diensten en betrouwbaarheidsniveaus horen bij elkaar? Hieronder vindt u enkele voorbeelden volgens de bovenstaande criteria.

Diensten	Niveau authenticatie
• Anoniem bezoeken overheidswebsites • Gemeentelijke lokale diensten (zoals meldingen over de openbare ruimte of aanvragen afvalcontainers) • Inzien WOZ-waardering[11]	Geen eisen
• Registreren gepersonaliseerde portalen • Kapvergunning • Evenementvergunning • Omgevingsvergunning particulieren • Aangifte lichte delicten (zoals een gestolen fiets)	Laag
• Aangifte overlijden (door een begrafenisondernemer) • Melding voorgenomen huwelijk of geregistreerd partnerschap (door partners) • Aangifte geboorte (door ouder) • Vergunningaanvraag seksbedrijven • Vooringevulde aangifte belastingdienst • Belastingaangifte ondernemingen • Aanvraag subsidie • Aanvraag financiële toeslagen • Aangifte ernstige delicten (zoals mishandeling of huiselijk geweld)	Substantieel
• Raadplegen medisch dossier • Raadplegen beslissingen bestuursorgaan met (medische) gegevens • Raadplegen strafrechtelijke gegevens • Aanvraag screening voor een derde	Hoog

[11] WOZ-waarderingen worden als openbare gegevens beschouwd.

5 Machtigingen

Welk betrouwbaarheidsniveau hoort erbij?

5.1 Waar gaat het eigenlijk over?

In veel situaties laten burgers of bedrijven zich vertegenwoordigen door iemand anders. Zo'n vertegenwoordiger is gemachtigd om te handelen namens die burger of dat bedrijf. Een machtiging heeft in principe geen invloed op het betrouwbaarheidsniveau van een individuele dienst: de aard van de dienst verandert er namelijk niet door. Er zijn wel bijzondere situaties, zoals bijvoorbeeld curatele, bewindvoering en attribuutverstrekking, waarin specifieke afwegingen en controles worden gevraagd waar we nu niet verder op ingaan. Dit hoofdstuk gaat verder over machtigingen in algemene zin.

Het is belangrijk om een gemachtigde zonder twijfel te herkennen. U wilt immers niet dat vertegenwoordigers met de eigen inloggegevens van burgers of bedrijven zelf inloggen. Het is dan namelijk alsof zij die burgers of bedrijven zelf zijn. Ook zouden die vertegenwoordigers die inloggegevens ook voor andere zaken kunnen gebruiken, terwijl dit de bedoeling niet was. Beter is het daarom te streven naar uitsluitend expliciet vastgelegde en herkenbare machtigingen. De machtiging ligt dan vast in een machtigingsregister. Daar is dus opgeslagen welke handelende partij bevoegd is welke handelingen te doen namens welke burger of welk bedrijf en tot hoever die handelingsbevoegdheid strekt. Dat machtigingsregister verstrekt ook bevoegdheidsverklaringen. Dit gebeurt via digitale berichten waarin staat wat de handelende partij, die is geauthenticeerd, daadwerkelijk bevoegd is de elektronische dienst in kwestie af te nemen namens die burger of dat bedrijf.

Voorbeeld: digitale belastingaangifte

Met DigiD Machtigen zijn digitale machtigingen deels mogelijk. Maar digitale machtigingsmogelijkheden bestaan nog lang niet overal, terwijl die in de digitale wereld noodzakelijk zijn. Zeker gezien de trend dat de overheid digitale gegevensverwerking door burgers en bedrijven steeds meer verplicht stelt. Een voorbeeld is de inmiddels min of meer verplichte digitale belastingaangifte. De Nationale Ombudsman stelt dat 'mensen die moeite hebben met de digitalisering hierbij adequate ondersteuning moeten kunnen krijgen' (zie ook hoofdstuk 2.2.4). Voor maatschappelijke dienstverleners bij de belastingaangifte (de zogeheten HUBA's: hulpverleners bij aangifte) bestaat in 2016 nog geen adequate machtigingsvoorziening. Logius werkt inmiddels aan de realisatie daarvan.

5.2 Wat betekenen machtigingen voor een individuele dienst?

Of u nu te maken hebt met een burger of bedrijf of met diens vertegenwoordiger, het betrouwbaarheidsniveau voor uw individuele dienst verandert er zoals gezegd niet door.

Wel zijn er machtigingsregisters nodig in situaties waarbij u als dienstaanbieder de machtigingen niet zelf administreert. Een machtigingsregister registreert machtigingen en geeft bevoegdheidsverklaringen af met een passend betrouwbaarheidsniveau. Machtigingsregisters moeten zo zijn ingericht dat het gewenste betrouwbaarheidsniveau van het proces van vastleggen van de machtigingen verzekerd is. Uitgangspunt hierbij zijn de betrouwbaarheidsniveaus van eIDAS.

Het is van belang te onderkennen dat machtigingen worden vastgelegd in een keten, waarbij niet alle stappen noodzakelijkerwijs digitaal zijn. In die gevallen zal de houder van het machtigingsregister de conversie naar een digitale machtigingsverklaring verzorgen.

Het is ook denkbaar dat er geen gebruik wordt gemaakt van machtigingsregisters. Als dienstaanbieder ontvangt u dan machtigingen op papier of via een digitaal gewaarmerkt bericht.

5.3 Wat betekent machtiging in de praktijk?

Voor het inrichten van de individuele dienst geldt het betrouwbaarheidsniveau zoals dat volgt uit eIDAS en de richtsnoeren van de Autoriteit Persoonsgegevens (AP) (zie hoofdstuk 4.3). Het vastleggen van machtigingen moet op minimaal hetzelfde betrouwbaarheidsniveau gebeuren. Als dienstaanbieder moet u daarom controleren of de authenticatie vergezeld gaat van een bevoegdheidsverklaring op minimaal hetzelfde betrouwbaarheidsniveau. Of er wel of niet wordt gemachtigd, is een zaak van de gebruiker van de dienst.

5.4 Overige aandachtspunten: misbruik en fraude

Het risico op misbruik of fraude kan groter worden bij vertegenwoordiging. Fraudeurs kunnen immers frauduleuze machtigingen claimen of registreren. Dit risico moet worden ondervangen. Ten eerste door iedere keer dat een dienst wordt afgenomen de machtiging aan te moeten tonen op het vereiste betrouwbaarheidsniveau. Ten tweede door juiste eisen te stellen aan de registratie en het gebruik van machtigingen. Die staan bijvoorbeeld in het afsprakenstelsel voor Idensys en eHerkenning.

Als een burger iemand (of bedrijf) wilt machtigen hem of haar te vertegenwoordigen dan moet het registreren van een machtiging relatief laagdrempelig zijn. Als de drempel te hoog is, blijft de kans op het doorgeven van de eigen inloggegevens en ander ongewenst gedrag groot. Neem deze overweging mee wanneer vertegenwoordiging een rol speelt bij uw aangeboden dienst.

Verder dient u als dienstaanbieder het gebruik van machtigingen terug te koppelen aan de betrokkenen. Daarmee krijgt de betrokken burger of het betrokken bedrijf concreet inzicht in wie namens hem diensten bij de overheid afneemt.
U kunt denken aan een opt-out mogelijkheid die de Belastingdienst aanbiedt. De burger of bedrijf ontvangt een brief met daarin de melding dat belastingintermediair X namens die persoon de aangiftes wil indienen. Die brief (Service Bericht Aangifte - SBA) stelt de burger/ondernemer hiervan op de hoogte en biedt de mogelijkheid dit te corrigeren door simpelweg een deel van die brief in een bijgesloten voorgeadresseerde enveloppe aan Logius te sturen, die voor de Belastingdienst de machtigingen beheert.

6 Applicatie-applicatieverkeer

Wat doet u met dienstverlening zonder menselijke tussenkomst?

6.1 Waar gaat het eigenlijk over?

Steeds vaker komt er bij digitale dienstverlening geen mens meer aan te pas. Zo kan een geautomatiseerd systeem een dienst afnemen bij een ander geautomatiseerd systeem. Dit wordt applicatie-applicatieverkeer genoemd. Een voorbeeld hiervan is Digipoort.

De volgende eigenschappen zijn kenmerkend voor applicatie-applicatie-verkeer:

- Er is geen menselijke tussenkomst.
- Het gaat om communicerende applicaties, de natuurlijke persoon is buiten beeld.
- Het gaat vaak om aanzienlijke volumes (opgeteld dan wel individuele stromen berichten).

6.2 Manieren van beveiliging

Zowel het kanaal als de inhoud van dit verkeer kan worden beveiligd:

- Door het kanaal te beveiliging wordt een 'veilige tunnel' gerealiseerd tussen de organisatie die de dienst levert en de organisatie die de dienst afneemt. Aan beide zijden is bekend waar de andere kant van de tunnel uitkomt. De tunnel zelf zorgt voor een veilig transport van gegevens. Die kunnen in de tunnel niet door een derde worden gelezen of gewijzigd.
- Het is ook mogelijk de inhoud te beveiligen: het bericht zelf. Een bericht wordt dan ondertekend of gewaarmerkt en veelal ook versleuteld. Berichten kunnen zo end-to-end beveiligd worden doorgegeven. Het is dan niet mogelijk het bericht tijdens het transport te lezen of te wijzigen.

In tabel 1 staan enkele kenmerkende verschillen tussen kanaalbeveiliging en inhoudsbeveiliging.

Tabel 1. *Kanaalbeveiliging versus beveiliging van de inhoud*

Kanaalbeveiliging	Beveiliging inhoud
Universeel Er kunnen meer soorten inhoud, vaak ook van meerdere applicaties over hetzelfde kanaal.	**Specifiek** Elke soort inhoud kent zijn eigen beveiliging
Vluchtig Aan de inhoud zie je niet dat die veilig is getransporteerd.	**Blijvend bewijs** Aan de inhoud zijn kenmerken gekoppeld die de authenticiteit bewijzen
Tot eerste tussenstation veilig Het verkeer is beschermd vanaf de tunnelingang tot het punt waar de tunnel 'boven' komt.	**End-to-end veilig** Ook veilig verkeer met voor- en achterliggende ketenpartijen is mogelijk.

Digitale certificaten zijn feitelijk de beveiligingsstandaard voor zowel kanaal- als inhoudsbeveiliging. Vaak worden ze in combinatie gebruikt. Digitale certificaten verschaffen meer zekerheid dan andere vormen van beveiliging, zoals met wachtwoorden.

Beveiligd verkeer met digitale certificaten

SBR
Digitale certificaten worden nu grootschalig ingezet bij Standard Business Reporting (SBR). Bedrijven of intermediairs doen met SBR bijvoorbeeld aangiften of deponeren jaarrekeningen. Hun systemen communiceren daartoe geautomatiseerd met die van de overheid via Digipoort. Het verkeer wordt daarbij beveiligd met een PKIoverheid(services)-certificaat.

Communicatie met basisregistraties
Overheidsinstanties hebben typisch tientallen van deze certificaten en vaak unieke certificaten per verbinding in gebruik voor de communicatie met de verschillende basisregistraties, welke verloopt via digikoppeling. Hierbij wordt er gebruik gemaakt van PKIoverheid Services Server certificaten.

6.3 Wat betekent dit voor toepassing van het classificatiemodel?

Voor applicatie-applicatieverkeer is deze handreiking minder zinvol. In de praktijk gebruikt u hiervoor digitale certificaten. De vraag is dan slechts hoe betrouwbaar die certificaten moeten zijn. In de praktijk kiest u voor PKIoverheid services server certificaten, zowel voor de beveiliging van het kanaal als voor de versleuteling van de inhoud. PKIoverheid is ook de verplichte standaard volgens de Baseline Informatiebeveiliging Rijksdienst(BIR) en daarvan afgeleide baselines.

Aandachtspunten voor digitale certificaten
Overheidsorganisaties zijn heel afhankelijk van digitale certificaten, zowel voor kanaalbeveiliging als voor de beveiliging van de inhoud. Drie belangrijke aandachtspunten voor u als dienstverleners:

- Zorg dat u voor kritische toepassingen reservecertificaten van alternatieve certificaatdienstverleners beschikbaar heeft;
- Zorg dat u in uw organisatie meer dan één gemachtigd certificaatbeheerder heeft aangewezen. Dat is een gemachtigde die namens uw organisatie bijvoorbeeld nieuwe certificaten van verschillende certificatenverleners kan aanvragen en oude certificaten kan intrekken.
- Voorkom een single-point-of-failure om te vooromen dat er bij falen een heel proces of een hele keten tot stilstand komt.

7 Retourstromen

Wat doet u als dienstverlener met digitale berichten die u verstuurt?

7.1 Waar gaat het eigenlijk over?

Als dienstaanbieder krijgt u niet alleen digitale berichten van gebruikers. U kunt hen ook digitaal benaderen of antwoorden. Deze interactie is er ook tussen applicaties. We noemen dit de 'retourstroom', een belangrijk onderdeel van de digitale communicatie. Het kan gaan om:

- *E-mail* – u verstuurt een digitaal bericht naar het e-mailadres van een natuurlijke persoon.
- *Een webportaal of Berichtenbox* – u plaatst berichten in een eigen, beveiligd webportaal of in een Berichtenbox en attendeert de burger er (via sms of e-mail) op dat er een bericht klaar staat.
- *Applicatie-applicatieverkeer* – u laat retourstromen via applicatie-applicatieverkeer verlopen, direct naar de betrokken organisatie of naar een intermediair (zie hoofdstuk 6).

7.2 Wat betekent dit voor een individuele dienst?

In de Algemene wet bestuursrecht (Awb) staan bepalingen over digitaal verkeer. De Awb stelt dat zowel u als de geadresseerde ervoor moeten zorgen dat het retourbericht de geadresseerde ook werkelijk bereikt. U moet een betrouwbaar en veilig medium regelen, de burger of het bedrijf moet zelf zijn post controleren.

Bij retourberichten is het belangrijk dat u de volgende zaken goed regelt:

- Zorg dat het bericht of document de geadresseerde bereikt.
- Voorkom dat onbevoegden toegang krijgen tot het bericht of het document.
- Zorg ervoor dat de geadresseerde kan verifiëren dat het bericht of document ook daadwerkelijk van u afkomstig is.

De Awb laat het aan de burger of het bedrijf over of zij via de digitale weg willen communiceren. Kiezen ze daarvoor, dan moeten ze via die weg ook bereikbaar zijn.
Met andere woorden: in de Awb zijn de gewone post en het elektronische kanaal nevengeschikt. Het elektronische verkeer is echter op een aantal punten inmiddels verplicht en de verwachting dat deze verschuiving nog verder zal voortgaan. Zie ook bijgaand kader.

E-mail

E-mail is over het algemeen niet geschikt voor retourstromen. Daar zijn enkele redenen voor:

- Burgers en bedrijven houden niet per se een actueel e-mailadres bij. Daardoor kan het gebeuren dat retourstromen niet op het juiste adres aankomen.
- E-mail is in veel opzichten een minder betrouwbaar en vertrouwelijk medium. Voor gevoelige gegevens moet u berichten versleutelen. Daarvoor heeft u een digitaal certificaat van de burger of het bedrijf nodig. Maar burgers en bedrijven ondervinden geen prikkel om een actueel certificaat ter beschikking te stellen.
- U moet iets extra's doen om aan te tonen dat uw bericht ook echt van u komt. Een van de mogelijkheden hiervoor is het waarmerken van de berichten zelf (zie hiervoor het kader 'Betrouwbare documenten van de overheid' onder 7.3).

E-mail is wel redelijk geschikt voor terugkoppeling van weinig gevoelige gegevens. Denk aan algemene informatie of serviceberichten. Daarbij moet het e-mailadres wel kort daarvoor zijn opgegeven of bevestigd door de burger of het bedrijf.

Webportaal en Berichtenbox

Als dienstaanbieder kunt u retourberichten op een eigen webportaal zetten. U geeft hen toegang met bijvoorbeeld hun DigiD. Maar steeds meer dienstaanbieders gebruiken hiervoor de generieke voorziening Berichtenbox (onderdeel van MijnOverheid). Geadresseerden openen en lezen hier (retour)berichten van de overheid in een veilige omgeving. Zij krijgen een attenderingsbericht als er nieuwe berichten in de Berichtenbox staan. Ook voor bedrijven is er een Berichtenbox.

Hoe zeker is het dat de juiste persoon toegang krijgt tot de (retour) berichten? De Berichtenbox voor burgers biedt betrouwbaarheidsniveau Laag door de authenticatie voor de Berichtenbox te laten plaatsvinden met DigiD. Dat een bericht van de overheid komt, weet de geadresseerde vrij zeker, omdat de bron de Berichtenbox of een andere vertrouwde overheidsdienst is.
Voor bedrijven wordt de toegang tot de Berichtenbox eveneens op niveau Laag geregeld, zij het op het niveau eHerkenning 2+, wat hoger is dan het gehanteerde DigiD niveau voor burgers.

Zwak punt blijft dat u afhankelijk bent van de beschikbaarheid van een actueel e-mailadres of 06-nummer om de burger of het bedrijf op nieuwe berichten te attenderen. Omdat het slechts om attenderingsberichten gaat, is dit een minder groot probleem dan wanneer u uitsluitend kiest voor e-mail bij retourberichten. Uiteraard heeft de burger zelf ook een belang bij een goede registratie van dergelijke bereikbaarheidsinformatie, niettemin is het een aandachtspunt.

Applicatie-applicatieverkeer

Als u een retourbericht rechtstreeks naar de betrokken organisatie stuurt, zorgt de kanaalbeveiliging voor de gewenste zekerheden. Omdat voor applicatie-applicatiekoppelingen de bereikbaarheid van de geadresseerde inherent goed is geregeld, is de kans groot dat het bericht ook daadwerkelijk aankomt. De kanaalbeveiliging verzekert bovendien dat buitenstaanders geen toegang kunnen krijgen tot het bericht. Een applicatie-applicatiekoppeling kan dus zeer betrouwbaar zijn.

Bij vertegenwoordiging zal u vaak zowel de intermediair als de betrokkene willen berichten. Sommige intermediairs leveren ook digitale diensten aan de klanten die zij vertegenwoordigen. U kunt dan overwegen om de retourstroom aan de burger of het bedrijf via het digitale kanaal van de intermediair te laten verlopen. Maar uiteindelijk bepaalt de betrokkene hoe hij digitaal bereikbaar wil zijn.

7.3 Wat betekent dit voor toepassing van het classificatiemodel?

U kunt het classificatiemodel toepassen op de retourstromen. U kijkt dan naar de gegevens van het retourbericht. Welk betrouwbaarheidsniveau hoort daarbij? Voor de dienst waarmee u retourberichten verstuurt, moet minimaal hetzelfde betrouwbaarheidsniveau gelden. Voor u staan dan de volgende mogelijkheden open:

- E-mail is alleen bruikbaar voor berichten met een maximaal betrouwbaarheidsniveau Laag.
- Of een webportaal of Berichtenbox geschikt is, hangt af van het betrouwbaarheidsniveau van authenticatie van de Berichtenbox. Vooralsnog is dat niveau Laag. Dat niveau moet dan ook voldoende zijn voor uw specifieke retourberichten.
- Voor applicatie-applicatieverkeer is de (kanaal)beveiliging goed geregeld, omdat vaak gebruik wordt gemaakt van PKIoverheid(services)-servercertificaten. Geldt voor het retourbericht nog een andere bestemming? Dan is de situatie gecompliceerder en moet u een uitgebreide risicoanalyse uitvoeren.

Verschuivingen met juridische gevolgen

Van breng- naar haalverplichting
Vroeger was het gangbaar dat overheid juridisch belangrijke documenten verstuurde naar de ontvanger. De overheid heeft dan een 'brengverplichting'. Dit maakt langzaam plaats maakt voor een model waarbij burgers en bedrijven een 'haalverplichting' krijgen.

Wat brengen en halen betekent verschuift met de technische invullingen. Vandaag kan halen betekenen dat een burger verplicht is zijn post te openen en te behandelen. Morgen kan halen betekenen dat de burger moet inloggen op een postbussysteem van de overheid of een andere 'in de cloud' opgenomen dienst.

Van optioneel naar verplicht kanaal
Een tweede verschuiving gaat over de status van digitale dienstverlening. Nu is er in de Awb en de Wet elektronisch bestuurlijk verkeer sprake van een 'nevenschikking': burger en overheid moeten naast een papieren kanaal bewust een digitaal kanaal openstellen.

Maar we zien onmiskenbaar de beweging naar 'digitaal, tenzij'. Het wordt feitelijk de norm. Zo is bijvoorbeeld voor de belastingaangiftes het digitale kanaal verplicht gesteld. Een goed voorbeeld is de verplichting voor de elektronische winstaangifte voor bedrijven en de meer recente afschaffing van de blauwe envelop voor de burger met de invoering van de Wet Elektronisch Berichtenverkeer Belastingdienst.

Ook de juridische situatie rond de retourstroom zal daarmee waarschijnlijk gaan veranderen. Maar het is nu nog onduidelijk hoe precies.

Belangrijk: waarmerk uw documenten

Vaak wil een burger of een bedrijf kunnen vaststellen dat bepaalde documenten inderdaad van een autoriteit afkomstig zijn, zoals de overheid. Denk bijvoorbeeld aan digitale documenten die je elders weer als bewijs moet overleggen, zoals beschikkingen, uittreksels, officiële verklaringen of openbare bekendmakingen. Burgers en bedrijven willen daarvan met zekerheid kunnen vaststellen dat het om officiële overheidsdocumenten gaat.

Zegels en tijdstempels
Voor de rechtszekerheid van burgers en bedrijven is het goed dat overheden dit soort documenten digitaal waarmerken. Zeker als de documenten als bewijsvoering gelden voor een derde partij. Overheden doen dit nog (te) weinig. Als ze het doen, gebruiken ze een digitale handtekening van hun organisatie of van een medewerker. eIDAS introduceert hiervoor speciale vertrouwensdiensten. Het ligt voor de hand om die te gebruiken. Het gaat om:

- *Elektronische zegels* – ze dienen als bewijs dat een digitaal document door bijvoorbeeld een overheidsorganisatie is afgegeven. Zowel de oorsprong als de integriteit van het document wordt hiermee gegarandeerd. Behalve voor documenten kunnen elektronische zegels ook worden gebruikt voor de authenticatie digitale bestanden die tegen wijziging of vervang door onbevoegden beveiligd dienen te worden, zoals programmacode.
- *Elektronische tijdstempels* – ze dienen als bewijs dat een document (of een verzameling gegevens) op een bepaald moment in de tijd bestond. Ze geven geen garanties over de oorsprong van het document of de integriteit en juistheid van de gegevens.

Eisen vanuit eIDAS
Aan zowel elektronische zegels als aan elektronische tijdsstempels worden eisen gesteld in eIDAS. Bij elektronische zegels zijn geavanceerde en gekwalificeerde zegels te onderkennen, geheel analoog aan de elektronische handtekeningen. Bij elektronische tijdstempels zijn gewone en gekwalificeerde elektronische tijdstempels onderkend.

Hoog betrouwbaarheidsniveau
Als u documenten wilt waarmerken, ligt het voor de hand dat u elektronische zegels en tijdstempels met een hoog betrouwbaarheidsniveau gebruikt. Denk aan een geavanceerd elektronisch zegel op basis van een gekwalificeerd certificaat. Of aan elektronische tijdstempels met het gekwalificeerde niveau.

Standaardformaten
Voor de interoperabiliteit is het verstandig om voor het ondertekenen van documenten te werken met de standaardformaten Pades, Xades of Cades. Deze formaten zijn ook vastgelegd in het Besluit EU 2011/130 en het Uitvoeringsbesluit (EU) 2015/1506. Ze zijn in de Dienstenrichtlijn aangemerkt als de formaten die u als overheidsinstantie in ieder geval moet accepteren.

Valideren
Naast het waarmerken van documenten moet u er ook zorg voor dragen dat de ontvanger de gewaarmerkte documenten ook online kan valideren. Soms gaat dit automatisch als u bijvoorbeeld met de voorhanden zijnde programmatuur, soms zult u hiervoor een validatiedienst moeten (doen) inrichten. Als u een ander dan een standaardformaat hanteert om documenten te ondertekenen of verzegelen, is het aanbieden van een gratis validatiedienst wettelijk verplicht.

Aangetekende bezorging
Ten slotte kent eIDAS nog diensten voor elektronisch aangetekende bezorging. Hierbij worden de identiteiten van zowel de verzender als ontvanger gegarandeerd en de bezorging aan de ontvanger. Het is belangrijk om een veilig en betrouwbaar communicatiekanaal met de burger te hebben. Aangetekende bezorging past mooi in dat streven.


Carrier
1:27 PM
100%
Password
1
2
3
4
5
6
7
8
9
0
Emergency
Cancel

8 Eenmalig inloggen

Wat betekent gebruiksgemak voor veiligheid en betrouwbaarheid?

8.1 Waar gaat het eigenlijk over?

Eenmalig inloggen, ook bekend als single sign-on (SSO), is de mogelijkheid voor gebruikers om via één authenticatie(voorziening) toegang te krijgen tot verschillende diensten. De gebruiker logt dan eenmaal in bij de eerste dienst en hoeft daarna niet nogmaals zijn identiteit nogmaals te bevestigen voor andere diensten. Wel zijn er mogelijkerwijs maatregelen aan de orde als de gebruiker van de dienst van de ene dienstverlener naar de dienst van een andere dienstverlener overstapt.

Voorbeeld van eenmalig inloggen
MijnOverheid biedt, wanneer een burger inlogt, toegang tot een hele set van (samengestelde) gegevens en diensten van verschillende (overheids)organisaties, zoals de Basisregistratie Personen (BRP), de RDW (Dienst Wegverkeer) en de stichting Pensioenregister. MijnRVO.nl biedt in het ondernemersdomein, na inschrijving, achter één authenticatie toegang tot tal van specifieke diensten in dat domein zoals de mestregistratie, tal van subsidies en verschillende regelingen rondom de visserij.

Een belangrijk begrip bij eenmalig inloggen is de federatie. In feite is de federatie de groep diensten die gezamenlijk gebruikmaken van een SSO-oplossing. Het varieert van één individuele organisatie met verschillende digitale diensten tot bijvoorbeeld een overheidsbreed portaal.

Er zijn federaties die maar één betrouwbaarheidsniveau hanteren. Als ze verschillende betrouwbaarheidsniveaus faciliteren, kan de gebruiker van een dienst overstappen naar een andere dienst met een hoger betrouwbaarheidsniveau. Hij moet zich dan opnieuw of aanvullend authenticeren.

Nauw verbonden aan eenmalig inloggen is eenmalig uitloggen (single sign-off). De gebruiker krijgt daarbij de zekerheid dat hij in één handeling de openstaande sessies en toegang tot diensten beëindigt.

8.2 Perspectief van de individuele dienst

Bij eenmalig inloggen is het voor u als dienstaanbieder van belang op welk niveau van betrouwbaarheid de authenticatie heeft plaatsgevonden en of deze nog geldig is. Maar er zijn meer aandachtspunten voor eenmalig inloggen. Wat betekent deelname aan een federatie? En hoe ervaart een gebruiker SSO? In paragraaf 8.4 gaan we hier dieper op in.

8.3 Wat betekent dit voor toepassing van het classificatiemodel?

Eenmalig inloggen werpt geen nieuw licht op de criteria en afwegingen van het classificatiemodel. Eenmalig inloggen is in feite een middel om te authenticeren. Op welk betrouwbaarheidsniveau dit gebeurt, moet u bepalen op basis van het classificatiemodel.

8.4 Overige aandachtspunten

Eenmalig inloggen kent enkele aandachtspunten die voor u als dienstaanbieder van belang zijn. We noemen twee belangrijke.

8.4.1 Deel uitmaken van een federatie

Kiest u voor SSO, dan komt u in een federatie terecht. Neem een aantal overwegingen mee voordat u kiest om deel te nemen.

1. Heeft u invloed op de inrichting en werking van de federatie? U bent niet de enige meer die bepaalt hoe de authenticatie verloopt.
2. Het betrouwbaarheidsniveau kan hoger of lager liggen dan voor uw dienst nodig is. Hier kan sprake van zijn als de federatie één enkel betrouwbaarheidsniveau hanteert.
3. Hoe zit het met het gebruiksgemak voor de klant? Een federatie met verschillende betrouwbaarheidsniveaus biedt weliswaar authenticatie op maat voor de dienst, maar relatief minder gebruiksgemak. Wanneer de gebruiker overstapt op een dienst met een hoger betrouwbaarheidsniveau moet hij zich opnieuw authenticeren. Daarmee verdwijnt het voordeel van eenmalig inloggen door SSO.

Lage drempel van de Sociale Verzekeringsbank

Als dienstaanbieder bepaalt u het gewenste betrouwbaarheidsniveau voor uw dienst. Is er via SSO een lager betrouwbaarheidsniveau beschikbaar? Dan kunt u toegang tot uw dienst weigeren. Maar u kunt uw dienst ook zo aanpassen dat een lager betrouwbaarheidsniveau volstaat, bijvoorbeeld door verderop in uw proces mitigerende maatregelen te nemen.

Een goed voorbeeld van een oplossing met lage drempelwerking zijn de diensten van de Sociale Verzekeringsbank (SVB). Gebruikers hebben slechts DigiD Basis nodig. De consequentie daarvan is wel dat gebruikers sommige zaken niet online kunnen afhandelen of dat de SVB een bevestigingsbrief stuurt na afronding van een online transactie.

8.4.2 Gebruikersperspectief

Vanuit het perspectief van de gebruiker kan eenmalig inloggen tot verwarring leiden. Wanneer hij verschillende diensten heeft geopend en eenmalig uitloggen niet beschikbaar is, worden sessies niet direct beëindigd. Het kan hierdoor onduidelijk zijn welke sessies nog open staan. Daardoor ontstaan extra beveiligingsrisico's.

Als dienstaanbieder kunt u stilstaan bij de effecten van eenmalig in- en uitloggen voor de gebruiker. U neemt dan een maatregel op het niveau van uw eigen organisatie. U wijst gebruikers bijvoorbeeld op wat eenmalig inloggen inhoudt en hoe ze daarmee om kunnen gaan. Ook kunt u wensen en eisen formuleren voor de federatie om daarmee de gebruiker beter en veiliger te kunnen bedienen.

9 Ondertekening

Heeft u een elektronische handtekening nodig voor uw dienst?

9.1 Inleiding

In de fysieke wereld zijn we gewend om documenten met een grote regelmaat te ondertekenen. Is dit ook een vereiste bij digitale dienstverlening?

Dit hoofdstuk geeft antwoord op:

1. Ondertekenen en de elektronische handtekening, waar hebben we het over? (Zie paragraaf 9.2.)
2. Heeft u als dienstaanbieder elektronische handtekeningen nodig? Zo ja, welk soort en met welke betrouwbaarheid? (Zie paragraaf 9.3.)
3. Overige vragen waaronder:
   - Wat regelt eIDAS grensoverschrijdend? (Zie paragraaf 9.4.1.)
   - Bent u verplicht elektronische handtekeningen te accepteren? Zo ja, welke dan? (Zie paragraaf 9.4.2.)
   - Moet u de ondertekening voor burgers en bedrijven zelf inrichten of kunt u dat uitbesteden aan ondertekendiensten? (Zie paragraaf 9.4.3.)

9.2 Ondertekenen en de elektronische handtekening, waar hebben we het eigenlijk over?

Het doel van ondertekening is om burgers of bedrijven (juridisch) te binden aan transacties of (een verzameling van) documenten.[12]
Daarbij zijn meerdere factoren van belang:

- De ondertekenaar *begrijpt* de betreffende inhoud en de consequenties van ondertekening.
- Hij *bevestigt* de betreffende inhoud.
- De ondertekening levert *bewijs* op van het bovenstaande voor een derde.

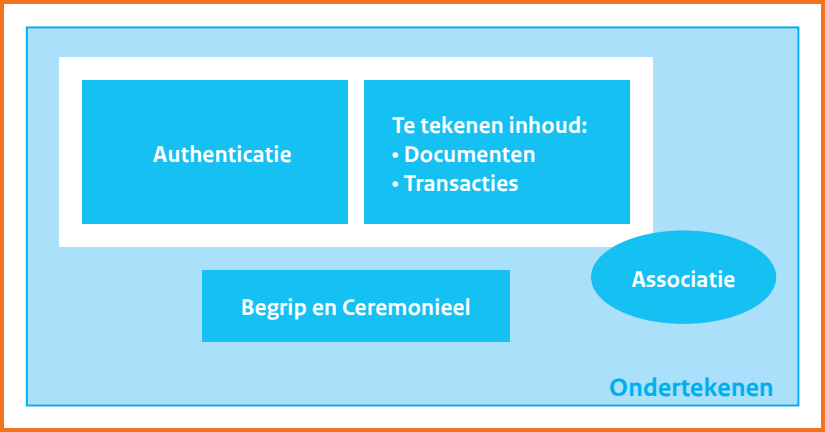
Deze juridische binding vereist een zeker *ceremonieel* dat het moment van ondertekening duidelijk markeert. Het reduceert de kans op overhaast ondertekenen.

[12] In wet- en regelgeving staat ook vaak de eis van schriftelijkheid. Maar het gaat dan niet per se om een ondertekening of een fysiek document. Schriftelijk is 'met schrifttekens samengesteld'.

Wat 'doet' een handtekening eigenlijk?

Het begrijpen en bevestigen van een transactie of document moet leiden tot een zogenoemde associatie. Een associatie wil zeggen dat op een betrouwbare wijze een verbinding is gekomen tussen: het ondertekende document, de identificatie en authenticatie van de ondertekenaar en de dienst of het proces waarin het document tot stand is gekomen en is ondertekend. Met een elektronische handtekening moet de associatie bewijsbaar zijn. Maar deze handtekening is eigenlijk niet meer dan een gegeven dat verbonden is aan een document of een andere set gegevens.

Bij een ondertekening spelen identificatie, authenticatie en associatie dus een belangrijke rol. Schematisch ziet het er zo uit:



Begrip en ceremonieel zijn geen impliciet onderdeel van de associatie. Maar ze horen wel impliciet bij een bepaalde dienst of ondertekeningssituatie.

Elektronische handtekeningen in eIDAS

Een elektronische handtekening is een set gegevens die geassocieerd is met het ondertekende document of de ondertekende gegevens. Zij geeft de identiteit van de ondertekenaar aan en de authenticiteit van het ondertekende document of de ondertekende gegevens.

De eIDAS-verordening geeft de volgende definitie:
Een elektronische handtekening is een verzameling gegevens in elektronische vorm, die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen.

Soorten elektronische handtekeningen
eIDAS onderscheidt drie soorten elektronische handtekeningen, namelijk de:
1. Elektronische handtekeningen,
2. Geavanceerde elektronische handtekeningen en
3. Gekwalificeerde elektronische handtekeningen.

1. Elektronische handtekening (zie artikel 3.10 van de eIDAS-verordening)
Een elektronische handtekening moet voldoen aan de eisen die impliciet zijn in de definitie. Het moet dus gaan om elektronische gegevens die door de ondertekenaar aan andere elektronische gegevens worden verbonden met als doel te ondertekenen. Verder worden er geen eisen aan gesteld.

2. Geavanceerde elektronische handtekening (zie artikelen 3.11 en 26 van de verordening)
De geavanceerde elektronische handtekening:
- is op unieke wijze aan de ondertekenaar verbonden;
- maakt het mogelijk de ondertekenaar te identificeren;
- wordt aangemaakt met gegevens die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken;
- is zo gekoppeld aan de ondertekende gegevens, dat latere wijzigingen in deze gegevens kunnen worden opgespoord.

De definitie van geavanceerde elektronische handtekening staat los van een bepaalde technologie. Maar in het algemeen wordt de digitale handtekening gebruikt, die op Public Key Technologie (PKI) is gebaseerd.

3. Gekwalificeerde elektronische handtekening (zie artikelen 3.12, 28 en 29 van de verordening)
De gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening. Maar bovendien is een gekwalificeerde elektronische handtekening
- gebaseerd op een gekwalificeerd certificaat en
- aangemaakt met een daarvoor gekwalificeerd middel voor elektronische handtekeningen.

Figuur 4. *De verschillende soorten elektronische handtekeningen. Sommige elektronische handtekeningen zijn geavanceerd. Sommige geavanceerde elektronische handtekeningen zijn gekwalificeerd.*

Een *gekwalificeerd certificaat* is een bevestiging van de identiteit van de ondertekenaar, gekoppeld aan gegevens waarmee de elektronische handtekening kan worden geverifieerd. Die gekwalificeerd certificaat wordt door een gekwalificeerde verlener van vertrouwensdiensten uitgegeven, na een zorgvuldige face-to-face identiteitsverificatie. De precieze eisen aan het gekwalificeerd certificaat zijn in bijlage I van de eIDAS-verordening opgenomen. Het voert te ver om die hier integraal te behandelen.

De gegevens om de elektronische handtekening aan te maken worden door een *gekwalificeerd middel* beschermd tegen uitlekken, kopiëren of misbruik door derden. Zo'n middel kan een smartcard of USB-stick zijn, maar er zijn ook andere middelen mogelijk.

Rechtsgeldigheid van elektronische handtekeningen

- Qua rechtsgevolg is de gekwalificeerde elektronische handtekening gelijk aan de handgeschreven handtekening. (Zie artikel 25 tweede lid van de eIDAS-verordening.)
- Ook andere elektronische handtekeningen kunnen een rechtsgevolg hebben en dienen als bewijsmiddel. Alleen het feit dat ze elektronisch zijn of niet voldoen aan de eisen voor gekwalificeerde elektronische handtekeningen, doet daar niets aan af.

In Nederland is in het Burgerlijk Wetboek (artikel 15a) een bredere gelijkstelling van de elektronische handtekening met de handgeschreven handtekening opgenomen. Dit geeft een concretere invulling aan het tweede punt. Het BW refereert aan elektronische handtekeningen (zoals bedoeld in de eIDAS-verordening, artikel 3) en stelt dat naast de gekwalificeerde handtekening ook andere elektronische handtekeningen dezelfde rechtsgevolgen hebben als de handgeschreven handtekening, mits ze voldoende betrouwbaar zijn voor de dienst waar ze voor worden gebruikt.
Bij eenvoudige processen en simpele transacties hiertoe kan worden volstaan met een eenvoudige elektronische handtekening (een elektronische handtekening, niet zijnde een geavanceerde elektronische handtekening), terwijl voor meer complexe transacties waarbij de belangen groter zijn een geavanceerde of gekwalificeerde elektronische handtekening nodig is.

Belang van het ondertekenproces en de omgeving

Bij de elektronische handtekening gaat het niet alleen om de identificatie en authenticatie van de ondertekenaar, maar ook om de vraag of het ondertekend document of de ondertekende gegevens authentiek zijn. Wat is er precies ondertekend en (hoe) heeft de ondertekenaar dat (letterlijk) gezien? Daarom zijn ook het proces en de omgeving waarin wordt ondertekend belangrijk. Ze zijn mede bepalend voor de betrouwbaarheid, voor de acceptatie van de ondertekening en voor de toetsing door een onafhankelijke partij, zoals een rechter of een arbiter.

Belangrijk voor de bewijskracht voor bijvoorbeeld een rechter of arbiter zijn vragen zoals:

- Hoe waarschijnlijk is het dat de elektronische handtekening daadwerkelijk is gezet door de ondertekenaar aan wie die handtekening wordt toegekend? (Was het de ondertekenaar echt zelf wel?)
- Is het ondertekenproces zo ingericht dat de ondertekenaar zich bewust is van de inhoud en de gevolgen van wat hij ondertekent?
- Is er een betrouwbare tijdsaanduiding gebruikt bij het moment van ondertekenen, zoals bijvoorbeeld een tijdstempel?
- Wat is de sterkte van het associatiemechanisme, dus behoort de elektronische handtekening ook daadwerkelijk bij de ondertekende gegevens of het ondertekende document?

9.3 Welke elektronische handtekeningen heeft u als dienstaanbieder nodig?

Heeft u wel elektronische handtekeningen nodig?

Het is de vraag of u überhaupt elektronische handtekeningen nodig heeft voor uw dienstverlening. Sta daarom stil bij de volgende punten:

- Wilt u dat burgers en bedrijven begrijpen waaraan ze zich verbinden en dat ze dit bevestigen?
- Wilt u een sterk op zichzelf staand bewijs hebben dat een persoon een bepaald document of bepaalde gegevens heeft ondertekend? Of vindt u een login op het door u beheerd computersysteem voldoende, ook als de samengestelde bewijsvoering daarmee complexer is? U kunt dan ook de te ondertekenen gegevens samenvatten en nogmaals door de ondertekenaar laten bevestigen, eventueel met een extra authenticatie.
- Dwingt wet- en regelgeving u om gebruik te maken van een elektronische handtekening?
- Verleent u diensten aan burgers en bedrijven uit andere EU-lidstaten waarvoor een elektronische handtekening moet worden geaccepteerd als toegang tot die dienst?

Analogie met papieren situatie

Vraagt u een handtekening in uw 'papieren' dienstverlening? Dan hoeft u dat *niet* per se te doen bij uw elektronische dienstverlening. Op papier kan een handtekening namelijk een andere functie hebben. Bijvoorbeeld ceremonieel, om de ondertekenaar ervan te doordringen dat hij zich aan iets verbindt. Of ter bevestiging van de opgegeven identiteit, zoals met authenticatie bij elektronische dienstverlening. Wees daarom voorzichtig om van de papieren situatie uit te gaan. Vraag u eerst af wat het doel en nut zijn van de handtekening op papier voor deze een-op-een te vertalen naar een elektronische handtekening.

Welke soort elektronische handtekening past bij uw dienstverlening?

Relevant voor deze vraag zijn dezelfde criteria als in hoofdstuk 4. Echter met een verschil. Anders dan bij authenticatie kunnen gebruikers met hun elektronische handtekening geen toegang krijgen tot privacygevoelige gegevens. Daarmee blijft één centrale vraag voor elektronische handtekeningen over:

'Worden er door de dienstverlening persoonsgegevens (van verschillende aard) in registraties opgenomen of aangepast?'

De afwegingen hierbij zijn vergelijkbaar met die in hoofdstuk 4. Het gaat dan om de volgende:

1. Worden persoonsgegevens verwerkt:
   - wat is de aard van de te beschermen gegevens? Worden er ook bijzondere gegevens verwerkt? Wordt het burgerservicenummer (BSN) verwerkt?
   - wat zijn de relevante kenmerken van de verwerking zelf?
2. Wat zijn de rechtsgevolgen van het gebruik van de dienst?
3. Worden er basisregistratiegegevens gewijzigd door de dienst?
4. Hoe groot is het economisch belang bij uw dienst?
5. Hoe groot is het publiek belang bij uw dienst?

Vraag u daarnaast af hoe sterk de gewenste *bewijskracht* van de elektronische handtekening moet zijn, zowel op korte als op lange termijn. Belangrijk daarbij is of u de gevolgen van een valse opgave van een burger of bedrijf kunt terugdraaien (*omkeerbaarheid*) en *sanctioneren* (zie kaders met voorbeeldcasussen).

Om een elektronische handtekening te selecteren kunt u de onderstaande tabel gebruiken.

Criteria	Soort elektronische handtekeningen
• Persoonsgegevens maximaal klasse 1 • Verwerking BSN uitsluitend door opgave burger en teruggekoppeld met persoonsgegevens van klasse I • Mogelijk indirect rechtsgevolg • Geen wijzigingen in basisregistratie • Gering economisch belang • Publiek belang laag • Beperkte bewijskracht nodig	Eenvoudige handtekening
• Persoonsgegevens maximaal klasse 2 • Verzwarende factor voor persoonsgegevens bovenop klasse 1 • Verwerking BSN met aanvullende persoonsgegevens • Direct rechtsgevolg • Beperkt effect wijziging van basisregistratiegegevens • Gemiddeld economisch belang • Gemiddeld publiek belang • Aanzienlijke bewijskracht nodig	Geavanceerde elektronische handtekeningen (of een elektronische handtekening met vergelijkbare betrouwbaarheid)
• Persoonsgegevens klasse 3 • Verzwarende factor voor persoonsgegevens bovenop klasse 2 • Verwerking BSN met aanvullende persoonsgegevens • Grote effecten door wijziging gegevens basisregistratie • Groot economisch belang • Groot publiek belang • Hoogst mogelijke bewijskracht nodig	Gekwalificeerde elektronische handtekening

Voorbeeldcasus: subsidieverstrekker
Stel u bent een dienstverlener en uw organisatie verstrekt op aanvraag subsidies aan Nederlandse bedrijven. Bedrijven doen een aanvraag waarin ze een aantal feiten verklaren. Op basis van deze feiten kent u een subsidie toe. De subsidies zijn bescheiden in relatie tot de omzet van de bedrijven, hooguit enkele duizenden euro's.

De bedrijven moeten de aanvraag en de onderliggende verklaring over de feiten ondertekenen. Hiermee wordt de ondertekenaar gebonden en kan hij later een eventuele valse verklaring over de feiten niet meer eenvoudig ontkennen.

Omkeer- en sanctioneerbaar?
In dit proces is er sprake van een hoge mate van omkeerbaarheid: een onterecht uitgekeerde subsidie kan bij een bedrijf meestal worden teruggevorderd.
De sanctioneerbaarheid is in dit geval belangrijk. De ondertekening is daarin echter slechts de eerste stap. Daarna volgt namelijk een schriftelijke terugkoppeling van de aanvraag en de beschikking.

Welke soort handtekening?
Soorten gegevens en economisch belang duiden op een geavanceerde elektronische handtekening. Maar door de schriftelijke terugkoppeling van de aanvraag en beschikking is het risico verder gereduceerd. Op basis hiervan kun je zelfs met een eenvoudige elektronische handtekening volstaan.

Voorbeeldcasus: uitzendbranche en payrolling
Uitzendbureaus en payrollbedrijven handelen sinds ongeveer twee jaar steeds vaker het gehele proces van overeenkomsten met medewerkers volledig digitaal af.

Omkeer- en sanctioneerbaar?
In dit geval zijn de gevolgen goed omkeerbaar.

Welke soort handtekening?
Het grote economische belang zou duiden op een gekwalificeerde elektronische handtekening. Vanwege de goede omkeerbaarheid en sanctioneerbaarheid kun je echter ook volstaan met een geavanceerde elektronische handtekening.

9.4 Overige vragen over elektronische handtekeningen

9.4.1 Internationale aspecten

eIDAS regelt een aantal grensoverschrijdende zaken:

- De gekwalificeerde elektronische handtekening is in alle lidstaten uniform gedefinieerd. De essentiële eisen voor die gekwalificeerde elektronische handtekening zijn EU-breed vastgesteld. De juridische status van deze handtekening is bovendien in alle lidstaten gelijk.
- Voor grensoverschrijdend verkeer is het niet toegestaan een hoger niveau te vereisen dan de gekwalificeerde elektronische handtekening. Er bestaat overigens ook geen gestandaardiseerd niveau boven 'gekwalificeerd'.
- Vereist u als dienstaanbieder minimaal een geavanceerde elektronische handtekening of zegel? Dan moet u elektronische handtekeningen en zegels op dit en op hogere betrouwbaarheidsniveaus accepteren (zie de eIDAS-verordening, artikel 27). Bovendien bent u dan volgens eIDAS verplicht om specifieke formaten van elektronische handtekeningen te ondersteunen, zoals de XAdES-, PAdES- en CAdES- en de ASiC standaarden (zie het EU-uitvoeringsbesluit 2015/1506).

9.4.2 Bent u verplicht elektronische handtekeningen te accepteren?

Handtekening binnen de Dienstenrichtlijn

Misschien bent u er zich niet van bewust, maar sinds de invoering van de Dienstenrichtlijn (2009) kunt u bijvoorbeeld al vergunningaanvragen krijgen met een elektronische handtekening. U mag zo'n elektronische handtekening niet weigeren, als die past bij het betrouwbaarheidsniveau van uw dienst.

Voorgeschreven handtekeningen

Volgens de Algemene wet bestuursrecht (tweede lid van artikel 2:16) kan de Rijksoverheid de elektronische handtekening voorschrijven. Ook een ander bestuursorgaan kan dit doen als het regelgevende bevoegdheid heeft in de eigen verordening. Reden kan bijvoorbeeld het gebruik van digitale gegevens zijn of de rechtsverhouding tussen de ondertekenaar en het bestuursorgaan.

Wordt de elektronische handtekening voorgeschreven? Dan kunt u te maken hebben met extra eisen rond de veiligheid en betrouwbaarheid van de ondertekening. Denk bijvoorbeeld aan het niveau van authenticatie om de elektronische handtekening aan te maken. Of aan de onafhankelijkheid en veiligheid van de ondertekening. Ook kunnen er aanvullende eisen gelden aan de elektronische handtekening die met een tablet wordt gezet.

Internationale handtekeningen

Heeft u te maken met een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat? Of met een gekwalificeerde elektronische handtekening? Dan zijn die in de hele EU geldig. U moet deze accepteren, in ieder geval als deze voldoen aan de geaccepteerde formaten voor elektronische handtekeningen (CAdeS, PAdES, XAdES en ASiC). Overigens kunt u ook andere elektronische handtekeningen niet zonder meer weigeren, gelet op het feit dat elektronische handtekeningen geen rechtsgevolg kunnen worden ontzegd, louter omdat ze elektronisch zijn of niet voldoen aan bepaalde betrouwbaarheidseisen. De handtekening moet dus worden geaccepteerd tenzij er goede redenen zijn om dat niet te doen. Wel mag u als dienstverlener een bepaald niveau van elektronische handtekening vereisen voor uw elektronische dienst.

9.4.3 Kunt u ondertekening voor burgers en bedrijven uitbesteden?

Lokale ondertekening

De belangrijkste vorm van ondertekening waar we in de praktijk mee te maken hebben, is de digitale (PKI) handtekening. Gebruikelijk vindt de ondertekening plaats in de eigen ICT-omgeving van de ondertekenaar, bijvoorbeeld op zijn computer. Het (persoonlijke) certificaat waarmee de ondertekenaar tekent, is veilig opgeslagen in de eigen omgeving van de ondertekenaar (zijn computer of, betrouwbaarder, op een daaraan gekoppelde smartcard). De externe dienstverlening blijft in dit geval beperkt tot het daadwerkelijk produceren en uitgeven van certificaten. Maar het is vooral de ondertekenaar die onder meer voor de juiste software en certificaten moet zorgen. (Zie variant 1 in onderstaand schema.)

Online ondertekening

Anders werkt het bij een ondertekenproces *in de cloud* via *ondertekendiensten*. Hoe is de authenticatie van de gebruiker dan geregeld? En zijn dergelijke ondertekendiensten bruikbaar en betrouwbaar voor u als dienstaanbieder?

Ondertekendiensten kunnen aanvullende eisen implementeren, die gunstig zijn voor een betrouwbare ondertekening. Denk aan:

- De onafhankelijkheid van de partijen die zijn betrokken in de transactie door positionering als trusted third party.
- De aanwezigheid van betrouwbare medewerkers, processen en systemen.
- Specifiek de sterkte van het associatiemechanisme.
- De vormgeving van het proces waardoor de ondertekenaar kennisneemt van de te tekenen inhoud en zich bewust is van de consequenties van de ondertekening.

- De (duurzame) archivering, waarbij de ondertekende stukken en de elektronische handtekening ook op langere termijn voldoende bewijskracht hebben?

Tussen ondertekendiensten bestaan echter in de technische zin wezenlijke verschillen, waarbij met name relevant is met wiens 'cryptografische sleutels' oftewel 'gegevens voor het aanmaken van de elektronische handtekening' wordt gewerkt. We zien daarbij twee smaken:

- 'Stelsels' zoals eHerkenning en Idensys hanteren een 'betrouwbare derde' model. (Zie variant 2b in onderstaand schema.)
  Daarbij wordt de ondertekenaar geïdentificeerd en geauthenticeerd en de ondertekenaar stemt expliciet in met de te tekenen inhoud. De ondertekendienst fungeert dan als betrouwbare derde die een verklaring afgeeft dat de ondertekenaar de betreffende inhoud heeft ondertekend. Die verklaring kunnen we zien als 'associatie'.
- 'Server based'-ondertekening werkt met een persoonlijke digitale handtekening die op een centrale server wordt gezet. (Zie variant 2a in onderstaand schema.)
  Ook hierbij staat de associatie los van de identificatie en de authenticatie van de ondertekenaar. De associatie gebeurt hier echter met de cryptografische sleutels van de ondertekenaar zelf. De server based-ondertekening past goed in het PKIoverheidstelsel.

Sleutel ondertekendienst / Persoonlijke sleutel	Lokaal	Online
	-	Ondertekendienst tekent als 'betrouwbare derde' (Variant 2b)
	Klassieke digitale handtekening (Variant 1)	Gebruiker ontsluit persoonlijke server-based handtekening (Variant 2a)

eIDAS: fysiek bezit niet nodig

Uit eIDAS blijkt de intentie om ondertekendiensten mogelijk te maken. Zo zijn de bepalingen rond de uitsluitende controle subtiel aangepast (zie onderdeel c van de eisen voor de geavanceerde handtekening). Controle impliceert niet meer *fysiek bezit*. *Persoonlijke beheersing (door logische afscherming) op de remote on-line omgeving waarin wordt getekend* volstaat ook.

Dit impliceert direct dat geavanceerde en gekwalificeerde elektronische handtekeningen als 'server-based' ondertekendienst mogelijk zijn, mits aan bepaalde eisen wordt voldaan om de uitsluitende controle door de ondertekenaar te waarborgen.

Online: met of zonder persoonlijke cryptografische sleutels

Ondertekendiensten die de persoonlijke cryptografische sleutels van de ondertekenaar gebruiken (variant 2a) kunnen dus worden geaccepteerd tot en met het niveau van gekwalificeerde elektronische handtekeningen, hetgeen ook nu al binnen het PKIoverheidstelsel het geval is.
Maar de status van 'betrouwbare derde' ondertekendiensten (variant 2b) ligt ingewikkelder. Namelijk rond één eis in eIDAS (artikel 26): kan de ondertekenaar gegevens voor het aanmaken van elektronische handtekeningen onder zijn uitsluitende controle gebruiken?

De gebruikelijke interpretatie van de 'gegevens voor het aanmaken van elektronische handtekeningen' zijn de cryptografische sleutels waarmee de digitale handtekening uiteindelijk wordt aangemaakt. In variant 2b betreft dit dus de ondertekensleutels van de ondertekendienst. Duidelijk is dat die niet onder de uitsluitende controle van de ondertekenaar staan. Wél kunnen ondertekendiensten van het type 2b ervoor zorgen dat elektronische handtekeningen, waarin de identiteit van de ondertekenaar is geassocieerd, uitsluitend kunnen worden aangemaakt onder controle en op het bewijsbaar initiatief van de ondertekenaar. Daarmee is op deze eis weliswaar niet aan de letter maar wel aan de geest van eIDAS voldaan.
En dat sluit weer aan op het nieuwe artikel 15.a van het Burgerlijk Wetboek. Dat stelt namelijk de *materiële betrouwbaarheid* centraal als het gaat om de gelijkstelling aan de handgeschreven handtekening.

De jure leveren 2b ondertekendiensten dus geen geavanceerde elektronische handtekeningen op, maar ze kunnen wel zo worden ingericht dat de facto eenzelfde betrouwbaarheid wordt geboden. In nationale context ligt gelijkschakeling met de geavanceerde elektronische handtekening dus voor de hand en kunt u 2b ondertekendiensten prima gebruiken.

Internationaal ligt het anders. Voor geavanceerde handtekeningen worden slechts die elektronische handtekeningen op basis van een *persoonlijk* certificaat erkend. Type 2b-ondertekendiensten zijn daar derhalve niet bruikbaar. Ook bieden de Europees erkende formaten voor elektronische handtekeningen geen ruimte voor type 2b-ondertekendiensten.

Kortom, kunt u ondertekening voor burgers en bedrijven uitbesteden? Het antwoord is meervoudig:

- Maakt u gebruik van een externe ondertekendienst, dan scheelt u dat implementatielast. Denk aan de invulling van de eisen rond het ondertekenproces. Ook profiteert u van de onafhankelijke positie van de ondertekendienst.
- Met eHerkenning en Idensys weet u zeker dat u betrouwbare ondertekendiensten herkent. Het gaat hier niet om gekwalificeerde handtekeningen en *de jure* ook niet om geavanceerde elektronische handtekeningen. In de praktijk liggen die ondertekendiensten echter wel op het niveau van de geavanceerde elektronische handtekeningen. We behandelen ze voor deze handreiking dus als ware het geavanceerde elektronische handtekeningen.
- Werkt u met elektronische handtekeningen die moeten voldoen aan de Europees erkende formaten of die grensoverschrijdende worden gebruikt? Dan is een ondertekendienst waarin de persoonlijke certificaten van gebruikers worden gehouden noodzakelijk. Type 2b ondertekendiensten zoals thans beschreven in Idensys en eHerkenning zijn hiervoor niet bruikbaar.

Bijlage 1 Relevante Wet- en regelgeving

1 eIDAS-verordening

Vanaf 1 juli 2016 is de Europese eIDAS-verordening van kracht. Uitvoeringshandeling 2015/1502[1] biedt in het verlengde daarvan bovendien een wettelijk kader voor betrouwbaarheidsniveaus. Vanaf deze (vierde) versie van de handreiking zijn deze als basis genomen. De eIDAS-verordening is een Europese verordening die rechtstreekse werking heeft in de lidstaten, dus ook in Nederland. Een verordening staat daarmee boven het nationale recht. Met Nederlandse wetgeving mag niet afgeweken worden van de verordening. Wel wordt een groot aantal implementatie-aspecten geregeld in de Implementatiewet eIDAS, die op het moment van schrijven van deze Handreiking in parlementaire behandeling is. Met de eIDAS-verordening wordt de Europese Richtlijn 1999/93 over elektronische handtekeningen ingetrokken. De meeste zaken die daarin werden geregeld, komen nu terug in deel 2 (Vertrouwensdiensten) van de verordening.

De Verordening bestaat uit twee delen:
1. Elektronische identificatie (authenticatie)
2. Vertrouwensdiensten (waaronder elektronische handtekeningen)

Hieronder volgt een toelichting per deel.

Deel 1. Elektronische authenticatiemiddelen

Een van de belangrijkste doelstellingen van de eIDAS-verordening is dat er werkelijk grensoverschrijdende elektronische dienstverlening mogelijk wordt. Daartoe geldt vanaf september 2018 een verplichte wederzijdse erkenning van elektronische identiteiten tussen de EU lidstaten. h En is met Uitvoeringshandeling 2015/1502 in tamelijk detail geregeld aan welke eisen authenticatiemiddelen van de verschillende niveaus dienen te voldoen. Ten slotte regelt de eIDAS-verordening ook de technische interoperabiliteit, zodat koppelingen tussen nationale stelsels voor elektronische identificatie en authenticatie met succes tot stand kunnen komen. Lidstaten zijn hiervoor verplicht de vereiste technische voorzieningen te realiseren.

Met het bovenstaande zal naar verwachting eindelijk de grensoverschrijdende elektronische dienstverlening mogelijk worden, waarvoor de Richtlijn Elektronische Handtekeningen destijds onvoldoende is gebleken.

[1] UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

De wederzijdse erkenning tussen lidstaten betreft stelsels voor elektronische identificatie en de daarin gehanteerde authenticatiemiddelen op niveaus Substantieel en Hoog. Lidstaten dienen hiertoe stelsels en middelen die voor grensoverschrijdend gebruik in aanmerking dienen te komen, te notificeren in Brussel en de andere lidstaten.

Om grensoverschrijdende toegang tot elektronische diensten te bewerkstelligen moeten elektronische identificatiemiddelen aan gemeenschappelijke eisen voldoen. Deze eisen gelden vervolgens grotendeels echter ook voor elektronische identificatiemiddelen binnen Nederland. Waar hieraan concessies gedaan mogen worden, wordt dat hieronder aangeduid.

De eisen zijn:

- Diensten waarvoor substantieel of hoog vereist wordt, moeten toegankelijk zijn voor private partijen (burgers en bedrijven) uit andere lidstaten. Een partij uit een andere lidstaat moet daarvoor het authenticatiemiddel van die andere lidstaat gebruiken. Uiteraard moet dit middel minimaal hetzelfde eIDAS-niveau hebben. Voor authenticatiemiddelen van niveau substantieel of hoog zijn de eIDAS-eisen daardoor ook nationaal van kracht.
- Middelen moeten onder dezelfde condities worden uitgegeven (wederzijdse erkenning). Op grond van overweging 14 van de eIDAS-verordening geldt dat het beginsel van wederzijdse erkenning echter alleen op authenticatie voor een onlinedienst betrekking dient te hebben. De toegang tot deze onlinediensten en de daadwerkelijke verlening ervan aan de aanvrager moeten nauw verbonden zijn aan het recht om dergelijke diensten af te nemen onder de in de nationale wetgeving gestelde voorwaarden. Nationale wetgeving kan toegang tot e-diensten verhinderen. Weigeren van toegang is gebonden aan grenzen, zoals non-discriminatiebepalingen. Dat betekent dat een burger uit een andere lidstaat, die met zijn authenticatiemiddel toegang krijgt tot de website van het UWV, niet automatisch recht heeft op een uitkering in Nederland. De elektronische toegang verandert uiteraard niets aan andere rechten en plichten.
- Middelen met niveau eIDAS laag zijn ook gedefinieerd in de verordening. Voor deze middelen geldt geen automatische Europese erkenning. Lidstaten kunnen er wel voor kiezen om specifieke middelen van niveau eIDAS laag van andere lidstaten toe te laten. Dit moet dan expliciet geregeld worden.

Deel 2. Vertrouwensdiensten

Met de Wet elektronische handtekeningen (Weh) werd de Richtlijn 1999/93/EG over een gemeenschappelijk kader voor elektronische handtekeningen geïmplementeerd. Per 1 juli 2016 is die Richtlijn komen te vervallen en is het onderdeel Vertrouwensdiensten van de eIDAS-verordening van kracht.

De Richtlijn is in Nederland geïmplementeerd door de Wet Elektronische handtekeningen (Weh). De Weh voegde de artikelen 15a en 15b toe aan Boek 3 van het Burgerlijk Wetboek. Het onderdeel Vertrouwensdiensten van eIDAS vervangt de huidige Wet elektronische handtekeningen en voegt daar nog andere vertrouwensdiensten aan toe.
Om de specifieke zaken uit de eIDAS-verordening te regelen maar ook om dubbeling in de nationale wetgeving van hetgeen is bepaald in de verordening te vermijden, is momenteel een voorstel een Implementatiewet eIDAS in parlementaire behandeling. Artikel 15a over de elektronische handtekening krijgt in dit wetvoorstel voor de Implementatiewet eIDAS een ietwat andere lezing (zie ook hoofdstuk 9). Artikel 15b komt te vervallen. Tevens worden enkele andere Nederlandse wetten, waaronder de telecommunicatiewet, aangepast.

Naast elektronische handtekeningen regelt de Verordening een aantal andere vertrouwensdiensten:
1. Elektronische zegels
2. Elektronische tijdstempels
3. Elektronische bezorgdiensten
4. Website-certificaten

Zie hiervoor ook hoofdstuk 7 van deze handreiking.

Uitgangspunt in de Verordening is dat de verlener van vertrouwensdiensten gevestigd in de ene lidstaat niet wordt belemmerd in het verlenen van zijn vertrouwensdiensten in een andere lidstaat. Voor vertrouwensdiensten regelt de Verordening onder meer de eisen waaronder deze mogen worden aangeboden op de markt, de inrichting van het toezicht daarop, een meldplicht bij veiligheidsinbreuken, de rechtsgevolgen en de grensoverschrijdende erkenning daarvan.
Daarbij wordt van deze vertrouwensdiensten zogenaamde gekwalificeerde varianten onderkend. Voor gekwalificeerde vertrouwendiensten gelden extra strenge eisen en een strenger (a priori) toezichtsregime dan voor niet-gekwalificeerde vertrouwensdiensten.

2 Algemene wet bestuursrecht

Met de Wet elektronisch bestuurlijk verkeer (Webv) is een afdeling 2.3 toegevoegd aan de Algemene wet bestuursrecht (Awb). Deze afdeling 2.3 bevat algemene regels over het verkeer langs elektronische weg tussen burgers en bestuursorganen en tussen bestuursorganen onderling. Inmiddels is ook de Wet elektronisch verkeer met de bestuursrechter van kracht geworden, een wijziging van de Awb die het elektronisch verkeer met de bestuursrechter regelt door het van overeenkomstige toepassing verklaren van afdeling 2.3 van de Awb daarop. In het onderstaande worden de artikelen van de Webv die zijn opgenomen in afdeling 2.3 van de Algemene wet bestuursrecht, kort besproken.

De hoofdlijnen van de Webv kunnen als volgt worden samengevat:

- De bepalingen over elektronisch verkeer met bestuursorganen zijn van
- toepassing op alle e-diensten die binnen de scope van deze handreiking vallen.
- Elektronisch verkeer is nevengeschikt aan conventioneel verkeer.
- De bepalingen van de Webv stellen dat elektronisch verkeer wordt aangeboden naast de mogelijkheid op papier of via bezoek aan een loket om de diensten af te nemen. Verplichtstelling van elektronisch verkeer als enige kanaal vereist een expliciete wettelijke grondslag.
- Elektronisch verkeer en het elektronisch verzenden van berichten, zoals bedoeld in deze bepalingen, moet ruim opgevat worden en omvat websites, e-mail, elektronische transacties, webservices etc.
- De Webv stelt voorwaarden die bij de uitvoering van e-diensten in acht moeten worden genomen. Dit zijn voorwaarden ten aanzien van:
  - het feit dat de verzender en de ontvanger (dus zowel bestuursorgaan als burger) eerst kenbaar moeten hebben gemaakt dat zij elektronisch bereikbaar zijn;
  - betrouwbaarheid en vertrouwelijkheid van het verkeer, gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt. Dit aspect is uiteraard belangrijk voor het classificeren van het vereiste betrouwbaarheidsniveau;
  - vereisten van ondertekening;
  - tijdstippen van verzending en ontvangst bij elektronisch verkeer.

Hierna worden deze hoofdlijnen nader uitgewerkt.

Artikel 2:13 Awb

Dit artikel bepaalt dat in het verkeer tussen burger en bestuursorgaan berichten elektronisch kunnen worden verzonden (eerste lid). Het bepaalt ook de reikwijdte van deze mogelijkheid. Bij het elektronisch verkeer moeten de bepalingen van afdeling 2.3 in acht worden genomen. Wat dat concreet betekent komt bij bespreking van de andere artikelen van afdeling 2.3 aan de orde.

Artikel 2:13 heeft betrekking op verzending in de ruimste zin van het woord. Dit begrip is in elk geval ruimer dan in het gangbare spraakgebruik. Het betreft het langs elektronische weg in kennis stellen, kennisgeven, ver-, toe-, door- en terugzenden, mededelen, bevestigen, aanzeggen, naar voren brengen, indienen, etc.

Onder 'verzenden langs elektronische weg' wordt iedere vorm van elektronische gegevensuitwisseling met een ander verstaan. Het betreft bijvoorbeeld zowel het versturen van een e-mailbericht als het plaatsen van een stuk op een website. Het betreft zowel het verkeer van de overheid naar burgers en bedrijven, als het verkeer naar de overheid toe.

Artikel 2:13 is in feite de basis voor het elektronisch uitvoeren van alle soorten diensten en processen tussen overheid en burger of bedrijf. Alleen bij wettelijk voorschrift (dat wil zeggen in een wet, AMvB of ministeriële regeling) kan deze mogelijkheid worden uitgesloten (tweede lid, onderdeel a). Tot op heden is geen wet- en regelgeving bekend waarin expliciet de mogelijkheid van elektronisch verkeer is uitgesloten. In bijlage 2 zijn enkele voorbeelden genoemd van formuleringen in wet- en regelgeving die niet als uitsluiting van elektronisch verkeer beschouwd kunnen worden.

Een tweede uitzondering op het beginsel dat verkeer tussen burger en bestuursorgaan elektronisch kan plaatsvinden is de situatie dat een vormvoorschrift zich tegen elektronische verzending van berichten verzet (tweede lid, onderdeel b). Concrete voorbeelden hiervan noemt de MvT bij het wetsvoorstel Webv niet. Wel wordt een aantal gevallen genoemd waarin vormvoorschriften die tot gebruik van papier lijken te leiden, ook elektronische 'verzending' toelaten, zoals 'per brief' (kan ook via e-mail) of 'aanplakken' (kan ook door publicatie op een site). Deze uitzondering zal elektronisch verkeer dus niet snel in de weg staan. In bijlage 2 wordt niettemin een aantal (wettelijke) vormvoorschriften genoemd die mogelijk een belemmering vormen voor elektronisch verkeer.

Artikel 2:14 Awb

Het eerste lid bepaalt dat het bestuursorgaan alleen elektronisch met de burger kan communiceren, indien de burger heeft kenbaar gemaakt dat hij via die weg bereikbaar is. Er is niet bepaald hoe die kenbaarmaking door de burger moet geschieden. Het enkel versturen van een e-mail door een burger aan een overheidsorganisatie zal in het algemeen niet voldoende zijn; er kan niet verwacht worden dat de burger per definitie op dat adres bereikbaar blijft. In bijlage 2 zijn voorbeelden van geschikte wijzen van kenbaarmaking opgenomen.

Het vereiste van kenbaarmaking geeft uitdrukking aan het beginsel van nevenschikking in de Webv: (de toename van) het elektronisch verkeer mag niet ten koste gaan van degenen die daar geen gebruik van kunnen maken. Voor die personen moet de overheid via de conventionele, papieren weg bereikbaar blijven. Het tweede lid bepaalt dat berichten die niet tot een of meer geadresseerden zijn gericht (openbare kennisgevingen, terinzagelegginen van bestemmingsplannen e.d.) niet uitsluitend elektronisch worden verzonden. Dit houdt in dat, naast de openbare kennisgeving langs elektronische weg, de kennisgeving plaatsvindt in een van overheidswege uitgegeven informatieblad of een dag-, nieuws- of huis-aan-huisblad, of op een andere geschikte wijze (vergelijk artikel 3:12 en 3:42 Awb). De stukken moeten ook op conventionele wijze (bijvoorbeeld op het stadhuis) ter inzage worden gelegd.

Het derde lid van artikel 2:14 noemt een ander belangrijk uitgangspunt van de Wet elektronisch bestuurlijk verkeer, namelijk betrouwbaarheid en vertrouwelijkheid van het berichtenverkeer. Indien een bestuursorgaan een bericht elektronisch verzendt, dan dient dit op een voldoende betrouwbare en vertrouwelijke manier te geschieden, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt.

De MvT bij de Webv onderscheidt drie maten van betrouwbaarheid en vertrouwelijkheid:

- *Maximale betrouwbaarheid en vertrouwelijkheid*
  Hiervan is sprake indien de beveiliging geheel conform de maximale (technische) mogelijkheden plaatsvindt.
- *Voldoende betrouwbaarheid en vertrouwelijkheid*
  Hiervan is sprake indien de veiligheid even groot is vergeleken met de situatie dat er uitsluitend van conventioneel verkeer gebruik zou worden gemaakt.
- *Pro-formabetrouwbaarheid en vertrouwelijkheid*
  Hiervan is sprake indien de beveiliging slechts één stap verwijderd is van het bieden van geen enkele beveiliging. Gedacht kan worden aan een (elektronische) mededeling ‘verboden toegang’.

Voor de goede orde: deze drie maten hebben ***geen*** directe relatie met de drie niveaus van betrouwbaarheid zoals de eIDAS-verordening deze bepaalt.

De wetgever beoogt met de eis van betrouwbaarheid en vertrouwelijkheid uitdrukking te geven aan de zogenaamde algemene beginselen van behoorlijk IT-gebruik. Hieronder worden verstaan de beginselen van authenticiteit, integriteit, onweerlegbaarheid, transparantie, beschikbaarheid, flexibiliteit en vertrouwelijkheid. Concreet kunnen deze beginselen bijvoorbeeld worden gewaarborgd met techniek waarmee een elektronische handtekening kan worden gezet, met een tijdsstempel of met behulp van cryptografische technieken (versleuteling).

Volgens de wetgever moet worden gestreefd naar de middelste optie van voldoende betrouwbaarheid en vertrouwelijkheid. Er dienen vergelijkbare waarborgen te worden geboden als de waarborgen die het 'papieren verkeer' biedt. De wetgever vindt het niet gewenst om in de elektronische situatie een hogere mate van betrouwbaarheid en vertrouwelijkheid te eisen dan bij conventionele communicatie.

Bij niveau hoog is sprake van maximale betrouwbaarheid en veiligheid, bijvoorbeeld voor toegang tot patiëntgegevens[2]. Daarmee vormen de eIDAS-niveaus en de in Nederland beschikbare middelen voor authenticatie een invulling van de open norm uit de Awb.

Ondanks de samenhang in de normen voor betrouwbaarheid op nationaal en EU-niveau, is in algemene zin moeilijk te zeggen wanneer in de praktijk sprake is van een voldoende mate van betrouwbaarheid en vertrouwelijkheid. De hoofdregel is dat aard en inhoud van een bericht en het doel waarvoor het wordt gebruikt, bepalend zijn voor de mate van betrouwbaarheid en vertrouwelijkheid die vereist is. Aan de verlening van een vergunning dienen bijvoorbeeld hogere eisen te worden gesteld dan aan het verstrekken van algemene informatie. Praktisch gezien betekent een en ander dat de norm van een betrouwbare en vertrouwelijke communicatie uitwerking zal moeten vinden in het beleid van het desbetreffende bestuursorgaan. Het toepassen van deze handreiking en het vastleggen van het vereiste betrouwbaarheidsniveau voor de eigen diensten is onderdeel van een dergelijk beleid.

[2] Zie het rapport 'Patientauthenticatie' van J.Krabben (PrivacyCare) en T.Hooghiemstra (PBLQ) in opdracht van de minister van VWS: *https://www.rijksoverheid.nl/documenten/rapporten/2016/08/25/bijlage-vi-onderzoek-betrouwbaarheidsniveau-patientauthenticatie*

Artikel 2:15 Awb

Het eerste lid van artikel 2:15 vormt als het ware het spiegelbeeld van het eerste lid van artikel 2:14. Het regelt dat ook het bestuursorgaan moet hebben aangegeven elektronisch bereikbaar te zijn. Deze zogenoemde openstelling van de elektronische weg door het bestuursorgaan kan zowel geschieden in een algemene regeling als in een bericht aan één of meer geadresseerden.
Het bestuursorgaan kan nadere eisen stellen aan het gebruik van de elektronische weg (eerste lid, tweede volzin), met het oog op een uniforme behandeling en een veilig dataverkeer. Zo kan een bestuursorgaan vereisen dat gebruik wordt gemaakt van een bepaald elektronisch postadres. Ook kan gedacht worden aan meer technische vereisten zoals het gebruik van bepaalde software of het gebruik van bepaalde elektronische (intelligente) formulieren. Voor massale processen kan een specifiek kanaal voor een specifieke berichtensoort met specifieke eisen worden opengesteld. Ook het vaststellen van betrouwbaarheidsniveaus voor bepaalde processen of diensten kan hieronder worden begrepen. De nadere eisen kunnen worden vastgesteld in overleg met betrokkenen. De in overleg gemaakte afspraken kunnen worden vastgelegd in een uitwisselingsprotocol. Een uitwisselingsprotocol bevat onder meer de normen en standaarden die nodig zijn voor de communicatie en berichtdefinities die noodzakelijk zijn voor de automatische verwerking van de gegevens.

Bij de openstelling van de elektronische weg zullen eigenlijk altijd nadere eisen nodig zijn om het elektronisch verkeer daadwerkelijk te realiseren. De nadere eisen zullen dus vaak fysieke voorzieningen ter ondersteuning van een effectief en efficiënt berichtenverkeer – gericht op het hele proces van verwerking – betreffen. Ze zijn dan ook vaak niet in een besluit of regeling van het bestuursorgaan vastgelegd. Indien een bestuursorgaan het beginsel van nevenschikking hanteert, en het elektronisch berichtenverkeer een aanvulling vormt op de conventionele weg, kunnen de eisen gezien worden als beleidsinvulling. Indien een burger of bedrijf zich daaraan niet wil conformeren, heeft hij de keuze om van de conventionele (schriftelijke) weg gebruik te maken. Waar het elektronisch berichtenverkeer expliciet verplicht is gesteld, met uitsluiting van de conventionele, papieren weg, ligt het in de rede om deze nadere eisen in algemeen verbindende voorschriften op te nemen. Het verplichte karakter en de consequenties die eventueel aan niet naleving van die verplichtingen verbonden worden, rechtvaardigen een wettelijke grondslag.

Dezelfde lijn kan worden gevolgd ten aanzien van betrouwbaarheidseisen aan de elektronische weg. Als deze eisen zich beperken tot het aanwijzen van een betrouwbaarheidsniveau, dan kan dat gezien worden als

beleidsinvulling, waarbij de gebruiker de mogelijkheid heeft om een middel voor identificatie en authenticatie te kiezen dat aan dit betrouwbaarheidsniveau voldoet. Als een specifiek middel voor identificatie en authenticatie wordt voorgeschreven, bestaat die keuzemogelijkheid niet meer en ligt een wettelijke grondslag voor de verplichting voor de hand.

Het tweede en derde lid van artikel 2:15 geven weigeringsgronden voor een elektronisch bericht. Het bestuursorgaan kan een bericht weigeren indien verwerking ervan tot onaanvaardbare last zou leiden, of indien de betrouwbaarheid en de vertrouwelijkheid van dit bericht onvoldoende gewaarborgd zijn. Onder voldoende betrouwbaar en vertrouwelijk wordt hier hetzelfde verstaan als in artikel 2:14, derde lid.

Artikel 2:16

De verwijzing in artikel 2:16 Awb naar de vereisten voor een elektronische handtekening in artikel 3:15a, tweede tot en met zesde lid is komen te vervallen, omdat deze bepalingen in het Burgerlijk Wetboek eveneens vervallen. De verordening geeft eigen regels over de onderwerpen die in deze artikelen geregeld waren. In de uitvoeringswet komt een nieuw artikel met de strekking dat een handtekening voldoende betrouwbaar moet zijn voor het proces waarvoor deze wordt gebruikt en dat bij wet bepaalde elektronische handtekeningen voorgeschreven kunnen worden al dan niet met specifieke eisen. Uitzondering zijn de geavanceerde handtekening en de gekwalificeerde handtekening, want daar regelt de verordening de eisen uitputtend voor.

Artikel 2:17

Dit artikel regelt de tijdstippen van verzending en ontvangst van een elektronisch bericht. Dit is van belang voor het bepalen van de aanvang van de bezwaar- of beroepstermijn.
Het eerste lid bepaalt dat als moment van verzending door een bestuursorgaan geldt het tijdstip waarop het bericht een systeem bereikt waarover het bestuursorgaan geen verantwoordelijkheid draagt. Als het bestuursorgaan en de geadresseerde gebruikmaken van hetzelfde systeem voor gegevensverwerking, is dit het moment waarop het toegankelijk wordt voor de geadresseerde. Deze bepaling ziet toe op de situatie dat de betrokkenen daadwerkelijk gebruikmaken van hetzelfde systeem. Een voorbeeld is het elektronisch verzenden van stukken tussen het college van Burgemeester en Wethouders en de gemeenteraad. In het verkeer tussen overheid en burger zal hiervan nooit sprake zijn. Volgens het tweede lid geldt als moment van ontvangst door een bestuursorgaan het tijdstip waarop het bericht van een burger het systeem van het bestuursorgaan heeft bereikt.

3 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) (aangescherpt per 1 januari 2016) is 1 juli 2016 vervangen door de Algemene Verordening Gegevensbescherming en van toepassing per 25 mei 2018. Een uitvoeringswet, zoals bij eIDAS, volgt nog. In het navolgende wordt nog uitgegaan van de Wbp.

De Wbp is van toepassing voor zover in het (elektronisch) verkeer tussen overheid en burgers/bedrijven persoonsgegevens aan de orde zijn. Artikel 1, onderdeel a, Wbp definieert een persoonsgegeven als: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Dat betreft bijvoorbeeld:

- Achternamen, voornamen
- Persoonlijk e-mailadres
- Telefoonnummer
- BSN
- Persoonsgebonden certificaat

De Wbp stelt in de artikelen 6 tot en met 14 strikte eisen aan het verzamelen, verwerken en bewaren van persoonsgegevens. Deze eisen betreffen onder meer:

- De verwerking vindt plaats ter uitvoering van publiekrechtelijke taken of er is sprake van uitdrukkelijke toestemming van degene van wie gegevens worden verwerkt.
- De verwerking moet overeenstemmen met het doel waarvoor de gegevens verkregen zijn.
- De verantwoordelijke voor de verwerking voorziet in passende technische en organisatorische maatregelen om verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen.

Artikel 16 Wbp stelt extra eisen aan bijzondere persoonsgegevens, zoals gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, en gegevens over het lidmaatschap van een vakvereniging, en strafrechtelijke persoonsgegevens. Voor deze persoonsgegevens geldt in beginsel een verbod op verwerking.

De artikelen 17 tot en met 22 bepalen welke instanties onder welke voorwaarden dergelijke persoonsgegevens wel mogen verwerken. Ook hier geldt een uitzondering op het verwerkingsverbod indien er een wettelijke grondslag is voor verwerking of indien de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking (artikel 23). Daarnaast kan de Autoriteit Persoonsgegevens ontheffing verlenen voor de verwerking van (deze) gegevens. Belangrijk is dat onder persoonsgegevens niet enkel de

identificerende kenmerken zelf worden verstaan, maar ook daarmee in combinatie getoonde gegevens die kunnen worden teruggebracht tot een bepaalde persoon, zoals gegevens over de financieel-economische of persoonlijke situatie. Om diezelfde reden zijn telefoonnummers, kentekens van auto's, postcodes met huisnummers en het BSN als persoonsgegevens te beschouwen.

De Autoriteit Persoonsgegevens heeft Richtsnoeren voor de Beveiliging van Persoonsgegevens uitgegeven. Zie paragraaf 4.3. van de hoofdtekst.

In artikel 10 van de voorgestelde uitvoeringswet in verband met de uitvoering van de eIDAS-verordening worden verleners van vertrouwensdiensten uitgezonderd van de meldplicht op grond van artikel 34a Wbp (meldplicht datalekken). De meldplicht door verleners van vertrouwensdiensten aan de Autoriteit Persoonsgegevens is in het wetsvoorstel door middel van een wijziging in de Telecommunicatiewet geregeld. Dit biedt de mogelijkheid specifiek rekening te houden met de rechtstreekse werking van de verordening.

4 Regelgeving inzake informatiebeveiliging

Naast de Wbp bestaan voor de rijksdienst (ministeries en daaronder direct ressorterende diensten) regelingen inzake informatiebeveiliging. Deze richten zich met name op de maatregelen die een (onderdeel van) een ministerie intern neemt op dit gebied. De toepassing hiervan kan echter relevant zijn voor het bepalen van het betrouwbaarheidsniveau voor een bepaalde dienst. De maatregelen voor informatiebeveiliging in de backoffice kunnen ertoe leiden dat aan de 'poort' met een lager betrouwbaarheidsniveau kan worden volstaan.

Zoals in hoofdstuk 2 gesteld, is de aandacht voor informatiebeveiliging de afgelopen jaren sterk toegenomen. Dit volgt de maatschappelijke ontwikkeling en de sterke groei van het gebruik van online diensten. Dit heeft geleid tot diverse voorschriften, normen en richtlijnen. Deze handreiking richt zich specifiek op betrouwbaarheidsniveaus die benodigd zijn voor online diensten van de overheid. Daarbij wordt ervan uitgegaan dat deze diensten voor andere aspecten de geldende normen volgen. In hoofdstuk 2 is de Norm ICT-beveiligingsassessments DigiD al genoemd, tezamen met de onderliggende richtlijnen van het NCSC. Welke voorschriften zijn verder van belang voor een overheidsorganisatie?

Voor onderdelen van het Rijk geldt het Voorschrift informatiebeveiliging 2007 (VIR 2007). Dit stelt onder andere dat informatiebeveiliging onderdeel is van de gewone control-cyclus en een verantwoordelijkheid is van het lijnmanagement. Hoe hieraan invulling moet worden gegeven, is uitgewerkt in het tactische normenkader Baseline Informatiebeveiliging Rijksdienst (BIR2012). Voor gemeenten en diverse andere overheden zijn vergelijkbare uitwerkingen gemaakt. Deze zullen opgaan in een overheidsbrede baseline. Al deze voorschriften zijn in feite een toepassing van de ISO 27001/27002-standaard voor de overheid. Deze standaard valt onder de *comply or explain*-lijst van Forum Standaardisatie[3]. Dat wil zeggen dat alle overheden linksom of rechtsom met deze voorschriften voor informatiebeveiliging te maken hebben.

Diverse zaken die in het kader van informatiebeveiliging zijn voorgeschreven kunnen hergebruikt worden om deze classificatie uit te voeren. De classificatie kan ook goed tegelijk worden uitgevoerd met een Quickscan BIR. De handreiking gaat dieper in op de interactie met burgers in e-diensten. De Quickscan BIR kijkt daarnaast breed naar interne aspecten zoals de bij een proces gebruikte IT-systemen en de vereiste beschikbaarheid. Indien uit de Quickscan BIR blijkt dat voor een bepaalde dienst een hoger risico geldt dan hetgeen door de BIR wordt afgedekt, dan volgt daaruit ook dat de hier voorgestelde vereenvoudigde risicoanalyse onvoldoende is. De voorschriften voor informatiebeveiliging en deze classificatie zijn dus beide nodig en vullen elkaar aan.

Voorschrift informatiebeveiliging rijksdienst 2007 (VIR 2007)

Een van de bedoelde regelingen is het Besluit voorschrift informatiebeveiliging rijksdienst 2007. Informatiebeveiliging betekent in dit besluit: het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen. Informatiebeveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen. De secretaris-generaal is ingevolge het besluit verantwoordelijk voor het vaststellen en uitdragen van en het verantwoorden over het

[3] Voor zover toepassing van ISO 27001 / 27002 en daarvan afgeleide overheidsvoorschriften op basis van comply of explain nog te relativeren is, geldt dat de nieuwe versie van de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC inmiddels naast de al bestaande technische maatregelen ook voor de organisatorische maatregelen een vergelijkbaar niveau voorschrijft. Te verwachten valt dat dit bij een volgende versie van de DigiD beveiligingsnorm een onontkoombaar voorschrift wordt. Dezelfde verwachting geldt voor de eisen die vanuit het Idensys stelsel aan afnemers gesteld gaan worden.

informatiebeveiligingsbeleid van zijn ministerie. Taken die het besluit in het verlengde hiervan aan het lijnmanagement opdraagt, zijn:

- Op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor de informatiesystemen vaststellen.
- Het toepassen van deze handreiking en vervolgens vastleggen van de daaruit volgende afweging zijn hier onderdeel van. Deze handreiking gaat daarbij enkel in op de betrouwbaarheidseisen, uitgedrukt in niveaus, voor elektronische toegang door externe gebruikers c.q. afnemers van een dienst.
- Het bepalen, implementeren en uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen.
- Vaststellen dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd.
- Voor overheidsbrede voorzieningen voor elektronische toegang zoals DigiD, PKIoverheid en eHerkenning geldt dat deze aantoonbare overeenstemming volgt uit het door de voor deze voorzieningen verantwoordelijke dienstverleners afgegeven betrouwbaarheidsniveau.
- Het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen periodiek evalueren en waar nodig bijstellen.

Baseline Informatiebeveiliging Rijksdienst (BIR)

Naast het procesgerichte VIR is er inmiddels een gemeenschappelijke baseline geformuleerd voor de rijksoverheid, die in 2012 is vastgesteld. Het BIR is inhoudelijk gericht. Het gaat om de gemeenschappelijke maatregeldoelstellingen en maatregelen, waarbij men zich baseert op de ISO 27001 en 27002-richtlijnen, aangevuld met specifieke maatregelen voor de rijksoverheid. Het gaat daarbij, net als in het VIR, om beschikbaarheid, integriteit en vertrouwelijkheid.

Het niveau van de baseline betreft Departementaal Vertrouwelijk en Wbp Risicoklasse II verhoogd (grofweg analoog aan de in hoofdstuk 5 gepresenteerde klasse II). Het BIR wordt geacht verplicht te zijn, met die aantekening dat men wel de toepasselijke maatregelen kan selecteren.

Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie (VIR-BI)

Naast het VIR geldt een apart besluit voor bijzondere informatie. Dit besluit geeft aan hoe binnen de rijksdienst omgegaan wordt met zogenoemde vertrouwelijke informatie in de zin van staatsgeheim. De laagste klasse daarvan is departementaal vertrouwelijk, wat ook het niveau is waarvoor het BIR een baseline biedt. Het VIR-BI is echter beperkt tot het aspect vertrouwelijkheid.

In de gevallen waar een onderdeel van de rijksdienst gebruiker is van elektronische diensten (bijvoorbeeld bij het aanvragen van een vergunning door een ministerie), zou dit besluit direct van toepassing kunnen zijn op informatie die in het kader daarvan wordt verstrekt.

Voor het overige biedt het een analogie. De rubricering staatsgeheim valt buiten de scope van deze handreiking. De rubricering departementaal vertrouwelijk is gebruikelijk voor onder andere aanbestedingsinformatie en kan als analogie worden gezien met wat een bedrijf als ernstig concurrentie- of economisch gevoelig beschouwt.

Naast de BIR zijn er ook voor andere overheden baselines van kracht (BIG, IBI, WABI). Dit betreft echter niet zozeer wettelijke verplichtingen maar daar gaat het om bestuurlijke afspraken.

5 Wet algemene bepalingen burgerservicenummer

Een belangrijke voorziening ten behoeve van identificatie en authenticatie van personen is het burgerservicenummer (BSN). De Wet algemene bepalingen burgerservicenummer geeft regels over onder andere uitgifte en gebruik van dit nummer.

De wet regelt dat alle overheidsorganen het nummer mogen gebruiken bij het verwerken van persoonsgegevens in het kader van hun publieke taak, zonder dat daarvoor nadere regelgeving vereist is. Voor het gebruik buiten de kring van overheidsorganen blijft een specifieke wettelijke grondslag nodig.

Het kan wel noodzakelijk zijn om de publieke taak als zodanig vast te leggen in de wet (als het bijvoorbeeld een nieuwe taak betreft in het kader waarvan de verwerking van het BSN gaat plaatsvinden).

Aan de beheervoorziening BSN kan langs elektronische weg de vraag worden gesteld of aan een bepaalde persoon een burgerservicenummer is toegekend en zo ja, welk burgerservicenummer. Op deze wijze kan het burgerservicenummer van een bepaalde persoon worden nagetrokken. Aan de beheervoorziening kan verder de vraag worden gesteld op welke persoon een bepaald burgerservicenummer betrekking heeft. Daarmee kan gecontroleerd worden of het burgerservicenummer dat een persoon opgeeft, inderdaad betrekking heeft op de persoon in kwestie, onder meer door vergelijking van de gegevens op een (Nederlands of buitenlands) identiteitsdocument.

De manieren van vergewissen berusten dus niet op de vermelding van het burgerservicenummer op een identiteitsdocument, maar zijn toepasbaar op alle personen die een burgerservicenummer krijgen toegekend. Door het burgerservicenummer te koppelen aan DigiD, kan de burger zich op een betrouwbare manier elektronisch kenbaar maken aan de overheid.

6 Wetboek van Burgerlijke Rechtsvordering

Als gevolg van de eIDAS-verordening wordt in artikel 1072b, derde lid, van het Wetboek van Burgerlijke Rechtsvordering de zinsnede 'een elektronische handtekening die voldoet aan het bepaalde in artikel 15a, eerste en tweede lid, van Boek 3 van het Burgerlijk Wetboek' vervangen door: 'een gekwalificeerde handtekening als bedoeld in artikel 3, onderdeel 12, van 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 (PbEU 2014, L 257).'

Artikel 156a van het Wetboek van Burgerlijke Rechtsvordering (Rv) bevat bepalingen over het opmaken van elektronische onderhandse akten. Onderhandse akten zijn stukken die tot bewijs kunnen of moeten dienen in het rechtsverkeer. Het kan hierbij ook gaan om bescheiden die bij een aanvraag voor een vergunning moeten worden overgelegd. Om die reden is dit artikel ook voor elektronische diensten relevant.

Voor de invoering van artikel 156a Rv moesten onderhandse akten op papier worden opgemaakt om het gewenste bewijs te kunnen leveren. De toevoeging van het artikel maakt onder meer het opmaken en verstrekken van elektronische verzekeringspolissen mogelijk. Het artikel luidt:

Artikel 156a

1. *Onderhandse akten kunnen op een andere wijze dan bij geschrift worden opgemaakt op zodanige wijze dat het degene ten behoeve van wie de akte bewijs oplevert, in staat stelt om de inhoud van de akte op te slaan op een wijze die deze inhoud toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de akte bestemd is te dienen, en die een ongewijzigde reproductie van de inhoud van de akte mogelijk maakt.*

2. *Aan een wettelijke verplichting tot het verschaffen van een onderhandse akte kan alleen op een andere wijze dan bij geschrift worden voldaan met uitdrukkelijke instemming van degene aan wie de akte moet worden verschaft. Een instemming ziet, zolang zij niet is herroepen, eveneens op het verschaffen van een gewijzigde onderhandse akte. Het in de eerste zin van dit lid bepaalde lijdt uitzondering indien de akte eveneens is ondertekend door degene aan wie de akte op grond van de wet moet worden verschaft.*

Artikel 156a, eerste lid, Rv vereist dat de wijze van opmaken van de akte een ongewijzigde reproductie van de inhoud van de akte mogelijk maakt. Deze formulering is ontleend aan het begrip duurzame drager in de Wet op het financieel toezicht.

Duurzame drager wordt in artikel 1:1 van die wet gedefinieerd als: 'een hulpmiddel dat een persoon in staat stelt om aan hem persoonlijk gerichte informatie op te slaan op een wijze die deze informatie toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de informatie kan dienen, en die een ongewijzigde reproductie van de opgeslagen informatie mogelijk maakt.' Deze eis gaat niet zo ver dat degene die de akte opmaakt een ongewijzigde reproductie van de opgeslagen informatie moet garanderen. Als reden hiervoor is aangevoerd dat hij geen invloed heeft op de keuze van het hulpmiddel (CD-rom, USB-stick) waarop degene ten behoeve van wie de akte bewijs oplevert, de akte opslaat.
Voor de ondertekening van elektronische onderhandse akten wordt in het algemeen een elektronische handtekening als bedoeld in artikel 3:15a Burgerlijk Wetboek vereist. De vraag of voor een bepaalde onderhandse akte een gewone, een geavanceerde of een gekwalificeerde handtekening is vereist, hangt af van het doel waarvoor de gegevens worden gebruikt en van alle overige omstandigheden van het geval. In artikel 156a Rv wordt daarom niet bepaald welke elektronische handtekening is vereist.

Anders dan voor de elektronische handtekening kent de wet geen algemene bepaling waarin aangegeven is onder welke voorwaarden een elektronisch document dezelfde rechtsgevolgen heeft als een papieren document (een geschrift). Wel is voor specifiek omschreven gevallen aangegeven dat waar de wet de eis van schriftelijkheid stelt, daaraan ook langs elektronische weg kan worden voldaan. Voorbeelden daarvan zijn artikel 6:227a Burgerlijk Wetboek over de totstandkoming van overeenkomsten en artikel 1021 Rv over de arbitrageovereenkomst.

Artikel 156a Rv bepaalt alleen onder welke voorwaarden onderhandse akten tot stand kunnen komen.

Bijlage 2 Voorbeelden van invulling van de wettelijke kaders en vertaling van papieren naar elektronische situatie

In deze bijlage worden voorbeelden gegeven van invulling van de vereisten uit de wettelijke regels inzake elektronisch verkeer tussen overheid en burgers. Verder is, op basis van het in bijlage 1 beschreven algemene wettelijk kader en enkele bijzondere wetten die elektronisch verkeer met de overheid regelen, aangegeven hoe de papieren situatie zich vertaalt naar de elektronische.

1 Verzenden van elektronische berichten

Artikel 2:13 Awb verstaat onder 'verzenden langs elektronische weg' iedere vorm van elektronische gegevensuitwisseling met een ander. Dat biedt veel meer opties voor communicatie tussen overheid en burger dan in het conventionele, papieren verkeer. Voorbeelden zijn:

- Versturen en ontvangen van een faxbericht of e-mail met inhoudelijke informatie. Geautomatiseerde berichtuitwisseling (bijvoorbeeld een fiscale aangifte of jaarrekening in de XBRL-standaard).
- Invullen van een formulier op een webportaal. Ook in het geval dat dit niet tot een voor de invuller zichtbaar 'bericht' leidt, kan het door de overheidsorganisatie in haar systeem ontvangen formulier als elektronisch bericht in de zin van de Awb beschouwd worden.
- Het vanuit een applicatie verzenden van een bericht (zoals de aangifte inkomstenbelasting via het van de site van de Belastingdienst gedownloade aangifteprogramma).
- Een sms-bericht van een overheidsorganisatie aan een burger of (medewerker van een) bedrijf (zoals de sms met eenmalige authenticatiecode bij DigiD).
- Een sms-bericht van een burger of (medewerker van een) bedrijf aan een overheidsorganisatie (zoals de sms'en waarmee schippers een doorvaart aan de dienst Binnenwaterbeheer van de gemeente Amsterdam kunnen melden).
- Een notificatie per e-mail van een overheidsorganisatie dat een bericht is klaargezet op een persoonlijke webpagina.
- Het inloggen op een portaal om een daar klaargezet bericht in te zien en/of te downloaden (zoals bij de Berichtenbox in *Mijnoverheid.nl*).
- Het beschikbaar stellen van een stuk op een openbare website van een overheidsorganisatie. NB: hier gaat het om een bericht dat 'niet tot een of meer geadresseerden is gericht' dus het publiceren van de informatie op een site kan niet de enige manier van informatieverstrekking zijn. (Dit zal vergezeld moeten gaan van terinzagelegging op het stadhuis en/of publicatie in een huis-aan-huisblad.)
- Een app voor het melden van gebreken (losliggende tegels, kapotte speeltoestellen en dergelijke) in de openbare ruimte.

Voorbeelden van 'verzending van elektronische berichten' die vermoedelijk niet onder artikel 2:13 Awb vallen:

- Een tweet op Twitter (maar waarschijnlijk wel als middel om 'ongeadresseerde' berichten te verspreiden, zij het niet als enig medium (zie bijlage 1, onderdeel 1, bij artikel 2:14 Awb)0.
- Een chat met een ambtenaar (vergelijkbaar met een telefoongesprek).
- Een telefoongesprek, ook al gaat dat in vergelijkbare berichten over internet (Voice over Internet Protocol (VoIP)).

2 Tijdstip van verzending en ontvangst

In het algemeen ligt het risico voor het verzenden van berichten via de elektronische weg bij de verzender, of dit nu een burger of bestuursorgaan is. Bij het verzenden van een elektronisch bericht aan een bestuursorgaan zal de verzender dan ook moeten bijhouden of en wanneer het bericht verzonden is. Bij twijfel moet hij nagaan of het bericht ontvangen is. Ook moet de verzender actief checken op status en voortgang, en in de gaten houden of het bericht (bijvoorbeeld om redenen van technische verwerkbaarheid) geweigerd wordt. Als de verzender een verzendjournaal kan overleggen, heeft hij daarmee in het algemeen voldoende aannemelijk gemaakt dat het bericht is verzonden. Het is dan aan de ontvanger om de ontvangst van het bericht 'op een niet ongeloofwaardige manier te ontkennen'.

Artikel 3:36 van de eIDAS-verordening definieert een 'dienst voor elektronisch aangetekende bezorging' als: 'een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen.'

Het bestuursorgaan is niet verplicht om een ontvangstregistratie of logfiles bij te houden. Als een ontvangstregistratie ontbreekt is het echter voor het bestuursorgaan moeilijker om 'niet ongeloofwaardig te ontkennen' dat hij het bericht heeft ontvangen. Met andere woorden: hij moet overtuigend aantonen dat het bericht niet is ontvangen. Als het bestuursorgaan daarin slaagt, dan moet de verzender op zijn beurt aannemelijk maken dat het bericht desondanks wel is ontvangen. In de jurisprudentie over artikel 2:17 Awb gaat het voornamelijk om het verzenden van berichten (bijvoorbeeld bezwaarschriften, aanvragen) per fax of e-mail. Ook bij verzending via applicatie-applicatieverkeer (zie hoofdstuk 2) is artikel 2:17 echter relevant

en geldt dat de verzender het risico draagt voor elektronische verzending. Bij applicatie-applicatieverkeer (zie ook hoofdstuk 6) kan het ook zijn dat berichten niet (direct) aan het bestuursorgaan worden gestuurd, maar via een generieke voorziening (een elektronisch postkantoor). Voorbeeld hiervan is Digipoort, voor berichten van ondernemers of hun intermediairs (e-facturen, belastingaangiftes) aan de overheid. Digipoort stuurt een ontvangstbevestiging die als bewijs dient dat 'het bericht het systeem van het bestuursorgaan heeft bereikt', zoals artikel 2:17 Awb vereist. Een eenvoudige transactiecode kan hiervoor volstaan, als het belang erg groot is kan een gewaarmerkt bericht, van een tijdsstempel voorzien, toegepast worden.

3 Kenbaarmaking

Zowel de burger als de overheidsorganisatie moeten kenbaar maken dat de elektronische weg openstaat. Wat betreft kenbaarmaking door de burger moet 'voldoende betrouwbare' informatie beschikbaar zijn over het elektronische adres waar hij bereikbaar is. Opties die daaraan voldoen zijn:

- Registreren op een portaal waarop informatie voor hem kan worden klaargezet.
- Het actief verstrekken van een e-mailadres waarop men bereikbaar is.

Het feit dat eerder vanaf een e-mailadres een bericht aan de overheidsorganisatie is verzonden, geldt niet per definitie als voldoende betrouwbare informatie omtrent de elektronische bereikbaarheid.

Ook aan de zijde van de overheidsorganisatie geldt dat de enkele beschikbaarheid van een elektronisch adres nog niet betekent dat daarmee voor alle mogelijke handelingen de elektronische weg openstaat. Ook kan de buitenwereld uit het feit dat er eerder per e-mail is gecorrespondeerd met de overheidsorganisatie niet afleiden dat de elektronische weg open staat in de zin van de Awb. Dit vereist een actieve kenbaarmaking door de overheidsorganisatie, bijvoorbeeld door middel van:

- Een brochure.
- Een mededeling in een huis-aan-huis-blad of op een website, waarin wordt aangegeven waar op het internet aanvragen voor bepaalde vergunningen kunnen worden gedaan, klachten kunnen worden ingediend, et cetera.
- Een openstellingsbesluit, zoals de Belastingdienst destijds heeft vastgesteld.

Bijlage 3 Begrippenkader

Het verschil met eerdere versies van deze handreiking is dat in deze versie is aangesloten bij de definities in de eIDAS-verordening. De verschillende vertalingen van de verordening bevatten niet altijd exact dezelfde definitie. Dit wordt door de verschillende talen veroorzaakt.

Het zijn definities specifiek voor elektronische diensten. Zo hanteren wij de definities in de handreiking ook. Een papieren paspoort valt derhalve niet onder de definitie van 'authenticatiemiddel' in deze handreiking. Het proces waarin iemands WID-document gecontroleerd wordt als onderdeel van het registratie- en uitgifteproces van een authenticatiemiddel, rekenen we niet als 'authenticatie.

Begrippen:

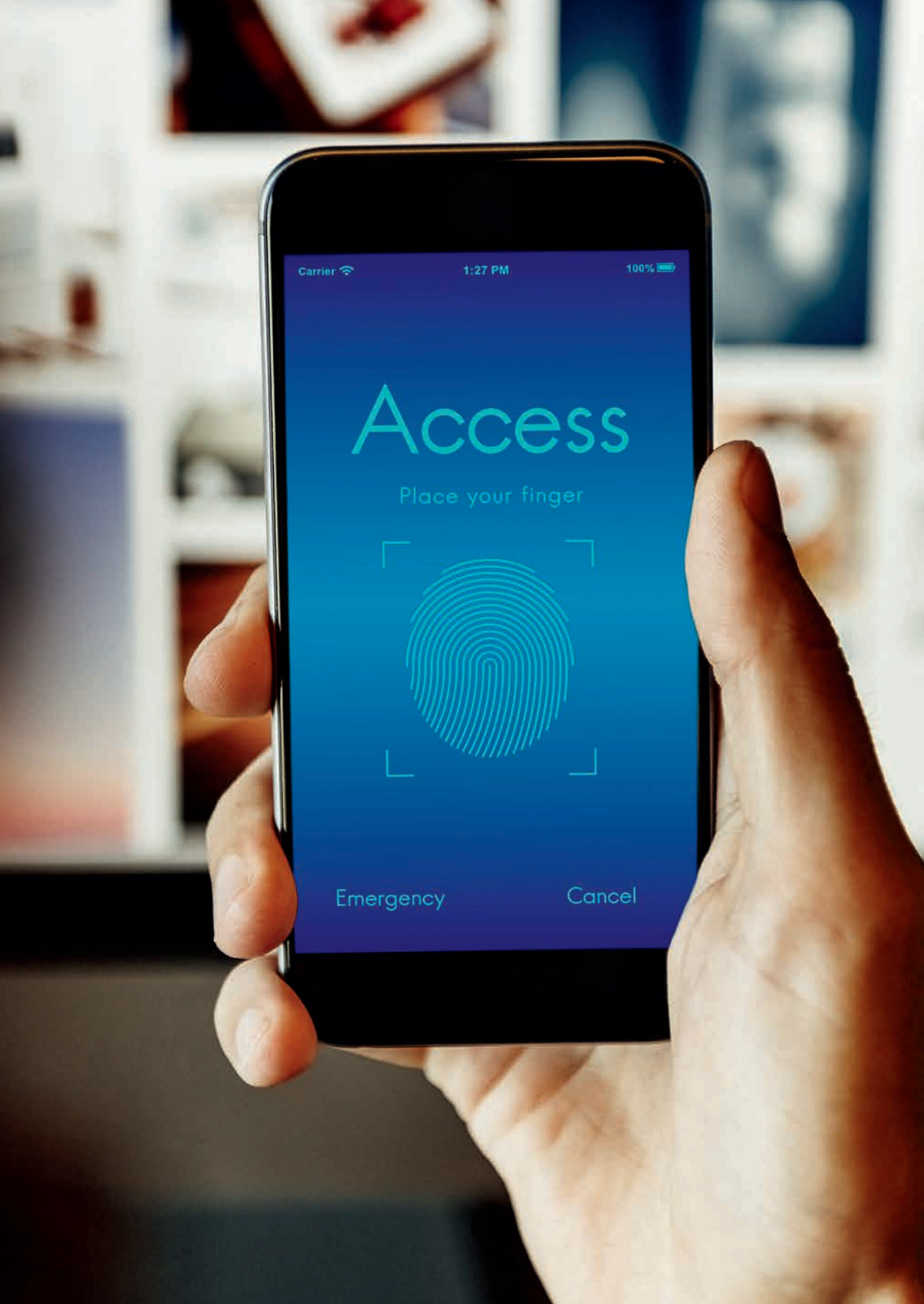
Begrip	Toelichting
Persoon	Een natuurlijke- of niet-natuurlijke persoon. Een persoon is drager van rechten.
Authenticatie	De bevestiging (het staven) van de (een) geclaimde identiteit van een persoon aan de hand van zijn authenticatiemiddel. De geclaimde identiteit is de 'elektronische identificatie' (zoals eIDAS deze definieert, zie hieronder). Voordat de persoon toegang krijgt tot een dienst moet deze bevestigd kunnen worden. Dat laatste noemen we 'authenticatie'.
Authenticatiemiddel	Een combinatie van bezit, kennis en eigenschappen, die persoonsgebonden is, die een bepaalde persoon uniek aanduidt en gebruikt kan worden voor authenticatie bij een online dienst. Aan de hand van de verificatie van bezit, kennis en eigenschappen kan de geclaimde identiteit op een bepaald betrouwbaarheidsniveau worden bewezen. Deze 'combinatie' kan gezien worden als een 'verzameling gegevens' of een 'reeks gegevens', zoals de verordening stelt. Dit zijn dan 'persoonsidentificatiegegevens' als gedefinieerd in de verordening (zie hieronder). 'Gegevens' dient ruim verstaan te worden omdat een authenticatiemiddel zoals de verordening stelt 'een materiële en/of immateriële eenheid' is. Een wachtwoord dat alleen in iemands geheugen vastligt is zo'n immaterieel onderdeel van de 'combinatie'. 'Combinatie' wil ook zeggen dat zowel in het uitgifteproces als bij het gebruik de gehele verzameling steeds volledig en in samenhang benut moet worden.
Betrouwbaarheidsniveau	Een niveau van zekerheid dat wordt geboden door vertrouwensdiensten in hun processen voor authenticatie, registreren van, beheren van machtigingen, et cetera.
Conventioneel verkeer	Verkeer, dat wil zeggen communicatie en/of berichten, waarbij berichten op papier worden verzonden en ontvangen, door persoonlijke bezorging of door tussenkomst van een postdienstverlener.
Elektronisch verkeer	Verkeer waarbij voor het verzenden en ontvangen van schriftelijke berichten gebruik wordt gemaakt van e-mail, internet, short message service (sms), fax of andere elektronische apparaten.

Definities conform artikel 3 van de eIDAS-verordening

Onderstaande definities zijn letterlijk overgenomen uit de Nederlandse versie van de eIDAS-verordening (artikel 3). Deze definities worden in deze handreiking exact gebruikt als in de verordening.

Definitie	Toelichting
Elektronische identificatie	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.
Persoonsidentificatiegegevens	Een reeks gegevens aan de hand waarvan de identiteit van een natuurlijke persoon of rechtspersoon, of een natuurlijke persoon die een rechtspersoon vertegenwoordigt, kan worden vastgesteld. In uitvoeringsbesluit 2015/1501 is een minimale reeks van persoonsidentificatiegegevens bepaald. Er is zowel een reeks voor natuurlijke personen als een reeks voor rechtspersonen. Al deze gegevens moeten in het aanvraagproces van een authenticatiemiddel worden gecontroleerd. De regels voor beoordeling van het betrouwbaarheidsniveau moeten steeds toegepast worden voor het geheel van deze reeks. Dit met dien verstande dat eIDAS dit enkel voor grensoverschrijdend gebruik verplicht. Voor betrouwbaarheidsniveau laag en niet grensoverschrijdende diensten kunnen hier dus concessies aan gedaan worden.
Vertrouwende partij	Een natuurlijke persoon of een rechtspersoon die vertrouwt op een elektronische identificatie of een vertrouwensdienst.
Ondertekenaar	Een natuurlijke persoon die een elektronische handtekening aanmaakt.
Elektronische handtekening	Gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen.
Geavanceerde elektronische handtekening	Een elektronische handtekening die voldoet aan de eisen in artikel 26 van eIDAS.
Gekwalificeerde elektronische handtekening	Een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen.
Gegevens voor het aanmaken van elektronische handtekeningen	Unieke gegevens die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken.
Certificaat voor elektronische handtekeningen	Een elektronische attestering die valideringsgegevens voor elektronische handtekeningen aan een natuurlijke persoon koppelt en ten minste de naam of het pseudoniem van die persoon bevestigt.
Gekwalificeerd certificaat voor elektronische handtekeningen	Een certificaat voor elektronische handtekeningen, dat is afgegeven door een gekwalificeerde verlener van vertrouwensdiensten en voldoet aan de eisen van bijlage 1.

Definitie	Toelichting
Vertrouwensdienst	Een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt: a) het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten of b) het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of c) het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben.
Gekwalificeerde vertrouwensdiens	Een vertrouwensdienst die voldoet aan de toepasselijke eisen, zoals vastgelegd in de eIDAS-verordening.
Verlener van vertrouwensdiensten	Een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent als een gekwalificeerde of als een niet-gekwalificeerde verlener van vertrouwensdiensten.
Gekwalificeerde verlener van vertrouwensdiensten	Een verlener van vertrouwensdiensten die een of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen.
Product	Software of hardware, of relevante componenten van hardware of software, die bedoeld zijn om te worden gebruikt voor de verlening van vertrouwensdiensten.
Middel voor het aanmaken van elektronische handtekeningen	Geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening aan te maken.
Elektronisch document	Elke inhoud die is opgeslagen in elektronische vorm, in het bijzonder tekst of geluid, beeld of audiovisuele opname.
Dienst voor elektronisch aangetekende bezorgin	Een dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden te verzenden en die bewijs verschaft ten aanzien van het hanteren van de verzonden gegevens, met inbegrip van bewijs van het verzenden en ontvangen van de gegevens, en die de verzonden gegevens beschermt tegen het risico van verlies, diefstal, beschadiging of onbevoegde wijzigingen.
Certificaat voor websiteauthenticatie	Attestering die het mogelijk maakt de authenticiteit van een website vast te stellen en die de website verbindt aan de natuurlijke persoon of rechtspersoon aan wie het certificaat is afgegeven.
Valideringsgegevens	Gegevens die worden gebruikt om een elektronische handtekening of elektronisch zegel te valideren.
Validering	Proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of een elektronisch zegel geldig is.


Carrier
1:27 PM
100%
Access
Place your finger
Emergency
Cancel

Deze brochure is een uitgave van:

Forum Standaardisatie
November 2016 | 96760