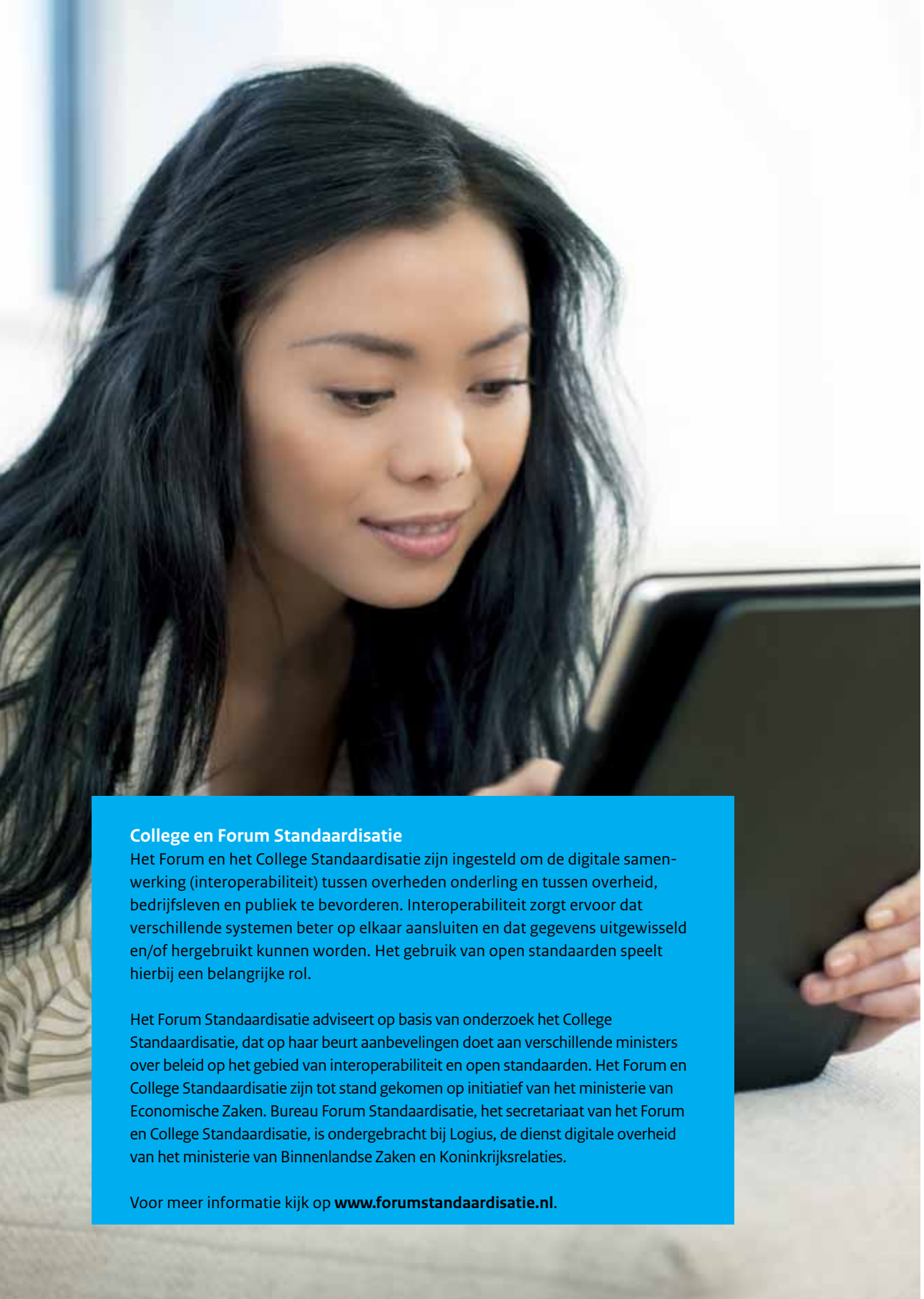
Een handreiking voor overheidsorganisaties

Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 2)

Forum Standaardisatie



College en Forum Standaardisatie
Het Forum en het College Standaardisatie zijn 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 College Standaardisatie, dat op haar beurt aanbevelingen doet aan verschillende ministers over beleid op het gebied van interoperabiliteit en open standaarden. Het Forum en College Standaardisatie zijn tot stand gekomen op initiatief van het ministerie van Economische Zaken. Bureau Forum Standaardisatie, het secretariaat van het Forum en College 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**.

Managementsamenvatting

Wat is de handreiking betrouwbaarheidsniveaus?

Met het oog op het realiseren van lastenverlichting, betere dienstverlening en een efficiëntere overheid zet de overheid in op grootschalige elektronische dienstverlening aan burgers en bedrijven. Daarbij moet de overheid er in meer of mindere mate, afhankelijk van de aard van de dienstverlening, op kunnen vertrouwen dat degene met wie zij zaken doet, ook werkelijk de persoon is voor wie hij zich uitgeeft. Dat stelt eisen aan elektronische identificatie en authenticatie.

In Nederland geldt tot nu toe een open norm ten aanzien van het gewenste betrouwbaarheidsniveau voor identificatie en authenticatie van personen en partijen bij e-overheidsdiensten. Deze open norm is neergelegd in de Algemene wet bestuursrecht (Awb) en in de regels over informatiebeveiliging. Een open norm wil zeggen dat de eisen niet concreet gedefinieerd zijn. Met de toename van e-diensten groeit de behoefte om deze open norm nader in te vullen, omdat het belangrijk is dat overheidsorganisaties in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid eisen (en borgen).

Deze handreiking geeft invulling aan die behoefte door een vereenvoudigde risicoanalyse te geven van de kwetsbaarheid van uw e-diensten. Die analyse helpt u te bepalen hoe gevoelig deze zijn voor misbruik en oneigenlijk gebruik. Op basis van zo'n risicoinschatting kunt u vervolgens het gewenste betrouwbaarheidsniveau kiezen voor uw e-diensten (en daarmee van de authenticatiemiddel(en) die uw klanten gebruiken). Speciale aandacht is er daarbij voor machtigingssituaties en de gevolgen van eenmalig inloggen.

Hoe werkt het?

De processen achter e-overheidsdiensten in Nederland zijn vaak gelijksoortig van aard en opbouw. Bovendien volgen ze de regels van de Algemene wet bestuursrecht, eventueel aangevuld met vereisten uit domeinwetgeving. Daardoor is het mogelijk 'families van diensten' te definiëren en daarop een generieke systematiek toe te passen om risico's in te schatten en te ondervangen.

De systematiek van deze handreiking gaat uit van een inschatting van de te beschermen waarde, aan de hand van een aantal objectieve (of objectiveerbare) criteria en belangen. Voorbeelden hiervan zijn wettelijke eisen, de aard van de gegevens die uitgewisseld worden (zijn bijvoorbeeld persoonsgegevens betrokken) en het economisch of maatschappelijk belang dat met een dienst of proces gemoeid is. Daarmee is vervolgens een inschatting te maken van de schade als de dienst onrechtmatig wordt afgenomen. Op basis van die vereenvoudigde risicoanalyse wordt de dienst tot slot ingeschaald op een bepaald betrouwbaarheidsniveau.

Voor wie is het bedoeld?

Deze handreiking is geschreven voor overheidsorganisaties die e-diensten leveren aan burgers en bedrijven. Daarbij kan het gaan om een webportaal met e-diensten voor burgers en/of bedrijven, maar ook om retourstromen of applicatie-applicatieverkeer.

De handreiking biedt een basis voor het gesprek tussen beleidsmakers, (proces)architecten en informatiebeveiligers over het gewenste betrouwbaarheidsniveau bij het inrichten van e-diensten en achterliggende back office processen. Ook biedt deze handreiking bestuurders inzicht in de afwegingen die aan het bepalen van het betrouwbaarheidsniveau ten grondslag liggen, zodat zij een weloverwogen keuze kunnen maken.

Waarvoor is het bedoeld?

De keuze voor een betrouwbaarheidsniveau voor een bepaalde elektronische dienst, en dus ook de keuze voor toepassing van deze handreiking, is en blijft de eigen verantwoordelijkheid van de overheidsorganisatie. Deze handreiking geeft de overheidsorganisatie 'gereedschap' om deze verantwoordelijkheid, uitgaande van de algemene wettelijke kaders, op een goede en eenduidige manier in te vullen. De handreiking wil daarmee bijdragen aan de transparantie, toegankelijkheid en geloofwaardigheid van de overheid en de rechtszekerheid van burgers en bedrijven.

Versie 2

Nieuw in deze versie 2 van de handreiking zijn de hoofdstukken 2, Afbakening en context, 5. Machtigingen, 6. Applicatie-applicatieverkeer, 7. Retourstromen en 8, Eénmalig inloggen. Nog in voorbereiding is een hoofdstuk over de Digitale handtekening. Dat hoofdstuk zal eind 2013 beschikbaar zijn.

Inhoudsopgave

Managementsamenvatting **3**
1 Inleiding 7
1.1 Uniforme betrouwbaarheidsniveaus als randvoorwaarde 7
1.2 Handreiking biedt houvast 7
1.3 Vereenvoudigde risicoanalyse met classificatiemodel 8
1.4 Ontwikkeling en beheer van de handreiking. 9
1.5 Leeswijzer 10
1.6 Meer informatie 10

2 Afbakening en context **12**
2.1 Afbakening 12
2.1.1 Typen diensten 12
2.1.2 Betrouwbaarheidsniveau per individuele dienst 14
2.2 Context 14
2.2.1 Ontwikkeling richting uitbesteding en externe vertrouwensdiensten 14
2.2.2 Vertrouwen op verklaringen 15

3 Uitgangspunten **18**
3.1 Vereenvoudigde risicoanalyse 18
3.2 Families van diensten 19
3.3 Stork-raamwerk als basis 20
3.4 De stork-betrouwbaarheidsniveaus 20

4 Inschaling van diensten **24**
4.1 Criteria 24
4.2 Het classificatiemodel 31
4.3 Referentiescenario 31
4.4 Correctiefactoren 32
4.5 Voorbeelden van diensten en de bijbehorende betrouwbaarheidsniveaus 33

5 Machtigingen **36**
5.1 Waar gaat het eigenlijk over? 36
5.2 Het perspectief van de individuele dienst 36
5.3 Wat betekent dit voor toepassing van het classificatiemodel? 37
5.4 Overige aandachtspunten 37

6 Applicatie-applicatieverkeer **38**
6.1 Waar gaat het eigenlijk over? 38
6.2 Het perspectief van de individuele dienst 39
6.3 Wat betekent dit voor toepassing van het classificatiemodel? 39
6.4 Overige aandachtspunten 40
Lessen uit het diginotar incident 40

7 Retourstromen 41
7.1 Waarover praten we eigenlijk? 41
7.2 Het perspectief van de individuele dienst 41
7.3 Wat betekent dit voor toepassing van het classificatiemodel? 43
7.4 Overige aandachtspunten 44

8 Eénmalig inloggen 47
8.1 Waar gaat het eigenlijk over? 47
8.2 Het perspectief van de individuele dienst 48
8.3 Wat betekent dit voor toepassing van het classificatiemodel? 48
8.4 Overige aandachtspunten 48
8.4.1 Deel uitmaken van een federatie 48
8.4.2 Gebruikersperspectief 49

Bijlagen
1 Relevante wet- en regelgeving 51

2 Voorbeelden van invulling van de wettelijke kaders en vertaling van papieren naar elektronische situatie 67

3 Begrippenkader 73

1 Inleiding

1.1 Uniforme betrouwbaarheidsniveaus als randvoorwaarde

De overheid zet grootschaling in op elektronische dienstverlening aan burgers en bedrijven. Het regeerakkoord benoemt als doelstelling dat alle diensten van de overheid in 2017 elektronisch beschikbaar moeten zijn. Het kabinet wil daarmee administratieve lastenverlichting, een betere dienstverlening en een efficiëntere overheid realiseren.

De Algemene wet bestuursrecht (Awb) vereist dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' geschiedt. Het Besluit voorschrift informatiebeveiliging rijksdienst (VIR) stelt daarnaast dat het betreffende lijnmanagement de betrouwbaarheidseisen voor elektronische diensten dient vast te stellen aan de hand van een risicoafweging. Vervolgens moeten zij erop toezien dat er passende maatregelen worden getroffen om aan die betrouwbaarheidseisen te voldoen. Daarmee zijn de Awb en het Besluit VIR open normen, in die zin dat de eisen niet concreet gedefinieerd zijn.

Met de groei in het gebruik van e-diensten groeit ook de behoefte om de hiervoor bedoelde open normen nader in te vullen. Het is belangrijk dat overheidsorganisaties in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid vereisen (en borgen) voor hun elektronische diensten. Dat draagt bij aan de transparantie, toegankelijkheid en geloofwaardigheid van de overheid. Bovendien is het met het oog op het zorgvuldigheidsbeginsel van belang dat de afwegingen die worden gemaakt bij het bepalen van een betrouwbaarheidsniveau helder en transparant zijn. Dat dient de rechtszekerheid van burgers en bedrijven. Deze handreiking geeft die invulling, op basis van de nationale geldende (wettelijke) regels en in aansluiting op het Europese STORK[1]-kader voor grensoverschrijdend gebruik van e-diensten.

1.2 Handreiking biedt houvast

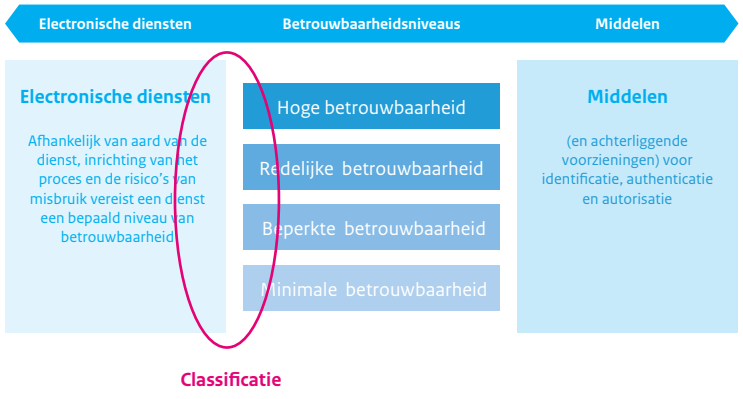
Er is sprake van een grote diversiteit aan elektronische overheidsdiensten. Gezien die diversiteit is het niet mogelijk voor identificatie, authenticatie en autorisatie een uniforme oplossing vast te stellen. Immers, een standaard oplossing met een zeer hoog betrouwbaarheidsniveau zou in veel gevallen te duur zijn en daarmee het gebruik van e-diensten onnodig beperken. Een oplossing met een laag betrouwbaarheidsniveau kan aanzienlijke risico's met zich mee brengen voor wat betreft fraude en de bescherming van de persoonlijke levenssfeer. Daarmee lijkt het onontkoombaar dat een burger verschillende oplossingen gebruikt voor verschillende diensten.

[1] Secure idenTities acrOss boRders linKed. Zie document D2.3 - Quality authenticator scheme, paragraaf 2.3 en 2.4, te vinden op www.eid-stork.eu, onder STORK materials, deliverables approved/public.

Om te voorkomen dat gebruikers door deze verschillende oplossingen te maken krijgen met een grote, onhandige, digitale 'sleutelbos', wordt binnen de overheid gewerkt aan generiek inzetbare oplossingen. Voorbeelden daarvan zijn DigiD, PKIoverheid en het afsprakenstelsel eHerkenning. Dit zorgt er tevens voor dat de kosten beheersbaar blijven.

1.3 Vereenvoudigde risicoanalyse met classificatiemodel

De vraag blijft echter welk middel in welke situatie dient te worden toegepast. Voor uitvoerders van publieke diensten blijkt dat in de praktijk lastig te beoordelen. Tegen die achtergrond is deze handreiking opgesteld. Hij is bedoeld om een bijdrage te leveren aan een eenduidige, efficiënte en bewuste bepaling van het betrouwbaarheidsniveau van elektronische overheidsdiensten. Hij bevat daartoe een 'classificatiemodel' dat in feite een vereenvoudigde risicoanalyse is. Het classificatiemodel maakt op basis van verschillende (wettelijke) criteria een generieke koppeling mogelijk tussen (soorten) diensten en betrouwbaarheidsniveaus. Ook geeft de handreiking indicaties die tot inschaling op een hoger of lager betrouwbaarheidsniveau zouden kunnen leiden. De handreiking bevat geen vertaling van de betrouwbaarheidsniveaus naar specifieke authenticatiemiddelen.



Figuur 1: Toepassingsgebied van de handreiking

Aan de hand van het classificatiemodel kunnen architecten, informatiebeveiligers, juristen en bestuurders een beredeneerde keuze maken voor het benodigde betrouwbaarheidsniveau voor de e-diensten die hun organisatie aanbiedt. Zij moeten zich daarbij realiseren dat deze handreiking gebaseerd is op een generieke benadering. Hij zal daarom in het merendeel van de gevallen een adequate bepaling geven van een betrouwbaarheidsniveau, maar uitzonderingen zijn mogelijk. Als in een bepaalde situatie op basis van het classificatiemodel geen keuze gemaakt kan worden, bijvoorbeeld omdat de aard van de dienst of de omstandigheden wezenlijk afwijken van wat in het classificatiemodel is opgenomen, ligt het voor de hand om een volwaardige risicoanalyse uit te voeren ter bepaling van het gewenste betrouwbaarheidsniveau voor die dienst.

Het is verder wenselijk dat de dienstaanbieder de inschaling van het betrouwbaarheidsniveau voor zijn diensten bekendmaakt in een regeling (beleidsregels of algemeen verbindende voorschriften, afhankelijk van de context). In de toelichting daarbij kan de inschaling worden onderbouwd, zodat deze ook voor gebruikers van de dienst helder is.

1.4 Ontwikkeling en beheer van de handreiking.

Deze handreiking is tot stand gekomen in samenwerking tussen verschillende overheidsorganisaties en enkele bedrijven[2], gefaciliteerd door Bureau 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. In vervolg daarop is deze breed verspreid onder overheidsorganisaties, met een advies over de wijze waarop zij deze kunnen verankeren in hun uitvoeringsbeleid rond elektronische dienstverlening.

De handreiking is geen statisch product. Het was bij de publicatie van de eerste versie duidelijk dat de verdere ontwikkeling van e-dienstverlening en van identificatie- en authenticatiemiddelen, maar ook de ervaringen met toepassing van de handreiking door overheidsorganisaties, aanleiding zullen geven tot aanpassing en aanvulling. Logius en Forum Standaardisatie gaven daarom aan het beheer en de doorontwikkeling te zullen blijven ondersteunen. Dit sluit aan bij de beheerverantwoordelijkheid die Logius heeft voor verschillende identificatie- en authenticatiemiddelen en -standaarden, zoals DigiD (Machtigen), PKIoverheid en eHerkenning.

De partijen die betrokken zijn geweest bij de eerste versie van de handreiking vormen de basis voor een 'community' van gebruikers die Bureau Forum

[2] Agentschap.nl, Dienst Regelingen, DUO, IND, KvK, Logius, Nictiz, SVB, RDW, UWV, de gemeenten Amsterdam, Den Haag, Enschede, Stadskanaal, Tilburg, Utrecht, Zoetermeer, KING en VNG, de provincies Flevoland en Noord Brabant, de ministeries BZK, EZ, Fin, I&M, LNV, SZW en V&J en de private organisatie Cap Gemini, PKIpartners en Post.nl.

Standaardisatie ondersteunt bij het onderhouden en verder ontwikkelen van de handreiking. Deze tweede versie van de handreiking is de eerste inhoudelijke uitbreiding van de handreiking waarbij deze 'community' als zodanig heeft gefunctioneerd.

1.5 Leeswijzer

Hoofdstuk 2 beschrijft de afbakening en context voor deze handreiking. Waar gaat deze wel en waar gaat deze niet over? Hoofdstuk 3 bevat de uitgangspunten voor de uitwerking van het classificatiemodel. In hoofdstuk 4 wordt de gehanteerde methodiek nader toegelicht en is het daadwerkelijke classificatiemodel opgenomen voor het inschalen van diensten op het vereiste betrouwbaarheidsniveau. Deze drie hoofdstukken vormen de kern van de handreiking.

In de hoofdstukken 5 t/m 8 komen specifieke vormen van communicatie of dienstverlening aan de orde. Achtereenvolgens betreffen dit: machtigingen, applicatie-applicatieverkeer, retourstromen en éénmalig inloggen.

Bijlage 1 beschrijft het wettelijke kader waarin de verschillende criteria voor inschaling van diensten op het vereiste betrouwbaarheidsniveau hun grondslag vinden. In bijlage 2 staan illustraties van de manier waarop wettelijke vereisten en formuleringen zich vertalen naar de elektronische praktijk. In bijlage 3 is een lijst met veel gebruikte begrippen opgenomen.

1.6 Meer informatie

De handreiking is digitaal beschikbaar op de sites van Logius en Forum Standaardisatie (www.logius.nl, www.forumstandaardisatie.nl) en van het programma eHerkenning (www.eherkenning.nl). Vragen over de toepassing van deze handreiking kunnen worden gericht aan Forumstandaardisatie@logius.nl.

2 Afbakening en context

De betrouwbaarheid van de elektronische dienstverlening van de overheid is een groot en complex domein. Het is onmogelijk om dat in zijn geheel binnen één handreiking te behandelen. Daarom maken we in dit hoofdstuk nog eens duidelijk waarop deze handreiking betrekking heeft. Er speelt echter buiten die 'afbakening' een aantal ontwikkelingen die zo direct raken aan het proces van het toekennen van betrouwbaarheidsniveaus aan diensten, dat we die in dit hoofdstuk ook kort willen beschrijven.

2.1 Afbakening

2.1.1 Typen diensten

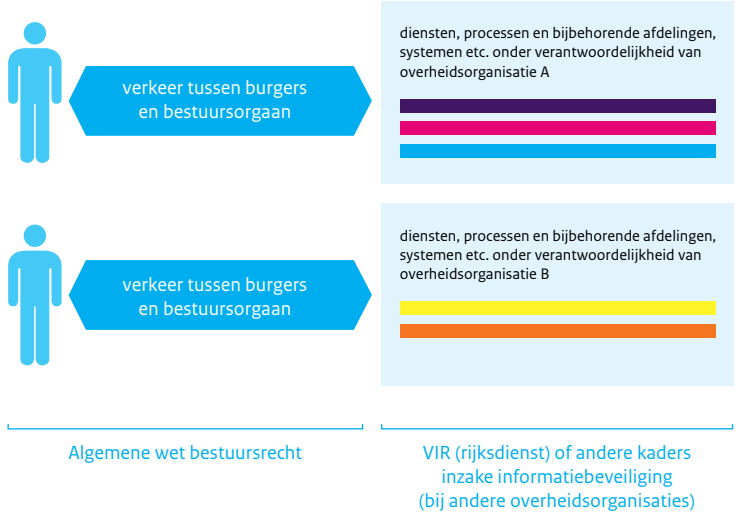
Deze handreiking betreft diensten en processen die de overheid verleent aan of inzet jegens burgers en bedrijven. Het gaat daarbij om het domein dat op hoofdlijnen wordt gereguleerd door afdeling 2.3 van de Algemene wet bestuursrecht (Awb).[3] Daarbij onderscheiden we grofweg de volgende typen diensten:

1. Diensten waarbij iemand voor zichzelf via internet een dienst afneemt en ook zelf de benodigde handelingen uitvoert (website bezoeken, e-mail verzenden, etc.). De afnemers van de dienst kunnen zowel burgers zijn als bedrijven.
2. Diensten die afgenomen worden door iemand die zelf de benodigde handelingen uitvoert, maar dat doet namens een andere natuurlijke of niet-natuurlijke persoon (machtiging).
3. Diensten waarbij geautomatiseerde systemen met elkaar communiceren zonder directe menselijke tussenkomst (applicatie-applicatieverkeer).

Waar de eerste versie van de handreiking zich uitsluitend richtte op situatie 1, beschrijft deze nieuwe versie ook situaties 2 en 3. Ook de zogenaamde retourstromen van dienstaanbieder naar burger of bedrijf zijn meegenomen in deze handreiking.

Met 'retourstromen' wordt allereerst de reactie bedoeld van de overheid op een aanvraag, aangifte of iets dergelijks. Maar ook wanneer de eerste stap in de interactie van de overheid afkomstig is, zoals bij officiële mededelingen of uitnodigingen tot het doen van een aangifte, wordt dit gezien als retourstroom. Ook bij retourstromen spelen identificatie, authenticatie en autorisatie een belangrijke rol. Het moet duidelijk zijn dat de organisatie/medewerker 'achter het loket' bevoegd is om bepaalde beslissingen te nemen en daartoe over informatie kan beschikken. Ook de vertrouwelijkheid moet in dat geval geborgd zijn. Hetzelfde geldt bij uitwisseling van gegevens tussen overheidsorganisaties onderling (bijvoorbeeld het raadplegen van basisregistraties, het uitwisselen van informatie die nodig is voor beoordeling van een vergunningaanvraag).

Dit domein van de 'retourstromen' wordt, in elk geval voor de ministeries en daaronder direct ressorterende onderdelen, bestreken door het Besluit voorschrift informatiebeveiliging rijksdienst (VIR). Decentrale overheden hanteren op vrijwillige basis nu vaak al een soortgelijke systematiek, waarmee zijn in de geest van het VIR handelen. Daarnaast zijn zij – net als onderdelen van de rijksoverheid – gebonden aan de informatiebeveiligingsregels ingevolge de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA) en (de invulling van) artikel 13 Wet bescherming persoonsgegevens (Wbp). De administratieve organisatie en interne controle (AO/IC) en het beveiligingsbeleid van de overheidsorganisatie moeten op basis van al deze regels voorzien in de nodige waarborgen voor de betrouwbaarheid en vertrouwelijkheid van de gegevensstromen.



Figuur 2: Relatie tussen Awb en regels inzake informatiebeveiliging

Tot slot komt het onderwerp 'eenmalig inloggen' oftewel 'Single Sign On (SSO)' aan de orde en de specifieke aandachtspunten daaromtrent voor overheidsdienstaanbieders. Nog in voorbereiding is een hoofdstuk over de digitale handtekening. Dat hoofdstuk zal eind 2013 beschikbaar komen.

[3] De artikelen 2:13-2:17, ingevoegd bij de Wet elektronisch bestuurlijk verkeer (Stb. 2004, 214).

2.1.2 Betrouwbaarheidsniveau per individuele dienst

De handreiking spitst zich toe op het vaststellen van het vereiste betrouwbaarheidsniveau voor één bepaalde dienst. Het kan voorkomen dat een dienstverlener meer diensten aanbiedt, die verschillende betrouwbaarheidsniveaus vereisen. De handreiking geeft niet specifiek aan hoe in dit soort situaties te handelen, maar beschrijft wel risicoverhogende en -verlagende aspecten rond de dienstverlening. Dat biedt aanknopingspunten om, binnen grenzen, het aantal betrouwbaarheidsniveaus dat een organisatie hanteert te beperken.

2.2 Context

2.2.1 Ontwikkeling richting uitbesteding en externe vertrouwensdiensten

Deze handreiking is geschreven met het oog op een dienstaanbieder die een individuele dienst aanbiedt en die ook zelf inricht en beheert. Met het oog op het verminderen van de beheerlast, kosten én risico's, is de trend dat steeds meer overheidsdienstverleners hun vertrouwensdiensten geheel of gedeeltelijk uitbesteden.

In het geval van gedeeltelijke uitbesteding belegt de dienstaanbieder de inrichting en/of het beheer van de vertrouwensdiensten bij een externe partij, maar stelt daaraan duidelijke eisen. Het moet ook goed mogelijk zijn om controle te houden over de dienstverlening.

De tweede zichtbare trend is dat dienstaanbieders steeds meer gebruik maken van bestaande authenticatiemiddelen en vertrouwensdiensten uit de markt. Een concreet voorbeeld daarvan is het gebruik van *social login*. Daarbij kunnen mensen zich met hun Facebook-identiteit bekendmaken en inloggen bij andere dienstverleners, zoals webshops. Voor de overheid, die administratieve lastenverlichting voor burgers en bedrijven beoogt, is dit ook een relevante ontwikkeling. Het gebruik van bestaande middelen of platforms, verkleint namelijk de 'digitale sleutelbos' van de gebruiker. Bij deze vorm van volledige uitbesteding heeft de dienstaanbieder vaak geen of zeer beperkte mogelijkheden om de precieze eigenschappen van de authenticatie, machtigingen en ondertekeningen te bepalen. Er vindt onder de authenticatiemiddelen in de markt momenteel een soort 'shake-out' plaats.

Zowel bij gedeeltelijke als bij volledige uitbesteding is het voor een dienstaanbieder belangrijk om te beseffen dat hij altijd verantwoordelijk blijft voor de betrouwbaarheid van zijn eigen dienst. Dat betekent dus dat hij nog steeds zelf het betrouwbaarheidsniveau van zijn dienst moet vaststellen, maar daarnaast ook strenge eisen moet (kunnen) stellen aan de externe leveranciers en hun authenticatieoplossingen in termen van betrouwbaarheid en kwaliteit. Ook de verantwoording en het toezicht moeten daarbij goed geregeld zijn. Hierbij is er geen fundamenteel onderscheid of uitbesteding plaatsvindt aan de markt of dat de organisatie gebruik maakt van gemeenschappelijke voorzieningen van de elektronische overheid, zoals DigiD. De manier waarop kwaliteit en betrouwbaarheid geborgd kunnen worden in situaties van uitbesteding, valt buiten de scope van deze handreiking.

2.2.2 Vertrouwen op verklaringen

Vertrouwensdiensten maken het mogelijk dat een dienstverlener er op kan vertrouwen dat een gebruiker van zijn dienst ís wie hij zegt dat hij is. Bij veel diensten is de vaststelling van de identiteit van de gebruiker echter niet voldoende. We moeten ook weten of hij de bevoegdheid heeft, of gemachtigd is, om de handelingen uit te voeren, die hij binnen de dienst wil uitvoeren. En als hij inderdaad die bevoegdheid of machtiging heeft, hoe lang die bijvoorbeeld geldig is.

Voorbeeld

Bij bureau Jansen & Jansen werken vier advocaten. Zij worden bijgestaan door mevrouw Pietersen. Deze Office Manager regelt veel praktische zaken. Ze beheert de agenda's van de advocaten en bij rechtszaken verzorgt ze de logistiek rond de aanlevering van de stukken. De advocaten hebben een advocatenpas en mevrouw Pietersen heeft een zogenaamde gemachtigdenpas van de Nederlandse Orde van Advocaten (NOvA), waarmee zij namens de advocaten in de systemen van de rechtbank kan komen.

Voor een bepaalde zaak wil advocaat Jansen enkele stukken toevoegen aan het dossier. Hij heeft deze stukken digitaal ondertekend in een speciale clouddienst die hem identificeert op basis van zijn A-nummer uit het NovA-register en een 'associatieverklaring' afgeeft, die waarborgt dat Jansen het stuk heeft ondertekend. Mevrouw Pietersen stuurt de digitaal ondertekende stukken elektronisch in via het portaal van de rechtbank, waarmee ze daadwerkelijk aan het dossier worden toegevoegd. Hierbij wordt zij geauthenticeerd aan de hand van haar NovA-gemachtigdenpas. De systemen van de rechtbank ontvangen de Identiteit van mevrouw Pietersen in een identiteitsverklaring en de bevestiging dat zij door Jansen gemachtigd is voor de betreffende diensten bij de rechtbank in een bevoegdheidsverklaring.

De vaststelling van de identiteit en bevoegdheden van gebruikers is binnen elektronische dienstverlening gebaseerd op ‘Verklaringen’. Soms zullen die verklaringen door de dienstverlener zelf worden opgesteld, maar naarmate dienstverleners vertrouwensdiensten extern betrekken, komen die verklaringen in toenemende mate ook van ‘buiten’, soms zelfs zodanig dat bij gebruik van één dienst verklaringen van verschillende externe partijen beschikbaar komen.

Afhankelijk van de complexiteit van de dienst en de mate van uitbesteding, kan een dienstaanbieder dus te maken krijgen met verschillende soorten Verklaringen. Hierbij is het belangrijk dat de dienstaanbieder erop kan vertrouwen dat de verklaringen – en de processen waaruit ze voortkomen – betrouwbaar zijn. Eenvoudig gesteld: wordt de dienstverlening ingeschaald op betrouwbaarheidsniveau 3, dan moeten de verklaringen tenminste hetzelfde betrouwbaarheidsniveau hebben. Hoewel dit een essentieel punt is (de betrouwbaarheid van een dienst wordt immers bepaald door de zwakste schakel) en er onder meer in het hoofdstuk over ‘machtigingen’ nog iets dieper op wordt ingegaan, zijn de criteria die maken dat een verklaring een bepaald betrouwbaarheidsniveau heeft, onderdeel van standaarden zoals STORK die de ‘aanbodszijde’ regelen. Daarmee vallen ze buiten deze handreiking die de ‘vraagzijde’ regelt en derhalve de vraag beantwoord welk betrouwbaarheidsniveau een bepaalde dienst nodig heeft.

3 Uitgangspunten

In dit hoofdstuk worden de uitgangspunten beschreven die bij de uitwerking van de handreiking gevolgd zijn. Deze betreffen:
- Kiezen voor een vereenvoudigde, makkelijk hanteerbare risicoanalyse;
- Definiëren van families van diensten;
- Hanteren van het STORK-raamwerk als basis voor interoperabiliteit.

Het resultaat van deze benadering is een systematiek die een globale inschatting geeft van de risico's van een specifieke e-dienst en die betrekkelijk eenvoudig uitvoerbaar is. Daarmee kunnen overheidsorganisaties snel het vereiste betrouwbaarheidsniveau voor hun elektronische diensten bepalen, tenzij een gedetailleerde risicoanalyse aangewezen is of verplicht is op basis van voorschriften voor informatiebeveiliging.

3.1 Vereenvoudigde risicoanalyse

In verschillende landen gebeurt het inschalen van betrouwbaarheidsniveaus op basis van risico-analyses.[4] Ook de VS hebben deze benadering gekozen. De Office of Management and Budget heeft hiervoor in 2006 de E-Authentication Guidance for Federal Agencies[5] vastgesteld. Ieder orgaan van de federale overheid dient volgens deze richtlijn voor elk afzonderlijk proces of elke dienst, op basis van inschatting van de risico's aan de hand van een groot aantal variabelen, het benodigde betrouwbaarheidsniveau te bepalen. De verwachting is dat op den duur, op basis van de gedocumenteerde risicoanalyses, bepaalde vaste lijnen te onderkennen zijn. Deze gedetailleerde risicoanalyse voor het bepalen van betrouwbaarheidsniveaus wordt ingegeven door de aansprakelijkheidsaspecten die in de Angelsaksische cultuur een dominante rol spelen.

In Nederland schiet een dergelijke benadering zijn doel voorbij. Het is kostbaar, tijdrovend en kan tot versnippering en ongerechtvaardigde verschillen leiden, terwijl processen en diensten vaak veel gemeenschappelijke kenmerken vertonen (onder andere door de toepasselijkheid van de Awb op beslisprocessen). Daarom is voor deze handreiking gezocht naar een systematiek om risico's generiek in te schatten en te ondervangen. Die systematiek gaat uit van een inschatting van de te beschermen waarde, aan de hand van een aantal objectieve (of objectiveerbare) criteria en belangen. Daarbij kan men denken aan wettelijke eisen, de aard van de gegevens die uitgewisseld worden (zijn persoonsgegevens betrokken?) en het economisch of maatschappelijk belang dat met een dienst of proces gemoeid is.

[4] Zie bv. in Spanje: MAGERIT, Methodology for Information System Risk Analysis and Management.
[5] Ministerio de Administraciones Públicas, June 2006, http://www.epractice.eu/document/3215. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

Daarmee kan vervolgens een inschatting gemaakt worden van de mogelijke schade in geval de authenticatie voor de dienst niet op de juiste wijze zou plaatsvinden. De aanname bij deze methode is dat de desbetreffende diensten vanuit vergelijkbare online omgevingen worden geleverd en vergelijkbare kwetsbaarheden hebben. Wel is in de gebruikte systematiek rekening gehouden 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. Daarbij kan worden gedacht aan maatregelen als terugkoppeling via een ander kanaal, bijvoorbeeld een brief naar het woonadres zoals opgenomen in de gemeentelijke basisadministratie persoonsgegevens (GBA).

3.2 Families van diensten

Zoals hiervoor is opgemerkt, zijn de processen die achter e-overheidsdiensten zitten vaak gelijksoortig van aard en opbouw. Ze volgen in het algemeen een standaard beslisproces dat voortvloeit uit de regels van de Awb, eventueel aangevuld met vereisten uit domeinwetgeving. De relatieve eenvormigheid maakt dat families van diensten te definiëren zijn, ook al varieert de informatie die bij de afwikkeling van die dienst nodig is en varieert de (technische) inrichting van de dienst (online portaal, applicatie).

We onderscheiden de volgende families van diensten:
- Algemene informatie opvragen;
- Aanmelden voor/reageren op discussiefora;
- Aanmelden voor nieuwsbrieven e.d.;
- Verzoek tot feitelijk handelen (afvalcontainer, grofvuil ophalen);
- Registreren voor gepersonaliseerde webpagina (een Mijn-domein);
- Klacht indienen;
- Aanvraag indienen (ten behoeve van een beschikking);
- Persoonsgebonden informatie opvragen/raadplegen (vgl. vooringevulde aangifte);
- Informatie verstrekken/muteren;
- Verantwoording afleggen;
- Bezwaarschrift indienen;
- Beroepschrift indienen.

Deze families van diensten, maken het mogelijk om een meer algemene uitspraak te doen over de mate van betrouwbaarheid die voor iedere familie vereist is. Die mate van betrouwbaarheid wordt bepaald door de algemene en specifieke karakteristieken van de dienst. Algemene karakteristieken zijn bijvoorbeeld de aard van de gegevens (persoonsgegevens vergen meer

zekerheid dan niet-persoonsgegevens). Specifieke karakteristieken zijn ingegeven door wettelijke vereisten voor de dienst (bijvoorbeeld een vereiste van ondertekening). Dit is een belangrijk uitgangspunt geweest voor de classificatie van diensten en betrouwbaarheidsniveaus in deze handreiking.

3.3 STORK-raamwerk als basis

Wanneer voor een bepaalde e-overheidsdienst het betrouwbaarheidsniveau is vastgesteld, is het concreet inrichten van de dienst de volgende stap. Daarbij moeten onder meer keuzes worden gemakkt ten aanzien van de toe te passen authenticatieprocedure en het authenticatiemiddel. Het aanbod van authenticatiemiddelen is uitgebreid en zeer divers. Er zijn grote verschillen in gebruiksvriendelijkheid, prijs en betrouwbaarheidsniveau. Daarbij hebben we niet alleen met de Nederlandse markt te maken. Er is steeds vaker sprake van grensoverschrijdende dienstverlening, waarbij ook met buitenlandse authenticatiemiddelen toegang moet kunnen worden verkregen tot Nederlandse diensten.

Om de vraag te beantwoorden met welk middel uit het ene land een dienst in een ander land afgenomen kan worden, is het noodzakelijk identificatie- en authenticatiemiddelen te kunnen classificeren. In dat kader bestaan er inmiddels verschillende normatieve documenten, waarbij het STORK-raamwerk[6] voor de Nederlandse overheid het meest relevant is. Het STORK-raamwerk voor 'Quality Authentication Assurance Levels' (ofwel 'betrouwbaarheidsniveaus voor de kwaliteit van authenticatie')[7] is opgesteld met het oog op het bevorderen van interoperabiliteit van elektronische identificatie en authenticatie in Europa.

Het STORK-raamwerk is in deze handreiking gehanteerd als vertrekpunt voor de definitie van betrouwbaarheidsniveaus, zodat diensten en middelen makkelijk te koppelen zijn. Hierbij moet wel worden opgemerkt dat STORK zich beperkt tot de authenticatie van burger of bedrijf en dan nog met name in de context van webportalen. Voor andere zaken zoals machtigingen, applicatie-applicatieverkeer en elektronische machtigingen geldt dat er nauwelijks algemeen geaccepteerde standaarden voorhanden zijn die een indeling in betrouwbaarheidsniveaus bieden of mogelijk maken.

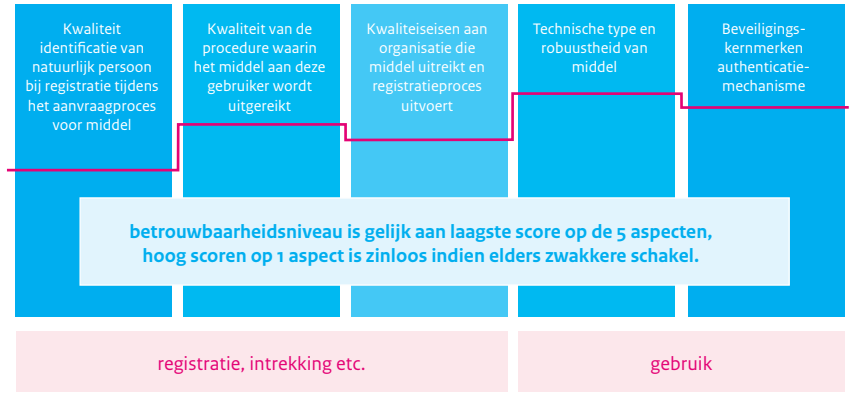
3.4 De STORK-betrouwbaarheidsniveaus

De eerste stap die het STORK-raamwerk hanteert om het betrouwbaarheidsniveau van een authenticatiemiddel vast te stellen is beoordeling van de volgende, losstaande, aspecten:

- De kwaliteit van de identificatie (of preciezer: identiteitsverificatie) van de persoon tijdens het aanvraagproces voor het middel;
- De kwaliteit van de procedure waarin het middel aan deze gebruiker wordt uitgereikt;
- De kwaliteit van de organisatie die het middel uitreikt en het bijbehorende registratieproces uitvoert;
- Het technische type en de robuustheid van het middel;
- De beveiligingskenmerken van het authenticatiemechanisme waarmee het authenticatiemiddel iedere keer dat het gebruikt wordt op afstand (via internet) herkend wordt.

De eerste drie aspecten zijn met name proceswaarborgen die gelden voor het registratieproces. De laatste twee zijn de meer technische beveiligingsaspecten van de wijze waarop het middel gebruikt wordt. Het uiteindelijke betrouwbaarheidsniveau van het authenticatiemiddel wordt bepaald door een combinatie van deze aspecten. Het STORK-raamwerk gaat uit van vier niveaus. Daarbij is het individuele aspect met het relatief laagste niveau (de zwakste schakel) bepalend voor het uiteindelijke niveau. In onderstaande figuur is dit verbeeld.

De vier niveaus die STORK definieert, zijn:



Figuur 3: Bepaling van het betrouwbaarheidsniveau volgens STORK

STORK QAA niveau 1

Dit niveau biedt het laagste niveau van zekerheid. Dat betekent: geen of minimale zekerheid ten aanzien van de geclaimde identiteit van de gebruiker. Bij het registratieproces ter verkrijging van het authenticatiemiddel worden identificerende kenmerken zonder nadere verificatie overgenomen. Een voorbeeld is een proces waarin de aanvrager van het middel een e-mail

[6] Zie www.eid-stork.eu.

[7] In de Nederlandse praktijk wordt ook wel gesproken van zekerheidsniveau. Dat begrip kan worden beschouwd als synoniem voor betrouwbaarheidsniveau.

ontvangt van de uitgever met daarin een hyperlink die de aanvrager slecht hoeft aan te klikken om het middel in gebruik te nemen. De enige zekerheid is dat het e-mail adres van de aanvrager bestaat op het moment van de aanvraag en dat een verder ongeïdentificeerde aanvrager in staat is te reageren op naar dat adres verzonden e-mailberichten. Een voorbeeld hiervan is het downloaden van een aanbestedingsdocument van de Aanbestedingskalender.nl.

STORK QAA niveau 2
Op dit niveau vindt bij het registratieproces ter verkrijging van het authenticatiemiddel verificatie plaats van de door de gebruiker geclaimde identiteit. Dit gebeurt door controle op basis van een door een Staat afgegeven document (bv. een kopie van een paspoort of rijbewijs) of registratie (bv. de GBA). Er is echter geen sprake van fysieke verschijning in het registratieproces, een middel met '1-factor authenticatie' volstaat. Onder een 'factor' wordt in dit kader verstaan een bewijsmiddel voor een geclaimde identiteit, bijvoorbeeld een username/password-combinatie, of een door een vertrouwde partij toegezonden unieke code. DigiD is een voorbeeld van een middel met 1-factor authenticatie.

STORK QAA niveau 3
Dit niveau vereist striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden. Middelenuitgevers moeten verder onder overheidstoezicht staan. Als type middel is '2-factor authenticatie' vereist. Voorbeelden daarvan zijn 'soft' certificaten of 'one-time-password'-tokens. De RDW gebruikt bijvoorbeeld 2-factor authenticatie bij communicatie met bedrijven uit de voertuigenbranche die in die hoedanigheid bepaalde RDW-gegevens mogen inzien. Ook de online bankapplicaties waarvoor de bankklanten een token nodig hebben zitten op dit niveau.

STORK QAA niveau 4
Dit niveau vereist tenminste eenmaal fysiek verschijnen van de gebruiker in het registratieproces en het voldoen aan alle eisen van de nationale wetgeving van het desbetreffende land aangaande uitgifte van gekwalificeerde certificaten als bedoeld in Annex II van Richtlijn 1999/93/EG betreffende elektronische handtekeningen. Voor Nederland betreft dat de eisen van artikel 1.1, onderdeel ss, van de Telecommunicatiewet. Tevens moet de middelenuitgever voldoen aan Annex I van diezelfde richtlijn. In Nederland is dat artikel geïmplementeerd in artikel 18:16, eerste lid, van de Telecommunicatiewet. Overheidspartijen of bijvoorbeeld notarissen die documenten elektronisch willen aanleveren bij het Kadaster, kunnen dat doen via de speciale applicatie 'Web-Elan'. Dit systeem vereist gebruik van een token, een gewaarmerkt certificaat èn een digitale handtekening. Gebruikers dienen zelf te zorgen dat zij over deze middelen beschikken.

4 Inschaling van diensten

Op grond van de uitgangspunten uit hoofdstuk 3 is een classificatiemodel geformuleerd voor de inschaling van e-overheidsdiensten op de verschillende betrouwbaarheidsniveaus. Dit classificatiemodel kan worden beschouwd als een eenvoudige risicoanalyse. Welk betrouwbaarheidsniveau voor een bepaalde dienst vereist is, kan worden ingeschat op basis van een aantal criteria. Deze criteria hebben te maken met de wettelijke eisen die gesteld zijn aan de dienst, de aard van de gegevens en de potentiële schade die ontstaat als ze in handen raken van onbevoegde derden of ongewenst worden gewijzigd.

In de gehanteerde systematiek, die gerelateerd is aan de gebruikelijke elementen van risicoanalyse, wordt de dreiging of de kans dat een dreiging zich manifesteert niet gekwantificeerd. In plaats daarvan worden aannames geformuleerd over de kwaliteit van de IT-beveiliging en relevante kenmerken van het achterliggende proces waarmee de betreffende dienst wordt geleverd. Deze aannames zijn verwerkt in een zogenaamd referentiescenario. Op basis van de criteria en het referentiescenario kan via een eenvoudige tabel (het 'classificatiemodel, zie pagina 31) een betrouwbaarheidsniveau worden vastgesteld.

Het classificatiemodel kent tot slot een aantal correctiefactoren. Dit zijn factoren die de dreiging reduceren óf verhogen ten opzichte van het referentiescenario. Met name in die laatste gevallen zal de vereenvoudigde risicoanalyse niet toereikend zijn en blijft een volledige risicoanalyse geboden.

4.1 Criteria

De volgende criteria zijn relevant bij het inschalen van betrouwbaarheidsniveaus:

1 Rechtsgevolg
Als de dienst zijn grondslag vindt in wetgeving zal deze leiden tot rechtshandelingen van de overheidsorganisatie (bv. een voor bezwaar en beroep vatbaar besluit nemen) en dus op rechtsgevolg gericht zijn. In gevallen waarin sprake is van feitelijk handelen (bv. het verstrekken van inlichtingen) is de dienst niet op rechtsgevolg gericht. Overigens kan het ook zijn dat een dienst aanvankelijk slechts feitelijk handelen betreft, maar in een vervolgtraject alsnog tot rechtsgevolg kan leiden. Een voorbeeld hiervan is het registreren van afvalcontainers op naam en adres, waarbij deze gegevens op een later moment ook de basis kunnen vormen voor handhaving (bv. toezien op het juist aanbieden van huisvuil). Voor de inschaling van het betrouwbaarheidsniveau is dit van belang.

Gehanteerde waarden:
- geen rechtsgevolg;
- wel rechtsgevolg.
- indirect rechtsgevolg.

2 Formeelrechtelijke vereisten
Veel diensten vereisen ondertekening, ofwel op grond van de Awb, ofwel op basis van specifieke wettelijke regels. Het kan gaan om ondertekening ten behoeve van authenticatie of ter bevestiging van wilsuiting. In specifieke gevallen kan zelfs expliciet een geavanceerde of gekwalificeerde elektronische handtekening worden vereist, afhankelijk van de vereiste bewijskracht.

Gehanteerde waarden:
- slechts algemene eisen betreffende betrouwbaarheid en vertrouwelijkheid zijn gesteld;
- ondertekening door of namens belanghebbende is vereist;
- ondertekening is vereist, tevens zijn nadere vormvereisten gesteld aan de ondertekening.

3 Opgeven van persoonsgegevens door de betrokkene
Verwerking van persoonsgegevens vraagt om passende beveiliging, zoals ook vereist is in art. 13 van de Wbp. Dit vraagt uiteraard een breed scala aan beveiligingsmaatregelen, waarvan authenticatie 'aan de poort' niet het enige, maar wel een zeer belangrijk beveiligingselement is omdat:
- het verhindert dat gevoelige persoonsgegevens terecht komen bij de verkeerde partijen of personen;
  en omdat
- opgave van (wijzigingen van) persoonsgegevens steeds stevig gekoppeld wordt aan de (betrouwbare) identiteit van de handelende persoon.

In deze handreiking zijn twee situaties uit elkaar gehaald. Enerzijds het door betrokkene zelf opgeven van persoonsgegevens (deze pragraaf) en anderzijds het geval dat dienstverleners reeds bekende persoonsgegevens communiceren (zie volgende paragraaf). De reden hiervoor is dat wanneer een betrokkene zelf de gegevens verstrekt, er geen sprake kan zijn van ongeoorloofde kennisname door derden. Bij verstrekking door de overheid, bijvoorbeeld door het tonen van de gegevens op een overheidswebsite, kan dit wel aan de orde zijn. Daarom worden de betrouwbaarheidsniveaus in deze twee situaties verschillend ingeschaald.

De criteria voor de inschaling van de gevoeligheid van de persoonsgegevens zijn primair de aard van de persoonsgegevens en secondair de aard van de verwerking [CBP Richtsnoeren voor Beveiliging Persoonsgegevens, 2013].

Waar de genoemde CBP richtsnoeren dus een heel open norm geven, gaat deze handreiking wel uit van een indeling in klassen, geïnspireerd door de eerdere CBP publicatie A&V 23.[8] Daarbij hanteren we voor de indeling in klassen echter uitsluitend het criterium 'aard van de gegevens'. Er is gekozen voor deze indeling in klassen omdat de open benadering van de richtsnoeren in de praktijk onvoldoende houvast blijkt te bieden.

De aard van de verwerking vindt niet zijn weerslag in de indeling in de hieronder vermelde klassen. Onder verwerking van persoonsgegevens wordt, overeenkomstig artikel 1, onder b, Wbp, verstaan: "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens [...]". Het betreft hier dus alle gegevensverwerkingen van verzamelen tot en met vernietigen. De aard van de verwerking functioneert de facto als een mogelijk verzwarend element. Dan moet gedacht worden aan een grote hoeveelheid persoonsgegevens van het individu dan wel een bovengemiddeld zwaarwegend effect dat verlies of onrechtmatige verwerking kunnen hebben. Daarbij staan steeds het risico en de schade voor het individu centraal. Extreem gesteld is het dus irrelevant of de gegevens van enkele personen of van miljoenen personen worden verwerkt.

Gehanteerde waarden:

- Er is geen sprake van verwerking van persoonsgegevens, of de gegevens zijn niet te herleiden tot geïdentificeerde of identificeerbare personen.;
- Klasse 0 (Publiek);
  Openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn (de gegevens uit) telefoonboeken, brochures en publieke internetsites.
- Klasse I (Basis);
  Beperkt aantal persoonsgegevens per individu, betrekking hebbend op één type vastlegging, bijvoorbeeld een lidmaatschap, arbeidsrelatie of klant-relatie, zolang deze niet gerekend kunnen worden tot de bijzondere persoonsgegevens.
- Klasse II (Verhoogd Risico)
  Bijzondere persoonsgegevens als genoemd in artikel 16 Wbp, of financieel-economische gegevens in relatie tot de betrokkene.
- Klasse III (Hoog risico)
  Gegevens van opsporingsdiensten en uit DNA databanken, gegevens waar bijzondere, wettelijk bepaalde, geheimhoudingsplicht op rust, gegevens die onder beroepsgeheim vallen (bv. medisch) in de zin van artikel 9, vierde lid, Wet geneeskundige behandelingsovereenkomst.

[8] Blarkom, G.W. van, Borking, drs. J.J., Beveiliging van persoonsgegevens, Registratiekamer, april 2001, Achtergrondstudies en Verkenningen 23, http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx.

Klasse	Aard van de gegevens
Geen persoonsgegevens	De gegevens zijn niet te herleiden tot geïdentificeerde of identificeerbare persoon.
Klasse 0	Publiek. Openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures en publieke internetsites.
Klasse I	Basis. Beperkt aantal persoonsgegevens dat betrekking heeft op één type vastlegging, bijvoorbeeld een lidmaatschap, arbeidsrelatie of klantrelatie zolang deze niet gerekend kunnen worden tot de bijzondere persoonsgegevens.
Klasse II	Verhoogd risico. Bijzondere persoonsgegevens als genoemd in artikel 16 Wbp, of financieel-economische gegevens in relatie tot de betrokkene.
Klasse III	Hoog risico. Gegevens van opsporingsdiensten, DNA databank, gegevens waar bijzondere, wettelijk bepaalde, geheimhoudingsplicht op rust, gegevens die onder beroepsgeheim vallen (bv. medisch) in de zin van artikel 9, vierde lid, Wbp.

De bepaling van de klasse voor persoonsgegevens gaat als volgt:

Stap 1. Doe een initiële inschatting van de klasse aan de hand van de aard van de gegevens, volgens de tabel hierboven.

Stap 2. Bepaal of er verzwarende factoren zijn.
De aard van de verwerking speelt hierbij een belangrijke rol. Ten eerste is hiervan sprake als de dienst een groot aantal gegevens per individu (meerdere vastleggingen, meerdere doelen), verwerkt. Ten tweede is hiervan sprake bij de verwerking van veel verschillende gegevens van veel verschillende personen. Ten derde is hiervan sprake als het doel van de verwerking leidt tot een bovengemiddeld zwaar effect in geval van onrechtmatige verwerking of verlies van de persoonsgegevens.

Stap 3. Indien sprake is van een of meer verzwarende factoren, ga dan één klasse omhoog. Een uitzondering hierop vormen de financieel-economische gegevens, waar geen verzwaring voor aan de orde is. Deze gegevens zijn altijd klasse II ingeschaald.

4 Communiceren van persoonsgegevens, anders dan in dezelfde sessie door gebruiker opgegeven
Het kan voorkomen dat via een website of in een elektronisch bericht persoonsgegevens worden verstrekt of getoond door de dienstverlener aan een burger of bedrijf. Ook kan er sprake zijn van uitwisseling van die persoonsgegevens tussen applicaties. Omdat hierbij sprake kan zijn van ongeoorloofde kennisname door derden, is hiervoor in de regel een hoger betrouwbaarheidsniveau vereist dan voor de opgave van diezelfde (soort) persoonsgegevens door de betrokkene zelf. Daarom is het tonen van persoonsgegevens door een overheidswebsite (of het verstrekken van die gegevens in een bericht) als gevoeliger aangemerkt in de inschaling: voor gegevens in dezelfde klasse is een hoger betrouwbaarheidsniveau vereist. Voor verdere toelichting over de gehanteerde klassen zie de tabel hiernaast.

Gehanteerde waarden:
- geen persoonsgegevens in aanvulling op zelf opgegeven;
- klasse 0;
- klasse I;
- klasse II;
- klasse III.

5 Verwerking van het BSN
In het verlengde van de criteria met betrekking tot de verwerking van persoonsgegevens, geldt de verwerking van het BSN als apart criterium. Het BSN is namelijk bij uitstek een sleutel die de koppeling (aggregatie) van persoonsgegevens mogelijk maakt, zowel binnen organisaties als over organisaties heen. Bovendien gelden voor het gebruik van BSN strikte wettelijke eisen.

Gehanteerde waarden:
- geen verwerking van het BSN;
- het BSN wordt uitsluitend opgegeven door de gebruiker en eventueel teruggekoppeld (eventueel in combinatie met bijvoorbeeld een naam teneinde zekerheid te verkrijgen over de juistheid van het opgegeven BSN). De impliciete opgave van het BSN door DigiD valt hierbinnen;
- het BSN en eventuele aanvullende persoonsgegevens die niet eerder in het proces zijn opgegeven, worden getoond.

6 Juistheid van opgegeven gegevens
Een bijzondere categorie wordt gevormd door de verwerking van opgegeven gegevens in een basisregistratie. De gevolgen van een dergelijke opname kunnen immers groot zijn, omdat afnemers van een basisregistratie verplicht gebruik moeten maken van de gegevens uit die registratie. Onderscheid wordt daarbij wel gemaakt naar mutaties op niet-authentieke gegevens en mutaties op authentieke gegevens, het verplicht gebruik heeft namelijk alleen betrekking op de authentieke gegevens.

Gehanteerde waarden:
- er is geen sprake van het creëren of muteren van een gegeven in een basisregistratie;
- mutatie van niet-authentieke gegevens in basisregistraties;
- mutatie van authentieke gegevens in basisregistraties;
- creëren van authentieke gegevens in basisregistraties.

7 Economisch belang
Er is sprake van economische belangen en ook economische schade bij foutieve identificatie. Het kan hierbij gaan om financiële schade door misbruik of fraude, toegang door onbevoegden tot concurrentiegevoelige informatie (potentiele “lost order”) of het uitlekken van koersgevoelige informatie.

Gehanteerde waarden:
- Nihil: er is geen economische waarde, in ieder geval geen economische schade te verwachten bij foutieve identificatie/authenticatie;
- Gering: het gaat over beperkte economische belangen van een individu. Foutieve identificatie/authenticatie kan leiden tot schade in de ordegrootte van € 1000,-;
- Gemiddeld: het gaat over grotere belangen op individueel niveau of beperkte bedrijfsbelangen. Eventuele schade is te overzien en/of corrigeerbaar. Bedragen tot in de ordegrootte van € 10.000,- per geval;
- Groot: economische omvang (wezenlijk), meer dan € 10.000,-.

8 Publiek belang
Waar hiervoor het belang van de individuele burger of het individuele bedrijf centraal werd gesteld, gaat het hier om het algemeen belang. Daarbij kunnen we onderscheid maken naar publicitaire onrust, politieke onrust en maatschappelijke ontwrichting.

Gehanteerde waarden:
- Publicitair, publiek vertrouwen in dienstverlening
  Laag: klachten, krantenberichten;
  Midden: interventie Nationale Ombudsman, Kamervragen, etc.;
  Hoog: minister valt.
- Maatschappelijke ontwrichting
  Laag: verstoringen, die dooreen enkele organisatie opgelost kunnen worden;

Criteria	Betrouwbaarheidsniveau
- geen rechtsgevolg; - algemene eisen aan betrouwbaarheid en vertrouwelijkheid opgave door betrokkene van publieke persoonsgegevens (klasse 0) - geen tonen van persoonsgegevens door dienstaanbieder - geen verwerking BSN - geen mutaties basisregistratie - economisch belang nihil - publiek belang laag	0 (geen eisen aan authenticatie)
- geen rechtsgevolg - algemene eisen aan betrouwbaarheid en vertrouwelijkheid - opgave van persoonsgegevens, maximaal klasse I - tonen of communiceren van persoonsgegevens, maximaal klasse 0 - geen verwerking BSN - geen mutaties basisregistratie - economisch belang nihil - publiek belang laag	1
- al dan niet (direct of indirect) rechtsgevolg - wettelijke eisen omtrent ondertekening - opgave van persoonsgegevens in maximaal klasse II - tonen of communiceren van persoongegevens, max. klasse 1 - BSN wordt verwerkt, opgave door gebruiker, evt. via DigiD - geen mutatie basisregistratie - economisch belang gering - publiek belang midden	2
- (direct of indirect) rechtsgevolg - wettelijke eisen omtrent ondertekening of wilsuiting - opgeven persoonsgegevens maximaal klasse III - tonen of communiceren persoonsgegevens klasse II - BSN wordt verwerkt, al dan niet opgave door gebruiker - mutatie nietauthentieke gegevens basisregistraties - economisch belang gemiddeld - publiek belang midden	3
- (direct of indirect) rechtsgevolg - wettelijke eisen aan ondertekening, nadere vormeisen - opgeven van persoonsgegevens van klasse III - tonen of communiceren van persoonsgegevens klasse III - BSN wordt verwerkt, al dan niet opgave door gebruiker - verwerking gegevens leidt tot muteren of creëren authentiek gegeven in basisregistratie - economisch belang groot - publiek belang hoog	4

Midden: verstoringen die gecoördineerd optreden van meerdere organisaties, veelal publiek en privaat, vragen;
Hoog: noodtoestand; verstoringen die noodmaatregelen vereisen buiten de normale juridische, financiële kaders, etc.

4.2 Het classificatiemodel

In het 'classificatiemodel' op de vorige pagina worden de gedefinieerde criteria afgezet tegen de betrouwbaarheidsniveaus. Door voor elk van de 8 criteria de meest toepasselijke waarde te kiezen voor de desbetreffende dienst, kan het toepasselijke betrouwbaarheidsniveau bepaald worden.

4.3 Referentiescenario

Het classificatiemodel is goed bruikbaar bij een gemiddelde kwetsbaarheid van proces en IT. De aannames over die gemiddelde kwetsbaarheid zijn hieronder expliciet gemaakt, ze vormen als het ware het referentiescenario. Een aantal veel voorkomende afwijkingen ten opzichte van dit scenario zijn aangewezen als correctiefactoren. Dat wil zeggen dat ze (kunnen) leiden tot een bijstelling van het op basis van het classificatiemodel bepaalde betrouwbaarheidsniveau of tot de conclusie dat een volledige risicoanalyse uitgevoerd moet worden.

Aannames betreffende de afbakening van het soort diensten en hun gebruikers:

- Het gaat om interactieve, online diensten voor burgers en/of bedrijven en daarnaast om applicatie-applicatieverkeer en retourstromen;
- Burgers nemen diensten af voor zichzelf of laten diensten afnemen door gemachtigden. Werknemers nemen diensten af voor de onderneming waarvoor ze werken;
- Het is duidelijk afgebakend welk soort regeling en welk type dienst het betreft.

Aannames betreffende de beheersing van IT beveiliging en privacy:

- De organisatie heeft werkende managementsystemen voor informatiebeveiliging en bescherming van persoonsgegevens;
- Er is een geïmplementeerd en actueel beveiligingsplan aanwezig voor de IT dat ten behoeve van de dienst in kwestie wordt gebruikt. Dit plan is gebaseerd op gangbare normen en/of een specifieke risicoanalyse;
- Er is specifiek voor de desbetreffende regeling/dienst bekend welke persoonsgegevens worden verwerkt en wat voor soort verwerkingsacties het betreft.

Aannames betreffende het proces dat de regeling afhandelt/de dienst voortbrengt:

- De geldende wettelijke vereisten voor de dienst worden in acht genomen;
- De gebruiker wordt bij het verlenen van toegang tot de gezochte dienst geauthenticeerd. In het navolgende proces wordt die identiteit gehanteerd;

- Aanvullende maatregelen om die identiteit langs andere wegen te verifiëren blijven beperkt tot backoffice-controles; er zijn geen extra controles waarbij aan de gebruiker gevraagd wordt aanvullende zekerheden over de identiteit te verstrekken;
- Bij diensten die een besluit van een bestuursorgaan omvatten, 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 dat waarlangs de dienst oorspronkelijk is aangevraagd.

4.4 Correctiefactoren

De bovengeschetste aannames (het referentiescenario) en het daarop gebaseerde classificatiemodel geven niet onder alle omstandigheden een juiste uitkomst. Er zijn zowel risicoverlagende als risicoverhogende factoren.

Risicoverlagende factoren komen vooral voor als er extra processtappen zijn, waarin het risico gemitigeerd wordt. Op basis hiervan kan beargumenteerd voor een lager betrouwbaarheidsniveau worden gekozen dan het classificatiemodel aangeeft.

Risicoverhogende factoren zijn met name gelegen in de context van de dienst in kwestie. Het gaat dan om factoren zoals politieke of bestuurlijke gevoeligheid en/of relevantie voor het imago. Hier is gekozen om niet te volstaan met het voorschrijven van een hoger betrouwbaarheidsniveau, maar om in dergelijke gevallen aan te raden alsnog een volledige risicoanalyse uit te voeren.

Risicoverlagende factoren

De volgende risicoverlagende factoren worden onderkend:

1. In het vervolgproces bevindt zich een processtap waarin de belanghebbende zich fysiek moet melden en legitimeren (ID-document en BSN). Op die manier wordt geborgd dat de belanghebbende daadwerkelijk de dienst in kwestie wil afnemen, met de aangeleverde gegevens in kwestie.
2. Terugkoppeling van mutaties of (voorgenomen) besluiten vindt plaats via een ander kanaal dan het oorspronkelijke (elektronische) kanaal.
3. In het vervolgproces bevindt zich een processtap waarin gegevens of stukken voorkomen die los van de dienstafname de betrokkenheid en toestemming van de belanghebbende bewijzen.
4. Er is sprake van voortdurende en actieve monitoring waarmee voorkomen wordt dat een dienst in korte tijd heel vaak benaderd wordt door dezelfde betrokkene of dat andere gebruikspatronen voorkomen die op fraude duiden. Ook het bijhouden van risico- of handhavingsprofielen kan hieronder worden geschaard.
5. Waar het economisch belang de bepalende factor is in de bepaling van het betrouwbaarheidsniveau en er sprake is van financiële diensten: verificatie van de rekeninggegevens waarop betalingen plaatsvinden.

Als een risicoverlagende factor van toepassing is, dan kan het betrouwbaarheidsniveau vaak met één stap verlaagd worden. Wanneer wettelijke eisen het betrouwbaarheidsniveau bepalen (bijvoorbeeld vormeisen aan ondertekening), is dat niet mogelijk.

Ook is verlaging van betrouwbaarheidsniveau 1 naar 0 niet toegestaan. Risicoverlagende factoren kunnen immers de aard van de gegevens niet veranderen. Daar waar er sprake is van persoonsgegevens zullen altijd enige maatregelen nodig blijven om de betrouwbaarheid en vertrouwelijkheid van die gegevens te garanderen.

Risicoverhogende factoren.

Situaties waarin een volledige risicoanalyse is geboden, betreffen de volgende:

- De dienst kent een inherent groot politiek, bestuurlijk of imagorisico;
- Het risico is moeilijk te bepalen omdat er sprake is van beperkte direct aan het incident gerelateerde schade maar grote potentiële vervolgschade (anders dan de situatie dat er gemuteerd wordt op authentieke gegevens van een basisregistratie);
- De dienst heeft een hoog potentieel voor grootschalig misbruik. Met name de combinatie van massale processen, beperkte controlemogelijkheden en (bij grote schaal) hoog potentieel gewin.

4.5 Voorbeelden van diensten en de bijbehorende betrouwbaarheidsniveaus

In deze paragraaf worden bij wijze van voorbeeld diensten genoemd met de daarbij volgens de bovenstaande criteria behorende betrouwbaarheidsniveaus.

Criteria	Betrouwbaarheidsniveau
Anoniem bezoeken overheidswebsites	0 (geen eisen)
Gemeentelijke lokale diensten (melden gebreken in de openbare ruimte, aanvragen afvalcontainers)	1
Registreren voor gepersonaliseerde portalen (MijnOverheid.nl, mijndenhaag.nl ed.) Gemeentelijke vergunningen (kap, evenementen ed.) Omgevingsvergunning particulieren Financiële aanspraak particulieren (subsidie, uitkering, toeslag) Verblijfsvergunning au pair (Status)informatie in MijnOverheid.nl Melden/registreren Aangifte (delicten, licht) Wijzigingen doorgeven Belastingaangifte particulieren, geen voorinvulling gegevens over persoonlijke financiele situatie. Naleving vergunning¬voorschriften particulieren Inzien WOZ waardering	2
Belastingaangifte particulieren; ophalen of muteren vooringe-vulde aangifte (tonen persoonsgegevens klasse II) Aanbestedingsdocumenten indienen Omgevingsvergunning ondernemingen, verblijfsvergunning arbeids/kennismigranten officiële documenten (VOG, paspoort, rijbewijs ed.) Belastingaangifte ondernemingen Financiële aanspraak ondernemingen (subsidie) (Financiële) verantwoordingen (jaarrekening ed.)	3
Aangifte (geboorte) Raadplegen medisch dossier Aangifte (delicten, zwaar) Octrooiaanvragen	4

5 Machtigingen

5.1 Waar gaat het eigenlijk over?

In veel situaties laten burgers of bedrijven zich vertegenwoordigen door iemand anders. Fiscaal dienstverleners of buren verzorgen de belastingaangifte voor burgers. Gespecialiseerde kantoren verzorgen een subsidieaanvraag voor hun klanten.

De overheid ontwikkelt steeds meer elektronische diensten. Het belang om het gebruik van machtigingen te kunnen herkennen en goed te ondersteunen neemt daardoor toe. Het is immers niet gewenst dat intermediairs en andere vertegenwoordigers aan burgers of bedrijven om hun inloggegevens vragen en daarmee inloggen, als waren zij die burger of dat bedrijf. In andere situaties claimen intermediairs zelf dat ze een bepaald bedrijf of een bepaalde burger vertegenwoordigen, maar kan de dienstaanbieder deze claims niet eenvoudig verifiëren.

Om vertegenwoordigingssituaties in de elektronische wereld beter te regelen, is het van belang te streven naar expliciet vastgelegde machtigingen.
De machtiging ligt veelal vast in een machtigingsregister, waaromheen een vertrouwensdienst wordt geboden. Het machtigingenregister verstrekt bevoegdheidsverklaringen: elektronische berichten omtrent de bevoegdheid van de handelende partij en de zekerheid omtrent die bevoegdheid, alsmede eventuele details omtrent de machtiging.

5.2 Het perspectief van de individuele dienst

Vertegenwoordiging heeft in principe geen invloed op het door de dienstverlener gevraagde betrouwbaarheidsniveau voor een individuele dienst, de aard van de dienst verandert er namelijk niet door.

Aannemende dat de machtigingen niet door dedienstaanbieder zelf worden geadministreerd, zijn er machtigingsdiensten nodig, die machtigingen registreren en bevoegdheidsverklaringen afgeven van een passend betrouwbaarheidsniveau. Als de dienst een betrouwbaarheidsniveau 3 vraagt, dan moeten ook de bevoegdheidsverklaringen van tenminste betrouwbaarheidsniveau 3 zijn.

Dat heeft consequenties voor de wijze van registreren en beheren van de machtiging door de machtigingsregisters, die moeten namelijk zodanig zijn ingericht dat het gewenste betrouwbaarheidsniveau verzekerd is. Hiervoor zijn internationaal nog geen geaccepteerde standaarden beschikbaar, maar er zijn op dit gebied wel documenten in de maak in zowel Europees (STORK) als nationaal (eID stelsel NL) verband. Verder hanteert eHerkenning standaarden voor betrouwbaarheidsniveaus van machtigingen, waarbij dezelfde denklijn als in STORK[9] is aangehouden. In de hier bedoelde documenten worden bepalingen over de geldigheidsduur van machtigingen, bewaartermijnen en geldigheid van bevoegdheidsverklaringen gegeven.

Het is van belang te onderkennen dat machtigingen worden uitgegeven 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 echter ook denkbaar dat er geen gebruik wordt gemaakt van machtigingsregisters en hun diensten en dat de dienstaanbieder machtigingen ontvangt in de vorm van papier, ongestructureerd digitaal (PDF) of gestructureerd digitaal (gewaarmerkt bericht).

5.3 Wat betekent dit voor toepassing van het classificatiemodel?

Voor het inrichten van de individuele dienst geldt het betrouwbaarheidsniveau zoals dat volgt uit de toepassing van het classificatiemodel. Of er al dan niet wordt vertegenwoordigd/gemachtigd, verandert niets aan de criteria of toepassing van de methodiek en daarmee niets aan de uitkomst. Voor de dienstaanbieder is het van belang dat de authenticatie die hij ontvangt van het juiste niveau is en, wanneer deze een gemachtigde betreft, ook vergezeld gaat van een bevoegdheidsverklaring op hetzelfde betrouwbaarheidsniveau. Of er wel of niet wordt gemachtigd, is een zaak van de gebruiker van de dienst.

5.4 Overige aandachtspunten

Het risico op misbruik of fraude kan in beginsel groter worden als de mogelijkheid wordt opengesteld voor vertegenwoordiging. Fraudeurs kunnen immers proberen massaal frauduleuze machtigingen te claimen of te registreren. Dit risico dient te worden ondervangen; ten eerste door iedere keer dat een dienst wordt afgenomen een machtiging te vereisen en ten tweede door voldoende stringente eisen te formuleren aan de registratie en het gebruik van machtigingen, via referentie aan normatieve documenten op dit gebied (van eHerkenning, of straks eID stelsel NL dan wel Europese voorschriften).

Wanneer het registreren van een machtiging een wezenlijk hogere drempel kent dan het gebruiken van de dienst zelf, zal ongewenst gedrag dat ook nu voorkomt, zoals het doorgeven van inloggegevens aan intermediairs, een probleem blijven. Dit moet worden meegewogen wanneer vertegenwoordiging een rol speelt bij de aangeboden dienst. Verder is het voor de dienstaanbieder te overwegen om de machtigingen i.c. het gebruik van die machtigingen terug te (laten) koppelen aan de betrokkenen. Daarmee krijgt de betrokken burger of het betrokken bedrijf concreet inzicht in wie namens hem diensten bij de overheid afneemt.

[9] Het STORK QAA framework zal waarschijnlijk worden aangepast in lijn met de aanbevelingen in het QAA Status Report dat in verband van STORK 2 is opgeleverd, zie https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=4&cid=31

6 Applicatie-applicatieverkeer

6.1 Waar gaat het eigenlijk over?

Steeds vaker is er bij elektronische dienstverlening geen sprake meer van menselijke tussenkomst. Wanneer een dienst door de ene geautomatiseerde entiteit wordt afgenomen bij een andere geautomatiseerde entiteit, noemen we dat applicatie-applicatieverkeer. Bij de beveiliging van dat verkeer is er een onderscheid tussen 'kanaal' en 'inhoud':

- De beveiliging van het kanaal.
  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 niet door een derde worden gelezen of gewijzigd;

- De beveiliging van de inhoud.
  Het is daarnaast ook mogelijk het bericht zelf te beveiligen. Een bericht wordt dan ondertekend of gewaarmerkt en wellicht ook versleuteld. Berichten kunnen zo end-to-end beveiligd worden doorgegeven. Het is niet mogelijk het bericht tijdens het transport te lezen of te wijzigen.

In tabel 1 zijn enkele kenmerkende verschillen weergegeven tussen kanaal-beveiliging en inhoudsbeveiliging.

Beveiliging kanaal	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

Tabel 1 Kanaalbeveiliging versus beveiliging van de inhoud

Voor zowel de beveiliging van het kanaal als de beveiliging van de inhoud geldt dat digitale certificaten de *de facto* beveiligingsstandaard zijn. Als gevolg van het feit dat voor beide soorten beveiliging (vergelijkbare) digitale certificaten nodig zijn, worden beide vormen van beveiliging vaak in combinatie ingezet. Vooraf tussen partijen gedeelde geheimen (wachtwoorden en dergelijke) worden ook wel gebruikt om te beveiligen, maar digitale certificaten genieten veelal de ze meer zekerheid verschaffen.

6.2 Het perspectief van de individuele dienst

De volgende eigenschappen zijn kenmerkend voor applicatie-applicatieverkeer:

- Er is geen menselijke tussenkomst;
- Het gaat om communicerende applicaties, de natuurlijke persoon is buiten beeld;
- Het gaat vaak om aanzienlijke volumes.

Een toepassing waar digitale certificaten nu grootschalig worden ingezet is de betrouwbare aanlevering van berichten in het kader van SBR (Standard Business Reporting). Bedrijven of intermediairs die aangiften VpB en/of IB (gaan) aanleveren, beveiligen hun communicatie (applicatie-applicatieverkeer) met DigiPoort met behulp van een PKIoverheid (services) servercertificaat. In de komende jaren gaan nog veel meer toepassingen gebruikmaken van SBR, zoals de OB-aangifte, het deponeren van jaarrekeningen en statistische rapportages.

6.3 Wat betekent dit voor toepassing van het classificatiemodel?

Voor applicatie-applicatieverkeer en daarmee de identificatie van de communicerende organisaties, wordt de risicogestuurde benadering uit deze handreiking minder zinvol geacht. In de praktijk gaat het toch om digitale certificaten, waarmee de keuze feitelijk wordt teruggebracht tot een keuze hoe betrouwbaar die certificaten dienen te zijn. Daarbij is er de facto gekozen voor PKIoverheid certificaten. Dit geldt zowel voor de beveiliging van het kanaal als van de inhoud. In het BIR wordt voor de betrouwbare authenticatie van en communicatie met organisaties gestandaardiseerd op PKIoverheidcertificaten.[10] Voor zeer gevoelige applicatie-applicatie communicatie wordt door de overheid overigens het gebruik van een 'private root' gepropageerd.

[10] Zie http://www.logius.nl/producten/toegang/pkioverheid/

6.4 Overige aandachtspunten

Lessen uit het DigiNotar incident

Het DigiNotar incident heeft zeer manifest gemaakt dat (overheids) organisaties heel afhankelijk zijn van het gebruik van digitale certificaten, zowel voor kanaalbeveiliging als voor de beveiliging van de inhoud. Rapporten zoals dat van de Onderzoeksraad voor Veiligheid[11] en de Adviescommissie A3 Bedrijven[12] gaan hier nader op in.
De drie belangrijkste aandachtspunten voor dienstverleners zijn:

- Zorg dat u voor tijdskritische toepassingen reservecertificaten van alternatieve certificaatdienstverleners op voorraad heeft;
- Zorg dat u in uw organisatie meer dan één certificatenbeheerder heeft, dat is een gemachtigde die namens uw organisatie nieuwe certificaten van verschillende certificaatdienstverleners kan aanvragen, oude certificaten kan intrekken, etc.);
- Voorkom single-points-of-failure die er bij falen toe leiden dat een heel proces of een hele keten tot stilstand komt.

[11] Zie https://www.onderzoeksraad.nl

[12] Zie http://www.eherkenning.nl

7 Retourstromen

7.1 Waarover praten we eigenlijk?

De verdere ontwikkeling van de elektronische overheid betekent niet alleen dat gebruikers de dienstaanbieder digitaal benaderen, maar ook dat de dienstaanbieder gebruikers digitaal benadert of antwoordt. Dit uitgangspunt geldt niet alleen voor communicatie met personen maar ook voor interactie tussen applicaties. Deze 'retourstroom' is een belangrijk onderdeel van de elektronische communicatie.

We onderkennen voor retourstromen in de praktijk de volgende scenario's.

- Het 'e-mail scenario'
  De dienstaanbieder verstuurt een elektronisch bericht naar het e-mailadres van een natuurlijke persoon;

- Het 'inzage op webportaal' of 'Berichtenbox' scenario
  De dienstaanbieder plaatst berichten in een eigen, beveiligd webportaal en attendeert de burger er (via SMS of e-mail) op dat er een bericht klaar staat.

  Het 'Berichtenbox' scenario is een functioneel hierop gelijkende variant, waarbij gebruik wordt gemaakt van een gemeenschappelijke voorziening, de Berichtenbox. De dienstaanbieder plaatst het bericht in dit scenario in de Berichtenbox (voor burgers dan wel bedrijven) in plaats van op het eigen webportaal;

- Het 'applicatie-applicatieverkeer' scenario
  De dienstaanbieder laat retourstromen via applicatie-applicatieverkeer verlopen, direct naar de betrokken organisatie of naar een intermediair.

7.2 Het perspectief van de individuele dienst

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

- Het bericht of document moet de geadresseerde bereiken;
- Onbevoegde derden moeten geen toegang kunnen krijgen tot het bericht of het document;
- De geadresseerde moet kunnen verifiëren dat het bericht of document ook daadwerkelijk afkomstig is van de betreffende dienstaanbieder.

Bovenstaande zaken volgen direct uit de bepalingen van de Algemene Wet Bestuursrecht (Awb) over elektronisch verkeer. Bij een retourbericht is er sprake van een gedeelde verantwoordelijkheid tussen dienstaanbieder en geadresseerde om er voor te zorgen dat het retourbericht de geadresseerde ook werkelijk bereikt. De dienstaanbieder moet een betrouwbaar en veilig medium regelen, de burger of het bedrijf moet zelf zijn post controleren.

Bij dit alles geldt dat de Awb het aan de burger of het bedrijf over laat of zij de elektronische weg willen openstellen. Vanaf het moment dat zij die elektronische weg openstellen, worden zij ook verondersteld langs die weg bereikbaar te zijn.

Met bovenstaande in het achterhoofd betekent dit het volgende voor de hierboven genoemde praktische scenario's.

Het e-mail scenario
In het e-mail scenario zit de zwakste schakel in het bijhouden, door de burger of het bedrijf, van een actueel e-mailadres. Burgers en bedrijven ondervinden maar een beperkte prikkel om een eerder opgegeven e-mail adres actueel te houden. Daarnaast speelt dat e-mail in veel opzichten een minder betrouwbaar en vertrouwelijk medium is. Voor gevoelige gegevens is het daarom nodig om de berichten te versleutelen. Om dat mogelijk te maken moet de dienstaanbieder kunnen beschikken over een digitaal certificaat van die burger of dat bedrijf. Dit leidt tot een probleem dat vergelijkbaar is met dat van het bijhouden van e-mailadressen: burgers en bedrijven ondervinden geen prikkel om een actueel certificaat ter beschikking te stellen.

Ook zijn bij e-mail aanvullende maatregelen nodig om de geadresseerde de mogelijkheid te bieden om te verifiëren dat het bericht inderdaad afkomstig is van de overheid. Een van de mogelijkheden hiervoor is het waarmerken van de berichten zelf (zie hiervoor het kader 'waarmerken door de overheid' onder 7.4).

E-mail is hierdoor niet geschikt als algemeen toepasbaar medium voor de inrichting van retourstromen. Waar e-mail wel redelijk geschikt voor is, is voor terugkoppeling van weinig gevoelige gegevens, waarbij het te gebruiken e-mailadres kort daarvoor door de burger of het bedrijf is opgegeven. Denk daarbij aan algemene informatie of serviceberichten.

Het 'Webportaal' of 'Berichtenbox' scenario
Dienstaanbieders kunnen retourberichten op een eigen webportaal zetten en burgers daar dan toegang toe geven met bijvoorbeeld hun DigiD. Zij maken echter steeds vaker gebruik van de generieke voorziening Berichtenbox (onderdeel van MijnOverheid) in plaats van hun eigen webportaal. In de Berichtenbox kunnen de geadresseerden (retour)berichten van de overheid openen en lezen in een veilige omgeving. De Berichtenbox stuurt de burger een attenderingsbericht als er nieuwe berichten op de Berichtenbox zijn aangekomen. Ook voor bedrijven is er een Berichtenbox waarnaar retourberichten voor bedrijven kunnen worden gestuurd.

Ervan uitgaand dat de omgeving van de Berichtenbox (c.q. het webportaal zelf) voldoende beveiligd is, blijft het belangrijk er zekerheid over te hebben dat de juiste persoon toegang krijgt tot de betreffende berichten. Daartoe biedt de Berichtenbox voor burgers zekerheden tot betrouwbaarheidsniveau 2 door toegang te verlenen met DigiD en aan de hand van het verkregen BSN de toegang tot de berichten van een persoon te beperken. Dat een document afkomstig is van de overheid weet de geadresseerde vrij zeker, aangezien de bron de Berichtenbox of een andere vertrouwde webdienst is.

Ook in dit scenario geldt dat men uiteindelijk afhankelijk is van de beschikbaarheid van een actueel e-mail adres of 06-nummer om de burger of het bedrijf op nieuwe berichten te attenderen. Deze zwakte is wat minder prominent aanwezig dan in het e-mail scenario, maar bestaat nog steeds.

Het applicatie-applicatieverkeerscenario
In het geval dat de dienstaanbieder een retourbericht rechtstreeks naar de betrokken organisatie stuurt, zorgt de kanaalbeveiliging voor de gewenste zekerheden. Deze kanaalbeveiliging verzekert namelijk dat buitenstaanders geen toegang kunnen krijgen tot het bericht. En gegeven het structurele karakter van het opzetten van applicatie-applicatiekoppelingen is de bereikbaarheid van de geadresseerde inherent goed geregeld. Een applicatie-applicatiekoppeling is dus zeer betrouwbaar.

In het geval van vertegenwoordiging zal de dienstaanbieder vaak zowel de intermediair als de betrokkene willen berichten. Een bijzondere situatie is daarbij dat sommige intermediairs ook elektronische diensten leveren aan de klanten die zij vertegenwoordigen. Het is dus een overweging om de retourstroom aan de burger of het bedrijf via het elektronische kanaal van hun intermediair te laten verlopen. In alle gevallen is het echter aan de betrokkene om aan te geven hoe hij elektronisch bereikbaar wil zijn.

7.3 Wat betekent dit voor toepassing van het classificatiemodel?

Het classificatiemodel wordt in principe toegepast op de toegang tot het retourbericht als dienst. In de praktijk betekent dat echter dat het classificatiemodel wordt toegepast op de totale dienst waar het retourbericht deel van uitmaakt. Waar het bij de classificatie gaat om de 'klasse' van de gegevens wordt dan specifiek gekeken naar de gegevens zoals die in het retourbericht zijn opgenomen.

De classificatie levert een gewenst betrouwbaarheidsniveau op voor het retourbericht, in de context van de dienst. Op basis van de uitkomst van de classificatie staan dan de volgende mogelijkheden open:

- Voor het e-mail scenario geldt dat dit niet bruikbaar is voor berichten waarbij een betrouwbaarheidsniveau hoger dan 1 aan de orde is;
- Voor het 'inzage op webportaal' of 'Berichtenbox' scenario geldt dat het voor de toegang tot portaal of Berichtenbox gebruikte betrouwbaarheidsniveau van authenticatie bepaalt tot welke retourberichten toegang kan worden gegeven. Het betrouwbaarheidsniveau van de authenticatie die toegang geeft tot het webportaal of de Berichtenbox moet dan dus gelijk aan of hoger zijn dan het gewenste betrouwbaarheidsniveau passend bij de retourberichten waartoe toegang wordt verleend;
- Voor het 'applicatie-applicatieverkeer scenario' geldt dat de beveiligingsbehoefte goed wordt gedekt door de voor de kanaalbeveiliging veelal gehanteerde PKIoverheids (services) servercertificaten. Als de situatie wordt gecompliceerd doordat de uiteindelijke bestemming voor een retourbericht nog een andere is, dan welke direct via de applicatie-applicatiekoppeling wordt bereikt, dan is een uitgebreide risicoanalyse nodig.

7.4 Overige aandachtspunten

Verschuivingen met juridische gevolgen
We zien dat het klassieke model "overheid verstuurt juridisch belangrijke documenten naar ontvanger" met de hieraan gekoppelde "brengverplichting" langzaam plaats maakt voor een model waarbij de burger of het bedrijf een "haalverplichting" krijgen. Feitelijk is er altijd een bepaalde actie zowel van verzender als ontvanger vereist, brengen en halen. Wat brengen en halen betekent verschuif 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.

Een tweede verschuiving betreft de verschuiving van het huidige nevengeschikte karakter van elektronische dienstverlening, naar de situatie dat de elektronische dienstverlening de geprefereerde optie wordt. Ook de juridische situatie rond de retourstroom zal daarmee waarschijnlijk gaan veranderen, hoewel nu nog onduidelijk is hoe precies. Momenteel is er in de Awb/Wet Elektronisch Bestuurlijk Verkeer sprake van 'nevenschikking' van het elektronische kanaal naast het papieren kanaal. Daarbij moeten burger en overheid (bestuursorgaan) het elektronische kanaal bewust openstellen voor elektronische communicatie mogelijk is. De beweging naar 'Digitaal, tenzij..' is echter onmiskenbaar en dit zal ook betekenen dat men steeds minder makkelijk onder de digitale vorm van dienstverlening uit kan.

Waarmerken van documenten door de overheid
Vaak wil een burger of een bedrijf kunnen vaststellen dat bepaalde documenten inderdaad van een autoriteit afkomstig zijn, bijvoorbeeld van de overheid. Dat kan bijvoorbeeld het geval zijn bij digitale documenten die men elders weer als bewijs dient te overleggen. Het gaat daarbij om een brede variëteit aan documenten zoals Beschikkingen, Uittreksels, Officiële verklaringen omtrent een medische of financiële situatie, et cetera. Het kan ook gaan om openbare bekendmakingen, waarvan men met zekerheid wil kunnen vaststellen dat het officiële documenten van een bepaalde overheid betreffen.

Ter vergroting van de rechtszekerheid van burgers en bedrijven is het wenselijk om al dit soort documenten digitaal te waarmerken. Dit waarmerken kan met een digitale handtekening van de betreffende overheidsorganisatie. Daarbij geldt dat het een waarmerking is namens een (geautomatiseerd systeem van een) organisatie en niet zozeer een elektronische ondertekening door een functionaris van die organisatie.

Omwille van interoperabiliteit met systemen die dit al uitvoeren voor documenten die worden opgesteld in het kader van de DienstenRichtlijn, verdient het aanbeveling om hierbij de standaardformaten Pades, Xades of Cades te hanteren, zoals vastgelegd in Besluit EU 2011/130.

Naast het waarmerken van dergelijke documenten doet een dienstverlener er goed aan om ook faciliteiten te bieden om gewaarmerkte documenten online te verifiëren. In de gevallen die onder de Dienstenrichtlijn vallen èn waar een ander formaat wordt gehanteerd dan de voornoemde is zo'n verificatiedienst zelfs verplicht.

8 Eénmalig inloggen

8.1 Waar gaat het eigenlijk over?

Eénmalig inloggen, ook bekend als Single sign-on (SSO), is de mogelijkheid voor gebruikers om via één authenticatievoorziening toegang te krijgen tot verschillende diensten. De gebruiker kan dan volstaan met inloggen bij de eerste dienst en hoeft daarna niet steeds opnieuw zijn identiteit te bevestigen. SSO is mogelijk voor een samenstel van diensten van één organisatie of domein maar ook over organisaties en domeinen heen.

Voorbeeld
MijnOverheid biedt, wanneer een burger inlogt, toegang tot een hele set van (samengestelde) gegevens en diensten van verschillende (overheids) organisaties, zoals de GBA, de RDW en de stichting Pensioenregister.

Het DR loket (dienst regelingen loket) van het ministerie van Economische Zaken 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 éénmalig inloggen is de federatie. In feite is de federatie de groep organisaties die gezamenlijk gebruik maken van een SSO-oplossing. Door deelname aan een federatie spreekt een organisatie het geclausuleerde vertrouwen uit in de authenticatie die afkomstig is uit het inlogproces dat (mogelijk) elders, bij een ander lid van de groep, heeft plaatsgevonden.

Federaties bestaan in verschillende smaken. Er zijn federaties die authenticeren op één betrouwbaarheidsniveau, maar ook federaties die verschillende betrouwbaarheidsniveaus kunnen faciliteren. In dit laatste geval moet, wanneer de gebruiker van een dienst overstapt naar een andere dienst met een hoger betrouwbaarheidsvereiste dan dat waarmee de gebruiker zich eerder heeft geauthenticeerd, de gebruiker zich opnieuw dan wel aanvullend authenticeren. Federaties kunnen sterk verschillen in omvang, van een individuele organisatie die een aantal elektronische diensten binnen één portaal aanbiedt tot een overheidsbreed portaal dat diensten van een groot aantal verschillende organisaties ontsluit.

Nauw verbonden aan éénmalig inloggen is éénmalig uitloggen (Single sign off) waarbij de gebruiker in één keer verschillende sessies waarin hij diensten afneemt beëindigt.

8.2 Het perspectief van de individuele dienst

Vanuit het perspectief van één enkele dienst, is éénmalig inloggen één van de manieren waarop een identiteit en een authenticatie daarvan kunnen worden aangeboden aan een dienstaanbieder. Voor de dienstaanbieder is alleen van belang op welk niveau van betrouwbaarheid de authenticatie heeft plaatsgevonden en of deze nog geldig is.

Eénmalig inloggen op zichzelf kent echter een aantal vraagstukken dat breder is dan de afweging die een dienstaanbieder voor zijn individuele dienst maakt. Daarom zijn in paragraaf 8.4 hieromtrent enkele aandachtspunten benoemd.

8.3 Wat betekent dit voor toepassing van het classificatiemodel?

Eenmalig inloggen en het perspectief van de individuele dienst werpen geen nieuw licht op de criteria en afwegingen van het classificatiemodel. Eenmalig inloggen is in feite onderdeel van het aanbod aan authenticatiediensten.

De individuele dienst wordt conform het classificatiemodel gewaardeerd en ingeschaald op een bepaald betrouwbaarheidsniveau. De authenticatie die toegang geeft tot deze dienst, zal moeten passen bij dit betrouwbaarheidsniveau, ongeacht de afkomst van deze authenticatie.

8.4 Overige aandachtspunten

Het perspectief van de individuele dienst vereenvoudigt het denken over éénmalig inloggen. Wanneer het onderwerp breder wordt beschouwd kent éénmalig inloggen echter een aantal aandachtspunten dat voor dienstaanbieders van belang is. De twee meest prominente aandachtspunten worden hier geïntroduceerd.

8.4.1 Deel uitmaken van een federatie

Het is een afweging voor de dienstaanbieder om wel of niet gebruik te maken van authenticaties die voortkomen uit een federatie. Verschillende aspecten spelen hierbij een rol:

1. De invloed die dienstverlener heeft op de inrichting en werking van de federatie;

2. De mogelijk opwaartse druk op het betrouwbaarheidsniveau die het gevolg is van het toetreden tot de federatie;
   Federaties zijn er in verschillende soorten en maten. Sommige federaties hebben de mogelijkheid verschillende betrouwbaarheidsniveaus te ondersteunen, andere federaties niet. Voor de dienstaanbieder geldt dat als de federatie één betrouwbaarheidsniveau kent, er een opdrijvende werking kan ontstaan als dat betrouwbaarheidsniveau hoger is dan het niveau waarom de dienst vraagt. Een (eventueel nieuwe) dienst binnen de federatie met behoefte aan een ho(o)g(er) betrouwbaarheidsniveau kan of zal daarnaast discussie uitlokken over het niveau waarop binnen de federatie als geheel wordt geauthenticeerd.

3. Het gebruiksgemak voor de klant.
   Een federatie met verschillende betrouwbaarheidsniveaus biedt relatief minder gebruikersgemak. Wanneer de gebruiker overstapt op een dienst met een hoger betrouwbaarheidsniveau moet hij zich opnieuw authenticeren, vergelijkbaar met de situatie zonder federatie en zonder SSO.

Voorbeeld

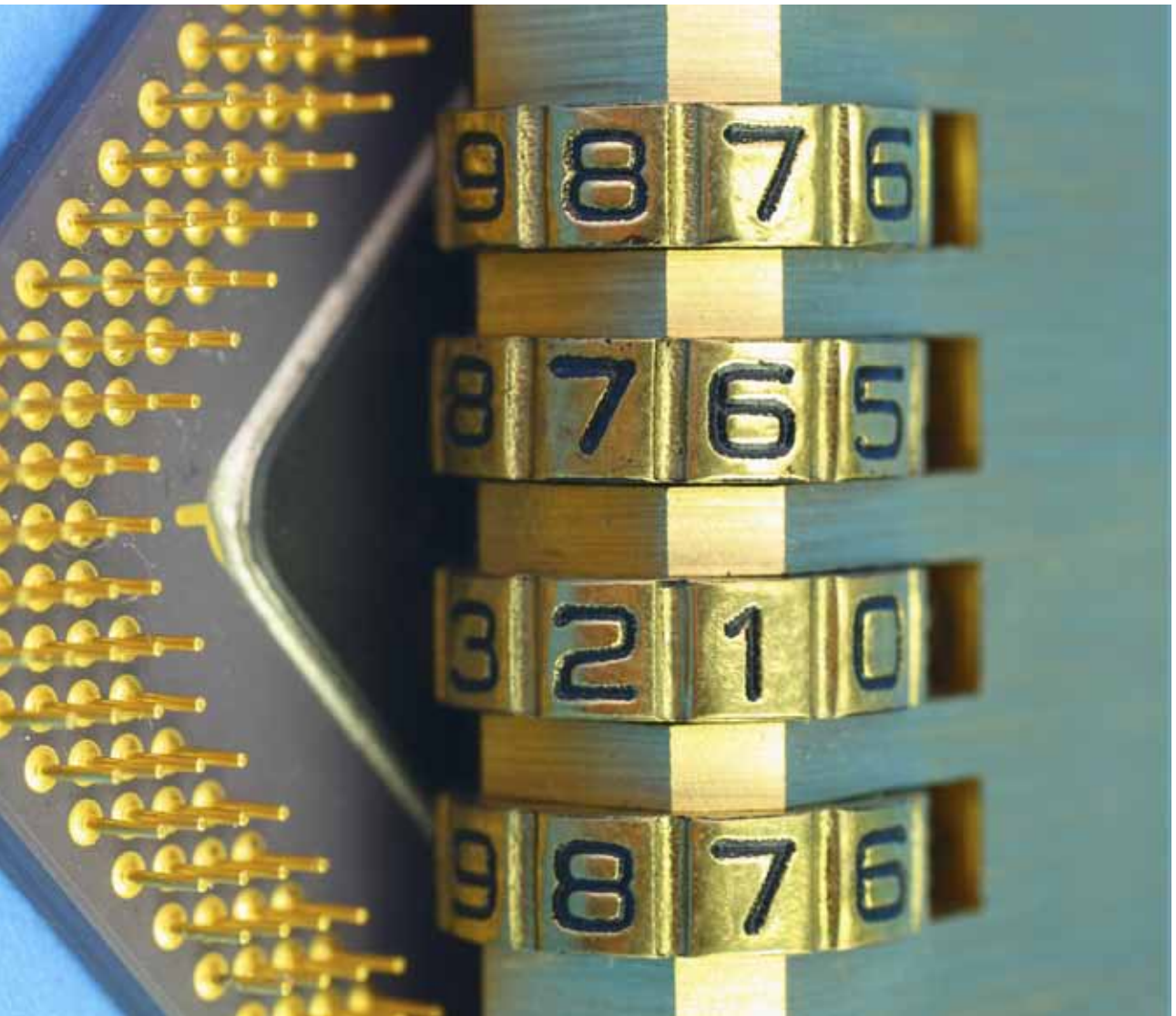
De dienstaanbieder bepaalt het gewenste betrouwbaarheidsniveau voor het afnemen van de individuele dienst. Als een lager betrouwbaarheidsniveau beschikbaar is dan de dienst vraagt, leidt dit tot het weigeren van de toegang tot de dienst. Wel kunnen dienstverleners overwegen hun diensten zo aan te passen dat een lager betrouwbaarheidsniveau ook verantwoord kan worden gehanteerd, bijvoorbeeld door verderop in het proces mitigerende maatregelen te nemen.

Een goed voorbeeld van een handelswijze waar is gekozen voor een dergelijke oplossing met lage drempelwerking zijn de diensten van de Sociale Verzekeringsbank (SVB). Daar heeft men er bewust voor gekozen om de diensten zo vorm te geven dat volstaan kan worden met DigiD Basis. De consequentie daarvan is wel dat sommige zaken niet online kunnen worden afgehandeld of dat er een bevestigingsbrief wordt gestuurd na afronding van de online transactie.

8.4.2 Gebruikersperspectief

Vanuit het perspectief van de gebruiker, zij het een burger, zij het een medewerker van een bedrijf,kan eenmalig inloggen tot verwarring leiden. Wanneer toegang is verkregen tot verschillende diensten en eenmalig uitloggen niet beschikbaar is, worden sessies niet direct beëindigd. Het kan hierdoor onduidelijk zijn welke sessies op enig moment nog open staan, waardoor extra beveiligingsrisico's worden geïntroduceerd.

Een dienstaanbieder die gebruik maakt van een authenticatie uit een federatie, kan stilstaan bij de effecten van eenmalig inloggen (en uitloggen) voor de gebruiker en hier de nodige actie aan verbinden. Die actie vindt dan plaats op het niveau van de eigen organisatie, bijvoorbeeld door gebruikers in de eigen dienstverlening te wijzen op specifieke effecten van (en handelingsperspectieven bij) het gebruik van éénmalig inloggen. Ook kan de dienstaanbieder wensen en eisen formuleren voor de federatie om daarmee de gebruiker beter en veiliger te kunnen bedienen.



Bijlage 1 Relevante wet- en regelgeving

1 Algemene wet bestuursrecht

Met de Wet elektronisch bestuurlijk verkeer (Webv) is een afdeling 2.3 toegevoegd aan de Algemene wet bestuursrecht (Awb).[13] 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.[14]

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 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. Dat aspect is uiteraard belangrijk voor het classificeren van het vereiste betrouwbaarheidsniveau;
  - vereisten van ondertekening;
  - tijdstippen van verzending en ontvangst bij elektronisch verkeer

Hieronder worden deze hoofdlijnen nader uitgewerkt.

Artikel 2:13 Awb
Dit artikel bepaalt dat in het verkeer tussen burger en bestuursorgaan

[13] Stb. 2004, 214, in werking getreden op 1 juli 2004 (Stb. 260).
[14] Stb. 2010, 173, in werking getreden op 1 juli 2010 (Stb. 207).

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 de 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, terinzagelegggingen 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 forma betrouwbaarheid 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'.[15]

De wetgever beoogt met de eis van betrouwbaarheid en vertrouwelijkheid uitdrukking te geven aan de zogenaamde algemene beginselen van

[15] Kamerstukken II 2001/02, 28 483, nr. 3, p. 16-17.

behoorlijk IT-gebruik.[16] Hieronder worden verstaan de beginselen van authenticiteit, integriteit, onweerlegbaarheid, transparantie, beschikbaarheid, flexibiliteiten 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 een 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.

Ook de STORK-niveaus passen binnen deze middelste optie. Daarmee vormen de STORK-niveaus en de in Nederland beschikbare middelen voor authenticatie een adequate invulling van de open norm uit de Awb.
In onderstaande figuur wordt deze relatie geïllustreerd

Figuur 4 Relatie open norm Awb en betrouwbaarheidsniveaus STORK

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

[16] Kamerstukken II 2001/02, 28 483, nr. 3, p. 15. Zie ook H. Franken, Kanttekeningen bij het automatiseren van beschikkingen, in: Beschikken en automatiseren, VAR-reeks 110, Alpen aan den Rijn 1993.

waarvoor het wordt gebruikt, bepalend zijn voor de mate van betrouwbaarheid en vertrouwelijkheid die vereist is.

Hier dient steeds een vergelijking gemaakt te worden met het conventionele, papieren verkeer: de mate van betrouwbaarheid en vertrouwelijkheid dient even groot te zijn als in het conventionele verkeer. Aan de verlening van een vergunning dienen bijvoorbeeld hogere eisen te worden gesteld dan aan het verstrekken van algemene informatie.[17]

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. In bijlage 3 zijn voorbeelden gegeven van de wijze waarop vereisten in het conventionele (papieren) verkeer zich vertalen naar de elektronische situatie.

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 zogenaamde openstelling van de elektronische weg door het bestuursorgaan kan zowel geschieden in een algemene regeling als in een bericht aan één of meer geadresseerden. Concrete voorbeelden zijn opgenomen in bijlage 2.

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.[18]

[17] Kamerstukken II 2001/02, 28 483, nr. 3, p. 17.
[18] Kamerstukken II 2001/02, 26 483, nr. 3, p. 13.

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
Dit artikel bepaalt op welke wijze voldaan wordt aan een vereiste van ondertekening van een elektronisch bericht. Hierbij worden de artikelen 15a en 15b van Boek 3 van het Burgerlijk Wetboek grotendeels van overeenkomstige toepassing verklaard. Deze worden in het onderstaande besproken. De mogelijkheid bestaat om die bepalingen bij wettelijk voorschrift aan te vullen.

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 op de situatie dat de betrokkenen daadwerkelijk gebruik maken van hetzelfde systeem (dezelfde fysieke servers). Een voorbeeld is het elektronisch verzenden van stukken tussen het College van BW 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.

In de jurisprudentie zijn deze bepalingen nader ingevuld. In bijlage 2 zijn enkele praktijksituaties rond verzending en ontvangst beschreven, waarbij ook wordt ingegaan op de situatie dat het bestuursorgaan gebruik maakt van een elders opstelde, generieke voorziening voor berichtenverkeer.

2 Wet elektronische handtekeningen (Weh)

Met de Wet elektronische handtekeningen[19] (hierna: Weh) is de Richtlijn 1999/93/EG over een gemeenschappelijk kader voor elektronische handtekeningen geïmplementeerd.[20] De Weh voegt de artikelen 15a en 15b toe aan Boek 3 van het Burgerlijk Wetboek. Deze regelen de rechtsgevolgen van elektronische handtekeningen en de vereisten waaraan voldaan moet zijn, willen die rechtsgevolgen intreden. Daarnaast wordt de aansprakelijkheid van certificatiedienstverleners, het toezicht op certificatiedienstverleners en de vrijwillige accreditatie van certificatiedienstverleners geregeld. De Wet elektronisch bestuurlijk verkeer verklaart zoals gezegd delen van de Weh van overeenkomstige toepassing.

Artikel 15a
Artikel 15a begint met een gelijkstellingsbepaling (eerste lid): een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische

[19] Stb. 2003, 199.
[20] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, PbEG 19-1-2000, L13/12. De bijlagen van de richtlijn zijn geïmplementeerd in het Besluit elektronische handtekeningen, Besluit van 8 mei 2003, Stb. 2003, 200.

gegevens werden gebruikt en op alle overige omstandigheden van het geval. Om te kunnen bepalen of een elektronische handtekening voldoende betrouwbaar is voor het doel waarvoor deze gebruikt wordt, is het van belang om inzicht te hebben in de definitie van en de eisen die aan een elektronische handtekening worden gesteld en aan de functies van ondertekening van een bepaald stuk. In het onderstaande wordt hierop achtereenvolgens ingegaan.

Eisen aan de elektronische handtekening
Het vierde lid van artikel 15a bevat de definitie van elektronische handtekening. Dit is een handtekening die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie. Onder authentificatie wordt verstaan dat de handtekening dient om vast te stellen dat het bericht daadwerkelijk afkomstig is van de ondertekenaar en dat de ondertekenaar is wie hij zegt te zijn.[21]

Deze definitie is behoorlijk ruim. Ook een ingescande handgeschreven handtekening kan hiermee als elektronische handtekening worden aangemerkt.[22] Als zo'n ingescande handtekening bijvoorbeeld onderaan een e-mail bericht geplaatst zou worden, zou deze 'vastgehecht' zijn aan andere elektronische gegevens, namelijk het e-mailbericht. Bovendien wordt de handtekening dan gebruikt voor authentificatie. De definitie is zelfs zo ruim dat ook het plaatsen van een naam onder een e-mailbericht als elektronische handtekening kan worden aangemerkt. De vermelding van de naam dient immers ter authentificatie. In deze gevallen wordt gesproken van een gewone elektronische handtekening. Dit wil niet zeggen dat een ingescande of getypte 'handtekening' in alle gevallen dezelfde status heeft als een 'natte' handtekening op een papieren drager. De methode van authentificatie (het typen van een naam of inscannen van een handtekening) zal niet voor elk doel voldoende betrouwbaar zijn. De naam zou immers evengoed door een ander persoon ingetypt of gescand kunnen zijn. Daarom stelt artikel 15a, tweede lid, een aantal eisen die gelden als men een elektronische handtekening gelijk wil kunnen stellen aan een conventionele handtekening.

Dit tweede lid bevat een regel op grond waarvan een methode voor authentificatie wordt vermoed voldoende betrouwbaar te zijn. Daarvan is sprake indien de gebruikte elektronische handtekening aan een aantal eisen voldoet, waardoor deze als geavanceerde elektronische handtekening kan worden aangemerkt. Die eisen zijn:
- zij is op unieke wijze aan de ondertekenaar verbonden;
- zij maakt het mogelijk de ondertekenaar te identificeren;
- zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
- zij is op zodanige wijze verbonden aan het elektronisch bestand waarop zij betrekking heeft, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

Deze eisen zijn bewust techniekonafhankelijk geformuleerd; een geavanceerde elektronische handtekening kan dus met alle technieken worden aangemaakt die aan deze eisen voldoen. Indien de elektronische handtekening behalve aan de bovenstaande eisen, ook nog aan de volgende vereist voldoet, dan is sprake van een gekwalificeerde elektronische handtekening:
- zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, Telecommunicatiewet;
- zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, Telecommunicatiewet.

Het vijfde lid van artikel 15a geeft een definitie van ondertekenaar. Dit is degene die een middel voor het aanmaken van elektronische handtekeningen gebruikt als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet. Het zesde lid bepaalt ten slotte dat partijen een hoger of lager betrouwbaarheidsniveau dan dat van het tweede lid kunnen overeenkomen voor juridische gelijkstelling van een elektronische handtekening aan een handgeschreven handtekening.

Functie van ondertekening
Een ondertekening heeft in het algemeen twee functies:
a Authenticatie: het kunnen vaststellen dat een stuk van een bepaalde persoon afkomstig is.[23]
b Wilsuiting: het uitdrukken van instemming met de in een stuk opgenomen gegevens of verklaringen.

Vaak wordt aan ondertekening ook nog een derde functie toegedicht, namelijk bescherming tegen overijling bij het verrichten van een rechtshandeling met (mogelijk) verstrekkende gevolgen. Deze functie ligt in het verlengde van de functie van wilsuiting. De vraag is of een enkel ondertekeningsvereiste deze bescherming kan bieden. In het algemeen zullen

[21] Kamerstukken II 2001/02, 28 483, nr. 3, p. 15.
[22] Kamerstukken II 2000/01, 27 743, nr. 3, p. 2.
[23] Voorbeeld hiervan is de ondertekening van de belastingaangifte, zie Kamerstukken II 1994/95, 24 341, nr. 3, blz. 2-3.

daarvoor meer en andere vormvereisten nodig zijn, zoals betrokkenheid van een notaris (die de stukken voorleest en expliciet vraagt of betrokkenen ze begrepen hebben), een expliciete bedenktijd of het apart expliciet kennisnemen van of bevestigen van een verklaring.[24]

Artikel 15b
Dit artikel bevat bepalingen over de aansprakelijkheid en accreditatie van en het toezicht op certificatiedienstverleners. Deze worden hier niet inhoudelijk besproken.

3 Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (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, strafrechtelijke persoonsgegevens. Voor deze persoonsgegevens geldt in beginsel een verbod op verwerking.

[24] Zie hierover ook R. van Esch, Electronic data interchange (EDI) en het vermogensrecht, Deventer 1999, pag. 139-141.

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 het CBP 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.

Het College bescherming persoonsgegevens (Cbp) heeft recent Richtsnoeren voor de Beveiliging van Persoonsgegevens uitgegeven[25], dat het uit 2001 daterende normerende document, Richtlijnen voor de beveiliging van persoonsgegevens (Achtergrondstudies en Verkenningen nr. 23 (A&V 23)[26], vervangt. Het in A&V 23 gehanteerde begrip 'risicoklasse' met de daaraan gekoppelde maatregelen is daarmee te komen vervallen. In plaats daarvan geven de huidige richtsnoeren een meer procesgerichte benadering, waarin het formuleren van betrouwbaarheidseisen en het uitvoeren van een risicoanalyse centraal staan.

Het zuiver procesmatig benaderen is echter niet in lijn met de opzet van deze handreiking, waarin we juist een in de praktijk standaardiserend effect trachten te bewerkstellingen. In hoofdstuk 5 van deze handreiking is daarom nog steeds een vertaling gemaakt van de voor privacy relevante criteria naar een indeling in klassen en bijbehorende betrouwbaarheidsniveaus.

Waar in de A&V 23 er drie criteria waren voor het indelen in risicoklassen, te weten de aard van de gegevens alsmede de omvang en de complexiteit van de verwerking, vinden we die laatste niet meer zo expliciet terug. In de richtsnoeren worden de gevolgen voor het individu voorop gezet bij het formuleren van de betrouwbaarheidseisen (pg 18): "Voor het vaststellen van de betrouwbaarheidseisen zijn, vanuit de beveiliging van persoonsgegevens en het belang van de betrokkenen bezien, de risico's voor één, individuele betrokkene maatgevend. De schade die betrokkenen ondervinden van verlies of onrechtmatige verwerking van hun persoonsgegevens wordt

[25] Zie http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf
[26] Blarkom, G.W. van, Borking, drs. J.J., Beveiliging van persoonsgegevens, Registratiekamer, april 2001, Achtergrondstudies en Verkenningen 23, http://www.cbpweb.nl/Pages/av_23_Beveiliging.aspx.

bepaald door de aard van de gegevens en de aard van de verwerking en niet door het aantal anderen van wie de persoonsgegevens eveneens verloren zijn gegaan of onrechtmatig zijn." Overigens is te beargumenteren dat het vanuit maatschappelijke optiek en daarmee ook vanuit de optiek van de dienstaanbieder wel degelijk relevant of er een enkel individu schade ondervindt of een grote groot mensen. Dit heeft in het classificatiemodel van hoofdstuk 5 dan ook een plek gekregen.

Het hierboven aangehaalde fragment duidt op criteria *aard van gegevens* en *aard van verwerking.* De *aard van de verwerking* wordt even verderop in de richtsnoeren nader geduid, zij het niet uitputtend:

- Hoeveelheid verwerkte persoonsgegevens *per persoon*.
  Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer. Bijvoorbeeld: het uitlekken van een compleet medisch dossier leidt over het algemeen tot een grotere inbreuk dan het uitlekken van een herhaalrecept.
- 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. Bijvoorbeeld: als een organisatie financiële gegevens gebruikt om iemands kredietwaardigheid te bepalen zijn de gevolgen ingrijpender dan bij gebruik van dezelfde gegevens voor marketingdoeleinden."

Wederom zien we dat de hoeveelheid gegevens geduid wordt als de hoeveelheid gegevens per persoon.

Het hoofdcriterium is en blijft echter de aard van de gegevens. De richtsnoeren geven enkele voorbeelden van persoonsgegevens, waarvan verlies, diefstal of onrechtmatige verwerking ernstige gevolgen kunnen hebben:

- Bijzondere persoonsgegevens in de zin van de wet;
- Gegevens over de financiële of economische situatie van de persoon;
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van betrokkene;
- Gegevens die betrekking hebben op mensen uit kwetsbare groepen;
- Gebruikersnamen, wachtwoorden etc.;
- Gegevens die misbruikt kunnen worden voor identiteitsfraude.

In hoofdstuk 5 van deze handreiking worden deze criteria gehanteerd om tot een afbeelding op betrouwbaarheidsniveaus te komen.

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 back office kunnen ertoe leiden dat aan de 'poort' met een lager betrouwbaarheidsniveau kan worden volstaan. In hoofdstuk 2 van de handreiking is nader ingegaan op de afbakening tussen informatiebeveiligingsbeleid (VIR, VIR-BI) en elektronisch verkeer (Awb).

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 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 27002 richtlijn, 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 o.a. aanbestedingsinformatie en kan als analogie worden gezien met wat een bedrijf als ernstig concurrentie- of economisch gevoelig beschouwt.

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 oa. 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.[27] Voor het gebruik buiten de kring van overheidsorganen blijft een specifieke wettelijke grondslag nodig.
Ten aanzien van BSN geldt een vergewisplicht. Dat betekent dat de organisatie die het nummer wil gebruiken, dient vast te stellen of het nummer daadwerkelijk behoort bij de persoon die het heeft opgegeven. De vergewisplicht wordt ondersteund door het burgerservicenummerstelsel.

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.[28] 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

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

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

[28] Ontleend aan memorie van toelichting Wabb.

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.[29]

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.[30]

Voor de ondertekening van elektronische onderhandse akten wordt in het algemeen een elektronische handtekening als bedoeld in artikel 3:15a BW 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 BW over de totstandkoming van overeenkomsten en artikel 1021 Rv over de arbitrageovereenkomst.

[29] Stb. 2006, 475, laatstelijk gewijzigd in Stb. 2006, 706.

[30] De vraag is of deze reden geheel valide is. Door gebruik van bepaalde bestandsformaten is ongewijzigde reproductie wel degelijk te waarborgen, ongeacht het gebruikte hulpmiddel.

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

Artikel 156a Rv bepaalt alleen onder welke voorwaarden onderhandse akten op een andere wijze dan schriftelijk kunnen worden opgemaakt.
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 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 geadresseerde 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 ed.) 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).
- Een chat met een ambtenaar (vergelijkbaar met 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 (bv. 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'.

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 (bv. bezwaarschriften, aanvragen) per fax of e-mail. Ook bij verzending via machine-machineverkeer (zie hoofdstuk 2) is artikel 2:17 echter relevant en geldt dat de verzender het risico draagt voor elektronische verzending. Bij machine-machineverkeer 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 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.[31] 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, etc.
- Een openstellingsbesluit, zoals de Belastingdienst destijds heeft vastgesteld.[32]

4 Belemmeringen voor elektronisch verkeer

a. Uitsluiten van elektronisch verkeer bij wettelijk voorschrift

Het uitsluiten van elektronisch verkeer bij wettelijk voorschrift (artikel 2:13, tweede lid, onderdeel a, Awb) lijkt een expliciet 'verbod' op elektronische

[31] Kamerstukken II 2001/02, 28 483, nr. 3, p. 13.
[32] Openstelling elektronische bestuurlijk verkeer met de belastingdienst, 27 april 2005, nr. CPP 2004/2807M, Stcrt. 87, p. 12.

aanleveren van berichten of stukken te vergen. De bestuursrechter heeft bijvoorbeeld bepaald dat het in een regeling voorschrijven van 'gebruikmaking van het origineel van een ondertekend formulier' geen expliciete uitsluiting van elektronisch verkeer inhoudt.[33] In het verlengde daarvan zal waarschijnlijk ook een definitie van 'schriftelijk' die zich uitdrukkelijk beperkt tot 'schrifttekens op papier' niet als expliciete uitsluiting van elektronisch verkeer gelden.[34]

De MvT bij de Wet elektronisch bestuurlijk verkeer onderstreept dit: "Vormvoorschriften staan dus niet zonder meer aan elektronisch verkeer in de weg." Als voorbeeld noemt de wetgever de vereisten van een brief of publicatie in de Staatscourant[35]; in beide gevallen blijft ook de elektronische weg openstaan.

Vormvoorschriften in wet- en regelgeving die elektronisch verkeer belemmeren (artikel 2:13, tweede lid, onderdeel b, Awb)

Formulering wetstekst	Voorbeeld	Belemmering
In persoon	Wet GBA, artikel 65, eerste lid: "zijn verblijf in persoon te melden ..." Zie ook art. 71 en artikel 74, tweede lid. Boek 1 BW, art. 43, derde lid, over ondertrouw. Kentekenregeling art. 25a, tweede lid. Waterschapsreglement art. 50.2, eerste lid.	De eis "in persoon" te verschijnen is een voorbeeld van een vormvoorschrift dat afhandeling op basis van een elektronisch bericht verhindert, conform artikel 2:13, tweede lid, onderdeel b, Awb.
Waarmerken	Regeling LNV subsidies, Bijlage bij artikel 1:14e	Dit gebruik in de papieren wereld is vergelijkbaar met de cryptografische koppeling van een elektronische handtekening aan hetgeen getekend wordt op basis van een hash.
Verifieert identiteit van de persoon door middel van visuele controle	Besluit elektronische handtekening art. 2, eerste lid, onderdeel g	De verplichtingen aangaande de uitgifte van een gekwalificeerd certificaat (STORK niveau 4), waarbij iemand in persoon (face tot face) moet worden geïdentificeerd zijn een evident voorbeeld van een vormvereiste dat toepassing van een elektronisch proces verhindert.

[33] CBB 4 juni 2008, LJN BD4039 (Aanvraag MEP-subsidie).
[34] Zie artikel 1 van de Pensioenwet. Overigens is de MvT bij deze wet ook niet geheel eenduidig in de mate waarin deze definitie aan elektronisch verstrekken van informatie in de weg staat.
[35] Dit voorbeeld is overigens inmiddels achterhaald, nu de Staatscourant sinds 2009 niet meer op papier verschijnt.

b. Vormvoorschriften die zich mogelijk tegen elektronisch verkeer verzetten

5 Analogieën voor elektronisch verkeer

Voor de hierna genoemde formuleringen in wetsteksten kunnen elektronische analogieën gegeven worden. Op grond daarvan kan geconcludeerd worden dat deze formuleringen niet kunnen gelden als "vormvoorschriften die zich tegen elektronische verzending verzetten" in de zin van artikel 2:13, tweede lid, Awb.

6 Verplichting om berichten elektronisch te verzenden

Voorbeelden hiervan zijn:

- De verplichte elektronische belastingaangifte voor ondernemers (artikelen 8, tweede lid, Algemene wet rijksbelastingen en artikel 20 Uitvoeringsregeling Algemene wet inzake rijksbelastingen 1994).
- De aanvraag voor een omgevingsvergunning voor een onderneming (artikel 2.8 van de Wet algemene bepalingen omgevingsrecht en artikel 4.1, tweede lid, Besluit omgevingsrecht).

Van volledig verplicht elektronisch verkeer voor burgers (met uitsluiting van het papieren kanaal) bestaan nog geen voorbeelden.

7 Ondertekening van berichten

Indien ondertekening van een bericht is vereist, wordt daarvoor ingevolge artikel 2:16 Awb een elektronische handtekening gebruikt. Op de volgende pagina is een overzicht opgenomen van typen elektronische handtekeningen ingevolge de Wet elektronische handtekeningen (artikel 15a, Boek 3 BW).

Type elektronische handtekening	Rechtsgevolgen	Technische betrouwbaarheid in relatie tot conventionele technieken
Gewoon	Alleen geldig als ondertekening indien dat tussen partijen is overeengekomen of indien (voor bestuurlijk verkeer) de aard van het bericht geen hogere betrouwbaarheid vereist en dit als zodanig door partijen geaccepteerd wordt.	Kopie van ondertekend document, print van document met gescande handtekening, elektronisch bestand die een gescande handtekening bevat.
Geavanceerd	Alleen indien er duidelijke gronden zijn anders dan de in BW boek 3 art 15a derde lid uitgesloten gronden om deze handtekening onvoldoende betrouwbaar te vinden zijn de rechtsgevolgen niet gelijk aan de handgeschreven handtekening.	In de papieren situatie wordt een ondertekening met pen op papier met eventueel paraaf op iedere pagina gehanteerd, waarbij de “vasthechting” versterkt kan worden door de handtekening deels over de gedrukte tekst te plaatsen.
Gekwalificeerd	Rechtsgevolgen zijn gelijk aan handgeschreven handtekening voor dezelfde situatie.	Idem als boven met extra waarborgen zoals een notaris die een handtekening valideert tegen het reisdocument en de GBA gegevens.

Voorts kan een indicatief overzicht worden gegeven van wettelijke formuleringen voor ondertekening van een bericht en de functies van de handtekening die deze formuleringen weergeven.

Wettelijke formulering	functie van de handtekening	soort elektronische handtekening
… wordt ondertekend …	identificatie/authenticatie van de zender	gewone of geavanceerde
… verklaart …	wilsuiting	geavanceerde of gekwalificeerde
… naar waarheid ingevuld… … duidelijk, stellig en zonder voorbehoud…	authenticatie van de inhoud van een bericht (juistheid van de gegevens)	geavanceerde of gekwalificeerde

Bijlage 3 Begrippenkader

In deze bijlage is een aantal sleutelbegrippen in de handreiking gedefinieerd. De begrippen zijn groepsgewijs geordend. Voor een uitgebreide lijst van begrippen op het terrein van identificatie en authenticatie wordt verwezen naar de begrippenlijst die in het kader van het eID-stelsel nl is ontwikkeld.

Begrip	Toelichting
Persoon	Een natuurlijke- of niet-natuurlijke persoon. Een persoon is drager van rechten en plichten. Een nbiet-natuurlijke persoon kan al dan niet rechtspersoonlijkheid hebben.
Handelende partij	Een handelende partij is een persoon (natuurlijk of niet-natuurlijk) die handelingen verricht, dan wel verantwoordelijkheid neemt voor de handelingen ten behoeve van het tot stand komen van een elektronische transactie met een dienstaanbieder, als onderdeel van een dienst. Van een handelende partij moet de bevoegdheid worden vastgesteld. Deze bevoegdheid kan gebaseerd zijn op basis van de volgende invullingen: • De handelende partij handelt voor zichzelf als de belanghebbende. Een belanghebbende is degene wiens belang rechtstreeks bij de dienst is betrokken. In deze situatie is wel relevant of de handelende partij voor de gevraagde transactie handelingsbekwaam is. • De handelende persoon handelt niet voor zichzelf, maar is bevoegd vanwege de uitoefening van een erkende persoonsrol. • De handelende persoon handelt niet voor zichzelf, maar is specifiek voor die belanghebbende bevoegd vanwege het bestaan van een wettelijke vertegenwoordiging (zoals bestuurders van rechtspersonen, eigenaren van eenmans¬zaken en curatoren) of vanwege een door de belanghebbende verstrekte volmacht (een privaatrechtelijke volmacht op basis van artikel 3:60 BW of een bestuursrechtelijke machtiging op basis van artikel 2:1 Awb).
Dienstaanbieder	Een dienstaanbieder is een overheidsorganisatie en/of bestuursorgaan die kenbaar heeft gemaakt dat zij elektronisch bereikbaar is voor burgers en bedrijven, zodat zij als handelende partij in staat wordt gesteld om elektronische transacties in het kader van een dienst te kunnen uitvoeren.
Belanghebbende	Degene wiens belang rechtstreeks bij een besluit is betrokken (artikel 1:2 Awb). De belanghebbende is dus de persoon op wie de rechtsgevolgen van een overheidsdienst direct betrekking hebben. De belanghebbende kan een natuurlijke persoon of een niet-natuurlijke persoon zijn.

Begrip	Toelichting
Dienst	Een dienst is in dit verband een samenstel van elektronische transacties, gericht op: • het tot stand komen van een rechtsbetrekking (het nemen van een besluit of een overeenkomst). • het leveren van een product of besluit). • het beantwoorden van een informatievraag. De dienst wordt gedefinieerd en aangeboden door een dienstaanbieder, die bepaalt welke eisen worden gesteld om de dienst te mogen afnemen. Deze eisen zijn: a. Het minimale STORK-betrouwbaarheidsniveau waarmee de handelende partij moet worden geauthenticeerd. b. Met welke mate van betrouwbaarheid de handelende partij wordt gebonden aan de inhoud van de transactie. c. Welke soort identiteit is toegestaan (bijvoorbeeld alleen een RSIN-nummer of ook een KvK-nummer). d. Of het voor de dienst is toegestaan dat de handelende persoon een niet-natuurlijke persoon mag zijn.
Authenticatie	De controle (het staven) van de (een) geclaimde identiteit van een persoon aan de hand van zijn authenticatiemiddel. Authenticatie is een proces dat wordt uitgevoerd door een authenticatiedienst.
Authenticatiemiddel	Een combinatie van bezit, kennis en eigenschappen, die persoonsgebonden is. Aan de hand van de verificatie van bezit, kennis en eigenschappen kan de geclaimde identiteit op een bepaald betrouwbaarheidsniveau worden gestaafd.
Betrouwbaarheidsniveau	Een niveau van zekerheid dat wordt geboden door vertrouwensdiensten in hun processen voor authenticatie, registreren van beheren van machtigingen et cetera. Het betrouwbaarheidsniveau wordt gecommuniceerd in de verklaringen die een vertrouwensdienst produceert. Het begrip betrouwbaarheidsniveau moet worden onderscheiden van het beveiligingsniveau. Dit betreft het niveau van alle beveiligingsmaatregelen die nodig zijn om een dienst van een passende beveiliging te voorzien. Dat is dus een wezenlijk breder bereik. Ook moet dit begrip worden onderscheiden van het zekerheidsniveau (assurance level) dat voor vertrouwensdiensten aan de orde is. Dat betreft de zekerheid waarmee is vastgesteld dat bepaalde beveiligingsmaatregelen of beveiligingsfunctionaliteit (correct) is geïmplementeerd. Hierop zijn bijvoorbeeld informatiebeveiligingscertificaties van ISO 27001 gericht.

Begrip	Toelichting
Vertrouwensdienst	In dit kader volgen we de concept EU verordening over eID: Iedere elektronische dienst bestaande uit het aanmaken, verifiëren, valideren, hanteren en bewaren van elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, elektronische bezorgingsdiensten, website-authenticatie en elektronische certificaten, met inbegrip van certificaten voor elektronische handtekeningen en voor elektronische zegels. In het verband van deze handreiking gaat het dan om diensten als: • Uitgifte en beheer van authenticatiemiddelen • Authenticatiediensten • Attributendiensten • Machtigingendiensten • Ondertekendiensten • Makelaardiensten
Verklaring	Een door een vertrouwensdienst gewaarmerkt bericht omtrent de identiteit van een persoon, zijn attributen, zijn bevoegdheden inclusief machtigingen, alsmede ondertekening van transacties of documenten. Tenminste kunnen de volgende verklaringen onderkend worden: • Identiteitsverklaringen • Attribuutverklaringen • Bevoegdheidsverklaringen • Associatieverklaringen
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.

Dit document verschijnt onder de licentie Creative Commons

Naamsvermelding 3.0 Nederland
www.creativecommons.org/licenses/by/3.0/n

Bij hergebruik graag vermelden:
Forum Standaardisatie: Handreiking betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten, versie 2, augustus 2013

Deze brochure is een uitgave van:

Forum Standaardisatie
Augustus 2013