Handreiking

Betrouwbaarheidsniveaus authenticatie voor elektronische overheidsdiensten

versie 1.0

Colofon

Auteur
Logius
Project

Organisatie
Logius
Titel
Handreiking betrouwbaarheidsniveaus voor elektronische overheidsdiensten

Status
Concept
Datum
3 feb 2011

Versie
1.0

Historie

Datum	Versie	Wijziging	Status	Auteurs
15-11-10	0.1	Concept outline	Concept	M. Stoelinga
22-11-10	0.2	Outline	Concept	M. Lokin M. Stoelinga T. Hooghiemstra
27-1-11	0.3	Concept	Concept	Idem
31-1-11	0.4	Concept	Concept	Idem
1-2-11	0.5b	Concept	Concept	Idem
3-2-11	0.6	Concept	Concept	M. Lokin
5-2-11	0.6b	Workshop 1	Concept	M. Stoelinga
25-2-11	0.7	Commentaren verwerkt	Concept	M. Lokin M. Stoelinga
9-3-11	0.8	Verdere commentaren en huiswerk	Concept	M. Stoelinga
13-05-11	0.9	Commentaren bijeenkomst 10 mei	Concept	M. Lokin
23-05-11	0.91	Toezending aan Forum	Concept	M. Lokin
21-06-11	0.92	Resterende commentaren en input Forum 14 juni 2011	Concept	M. Lokin
30-08-11	0.95	Hoofdstuk 3 en bijlage 3 opgelijnd. Eén methode van gemaakt.	Concept	R. vd. Assem
19-9-11	0.96	Bijlage 3 opgeheven, alle methode in hoofdstuk 3.	Concept	R. vd Assem
19-9-11	1.0	Eindredactie	Definitief	M. Lokin

Distributielijst

Datum	Distributie	Versie
5-2-2011	Deelnemers werkgroep	0.6b
25-2-2011	Deelnemers werkgroep	0.7d
4-5-2011	Deelnemers werkgroep	0.8
31-8-11	Deelnemers werkgroep	0.95

Inhoudsopgave

Managementsamenvatting

Inleiding

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. Een essentiële randvoorwaarde daarbij is de beschikbaarheid van adequate middelen voor identificatie, authenticatie en autorisatie. Daarmee kunnen burgers en bedrijven er zeker van zijn dat hun (vertrouwelijke) gegevens op een betrouwbare manier bij de overheid terecht komen en kunnen worden opgehaald. De overheid kan er op haar beurt zeker van zijn dat zij met de juiste persoon te maken heeft.

Om deze middelen voor alle belanghebbenden betaalbaar te houden en een voor gebruikers onhandige digitale sleutelbos te voorkomen zijn zo generiek mogelijk inzetbare middelen voor identificatie en authenticatie ontwikkeld. Voorbeelden daarvan zijn DigiD, PKIoverheid en het afsprakenstelsel eHerkenning. Met DigiD Machtigen is een begin gemaakt met ontwikkeling van autorisatievoorzieningen, gericht op machtigingssituaties.
Op Europees niveau wordt gewerkt aan standaardisatie van betrouwbaarheidsniveaus voor authenticatie bij e-dienstverlening in het STORK-project.[i] Dit heeft tot doel om identificatie- en authenticatiemiddelen ook voor grensoverschrijdend dienstenverkeer bruikbaar te maken en houden.

In Nederland geldt tot nu toe een open norm ten aanzien van het betrouwbaarheidsniveau van e-overheidsdiensten, neergelegd in de Algemene wet bestuursrecht (Awb). De Awb vereist dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' geschiedt.
Vanuit het Besluit voorschrift informatiebeveiliging rijksdienst is daarnaast gesteld dat het betreffende lijnmanagement de betrouwbaarheidseisen dient vast te stellen aan de hand van een risicoafweging. Het lijnmanagement dient vervolgens er op toe te zien dat er maatregelen worden getroffen die voortvloeien uit die betrouwbaarheidseisen. Ook dit is dus een open norm.
Met de toename van e-diensten groeit ook de behoefte om deze open norm nader in te kleuren. Het is belangrijk dat overheidsorganisaties in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid vereisen (en borgen) voor hun elektronische diensten. Het doet de transparantie, toegankelijkheid en geloofwaardigheid van de overheid geen goed als hierin geen eenduidige lijn wordt gehanteerd. Met het oog op het zorgvuldigheidsbeginsel is het 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 inkleuring, op basis van de nationale geldende (wettelijke) regels en het STORK-kader. Hij bevat daartoe een 'menukaart' die op basis van (wettelijke) criteria een generieke koppeling van (soorten) diensten en betrouwbaarheidsniveaus bevat. Indien in voorkomend geval op basis van dit menu geen keuze gemaakt kan worden, bijvoorbeeld omdat de aard van de dienst of de omstandigheden wezenlijk anders liggen, dan ligt het voor de hand om een volwaardige risicoanalyse uit te voeren ter bepaling van het betrouwbaarheidsniveau.

Scope

De handreiking ziet op e-diensten van de overheid aan burgers en bedrijven, die deze afnemen via internet. Het gaat dus primair om diensten die via een online portaal worden aangeboden (bv. het Omgevingsloket online), of waarbij de afnemer in een lokale applicatie handelingen verricht en de uitkomst daarvan aan de overheidsorganisatie toestuurt (bv. de elektronische belastingaangifte voor particulieren).

De scope is vooralsnog niet gericht op machtigingen, het gaat dus voor diensten voor zichzelf als burger of voor het eigen bedrijf. Niet omdat machtigingen niet relevant zijn bij e-dienstverlening, maar omdat het domein van autorisatie nog (te) sterk in ontwikkeling is en inkadering zoals voorzien in deze handreiking nog niet mogelijk is. Ook verkeer tussen overheidsorganisaties onderling (bijvoorbeeld het raadplegen van basisregistraties, het uitwisselen van informatie die nodig is voor beoordeling van een vergunningaanvraag) is buiten het bereik van deze handreiking gelaten.
Hetzelfde geldt tot slot voor processen waarbij machine-machine communicatie plaatsvindt met de overheid.

De handreiking ziet in beginsel op het classificeren van het betrouwbaarheidsniveau voor een bepaalde dienst. Indien een overheidsorganisatie echter meer diensten aanbiedt met verschillende betrouwbaarheidsniveaus dan zal hij met gebruikmaking van de handreiking wel kunnen bepalen of voor deze diensten wellicht ook één niveau kan worden gehanteerd, en zo ja, welk niveau dat zou moeten zijn. Risicoverhogende en – verlagende factoren en de aard van de doelgroep van zijn diensten spelen daarbij een rol.

Status van de handreiking

De keuze voor een betrouwbaarheidsniveau voor een bepaalde elektronische dienst is en blijft de eigen verantwoordelijkheid van de overheidsorganisatie. Deze handreiking geeft de overheidsorganisatie 'gereedschap', gebaseerd op de algemene wettelijke kaders, om deze verantwoordelijkheid op een goede en eenduidige manier in te vullen. Verwacht mag worden dat van het gebruik een harmoniserende werking zal uitgaan. Een overheidsorganisatie kan echter voor een hoger of lager niveau kiezen, afhankelijk van de omstandigheden van het geval. Om die reden kunnen voor vergelijkbare diensten toch verschillende betrouwbaarheidsniveaus gelden. De meerwaarde van toepassing van de handreiking ligt dan in het feit dat een afwijking steeds helder te onderbouwen is.

Het ligt in de rede dat de uitvoeringsorganisaties de handreiking verankeren in hun uitvoeringsbeleid en dat zij de wijze waarop zij die hebben toegepast expliciet maken bij het vastleggen of communiceren van het voor hun diensten vereiste betrouwbaarheidsniveau.

Doelgroep

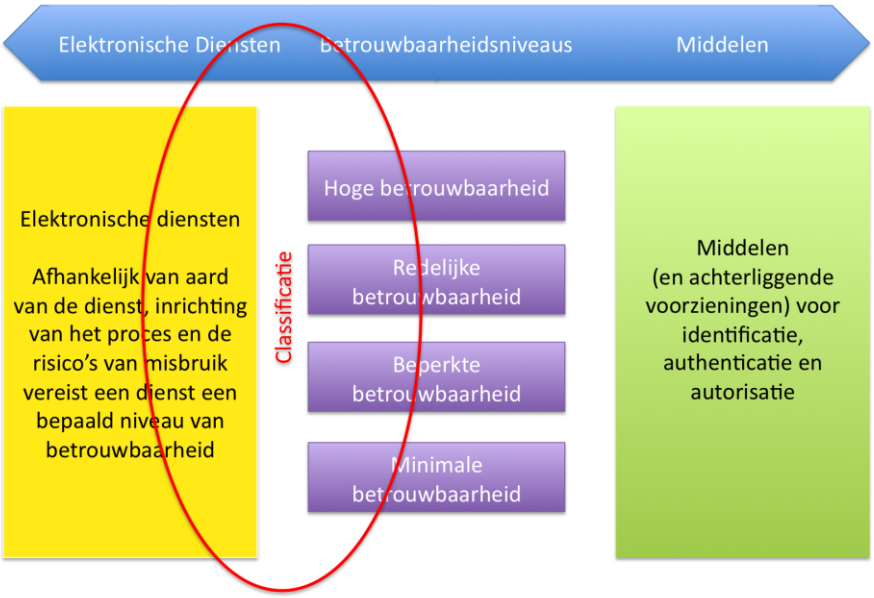
De handreiking bedient verschillende doelgroepen. Enerzijds biedt hij de basis voor de dialoog tussen beleidsmakers, (proces)architecten en informatiebeveiligers bij het inrichten van e-diensten en back office processen. Anderzijds biedt hij bestuurders inzicht in de afwegingen die aan het bepalen van betrouwbaarheidsniveaus ten grondslag hebben gelegen, zodat zij een weloverwogen keuze kunnen maken.

1 Inleiding

1.1 Uniforme betrouwbaarheidsniveaus voor diensten dragen bij aan e-overheid

Met het oog op het realiseren van lastenverlichting, betere dienstverlening en een efficiëntere overheid, zet de overheid in op grootschalig gebruik van elektronische diensten voor burgers en bedrijven. Een essentiële randvoorwaarde daarbij is de beschikbaarheid van adequate middelen voor identificatie, authenticatie en autorisatie. Daarmee kan de overheid er zeker van kan zijn dat zij met de juiste persoon te maken heeft. Burgers en bedrijven kunnen er op hun beurt zeker van zijn dat hun (vertrouwelijke) gegevens op een betrouwbare manier bij de overheid terecht komen of daar kunnen worden opgehaald.

Om deze middelen betaalbaar te houden en een voor gebruikers onhandige digitale sleutelbos te voorkomen wordt gewerkt aan zo generiek mogelijk inzetbare middelen voor identificatie, authenticatie en autorisatie. Voorbeelden daarvan zijn DigiD, PKIoverheid en het afsprakenstelsel eHerkenning. Met DigiD Machtigen en eHerkenning is tevens een begin gemaakt met ontwikkeling van autorisatievoorzieningen, gericht op machtigingssituaties.
Gezien de grote diversiteit aan elektronische diensten en de grote verschillen in behoeften van burgers en bedrijven bestaat er geen uniforme, "grootste gemene deler" oplossing voor situaties waarin authenticatie nodig is. Deze zou te duur en ingewikkeld zijn voor het ene geval of te slecht beveiligd voor het andere.
Een bredere selectie van middelen, ingedeeld op basis van betrouwbaarheidsniveaus, biedt wel een werkbare oplossing. Ieder van die betrouwbaarheidsniveaus geeft het resultaat weer van een afweging basis van objectiveerbare criteria en belangen. Deze aanpak leidt tot het classificeren van middelen op een bepaald niveau. Alle middelen van hetzelfde niveau worden daarmee in principe herbruikbaar voor soortgelijke situaties.



Figuur 1 Toepassingsgebied van de handreiking

De andere kant van de medaille is de noodzaak om voor een elektronische dienst te bepalen welk niveau van betrouwbaarheid deze vereist bij identificatie en authenticatie van de gebruiker. Het is belangrijk dat overheidsdiensten in vergelijkbare situaties hetzelfde niveau van betrouwbaarheid vereisen voor elektronische diensten. Het doet de transparantie, toegankelijkheid en geloofwaardigheid van de e-overheid namelijk geen goed als blijkt dat verschillende overheidsdienstverleners hierin tot verschillende conclusies komen, tenzij daar een duidelijke reden voor is. In het licht van het bestuursrechtelijke zorgvuldigheidsbeginsel is het van belang dat de afwegingen die zijn gemaakt bij het bepalen van een betrouwbaarheidsniveau helder en transparant zijn. Dat dient uiteindelijk ook de rechtszekerheid van burgers.

Tegen deze achtergrond is deze handreiking opgesteld, die overheidsdienstverleners helpt om voor hun diensten het juiste betrouwbaarheidsniveau te bepalen. Hij ziet derhalve op het met de rode cirkel in bovenstaande figuur gemarkeerde gebied.

Aan deze handreiking liggen algemene en specifieke wettelijke voorschriften voor elektronisch verkeer tussen overheid en burgers ten grondslag. Daarnaast haakt het kader aan op het raamwerk dat in Europees verband voor classificatie van identificatie en authenticatiemiddelen is ontwikkeld, STORK[1]. Dit raamwerk ondersteunt de betrouwbaarheid bij grensoverschrijdend gebruik van e-diensten. Ook in het afsprakenstelsel eHerkenning is aangesloten bij STORK.

Samengevat kan het doel van de handreiking worden omschreven als het leveren van een bijdrage aan een eenduidige, efficiënte en bewuste bepaling van het betrouwbaarheidsniveau van elektronische overheidsdiensten. Die bepaling moet een integraal onderdeel vormen van de ontwikkeling van elektronische diensten en niet gezien worden als een (puur technisch) sluitstuk daarvan.

1.2 Afbakening: wat is de scope van de handreiking?

Deze handreiking betreft diensten en processen die de overheid verleent aan of inzet jegens burgers en bedrijven. Het gaat hierbij om het domein dat op hoofdlijnen wordt gereguleerd door afdeling 2.3 van de Algemene wet bestuursrecht (Awb).[2]

Hierbij kunnen we in het algemeen de volgende situaties onderscheiden:
1. Diensten die afgenomen worden door iemand die voor zichzelf via internet een dienst afneemt en dus zelf degene is die de benodigde handelingen (website bezoeken, e-mail verzenden etc.) uitvoert.[3]
2. Diensten die afgenomen worden door iemand die zelf de benodigde handelingen uitvoert, maar dat doet namens een ander, waarbij deze ander een natuurlijke persoon of een niet-natuurlijke persoon is.
3. Diensten waarbij in dagelijkse gebruikssituatie systemen met elkaar communiceren zonder directe menselijke tussenkomst.

Deze handreiking ziet alleen op situatie 1. Mede op basis van ervaringen met het gebruik ervan zou doorontwikkeling naar de situaties 2 en 3 mogelijk zijn.

Het betreft daarnaast een handreiking voor het classificeren van het vereiste betrouwbaarheidsniveau voor een bepaalde dienst. Het kan voorkomen dat een dienstverlener meerdere diensten aanbiedt die een verschillend betrouwbaarheidsniveau vereisen. De vraag dient zich dan aan of deze diensten elk een middel op hun eigen betrouwbaarheidsniveau vragen, of dat voor bepaalde groepen diensten gekozen wordt voor één enkel betrouwbaarheidsniveau. Deze handreiking ziet er niet specifiek op toe hoe in dit soort situaties te handelen. Deze handreiking raakt wel aan risicoverhogende en – verlagende aspecten rond de dienstverlening en biedt daarmee een instrument om, binnen grenzen, het aantal betrouwbaarheidsniveaus dat een organisatie vraagt, te beperken.

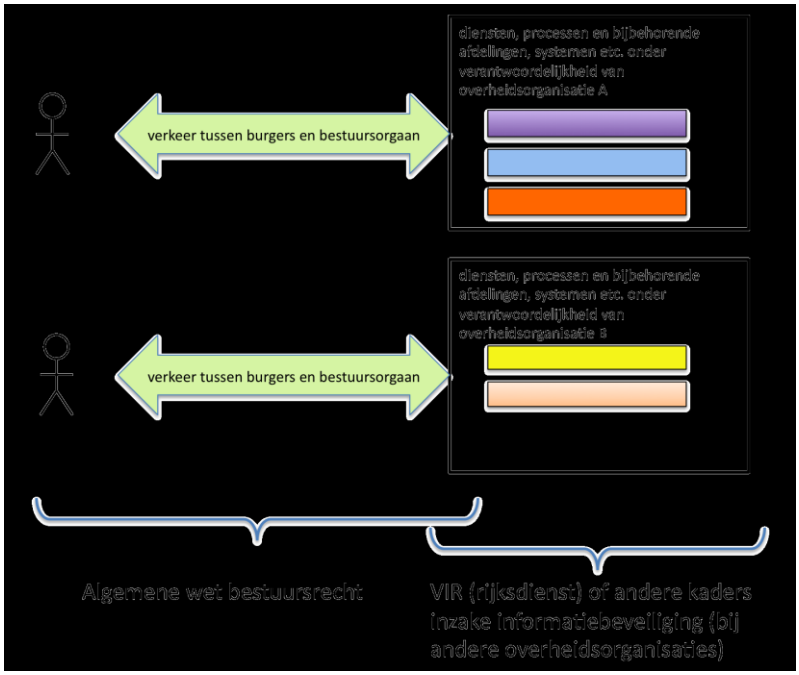
Buiten de scope van deze handreiking valt de 'retourstroom' vanuit de overheid (een reactie van het bestuursorgaan op een aanvraag of melding), hoewel identificatie en authenticatie (en autorisatie) daarbij uiteraard ook een rol spelen. Het moet duidelijk zijn dat de organisatie 'achter het loket' (of de medewerker daarvan) bevoegd is om bepaalde beslissingen te nemen en daartoe over informatie te beschikken. Ook de vertrouwelijkheid moet in dat geval geborgd zijn, zeker indien sprake is van uitwisseling van persoonsgegevens. Hetzelfde geldt bij uitwisseling van gegevens tussen overheidsorganisaties onderling ten behoeve van de dienstverlening, bijvoorbeeld uit basisregistraties. Dit is het domein dat (in elk geval waar het de ministeries en daaronder direct ressorterende onderdelen betreft) wordt bestreken door het Besluit voorschrift informatiebeveiliging rijksdienst (VIR). Decentrale overheden hanteren op vrijwillige basis nu vaak al een soortgelijke systematiek van risicobeheersing en vastgestelde generieke maatregelen, waarmee zijn in de geest van het VIR handelen. Voorts zijn zij – evenals onderdelen van de rijksoverheid – gebonden aan de informatiebeveiligingsregels ingevolge de Wet gemeentelijke basisadministratie persoonsgegevens (Wet GBA) en (de invulling van) artikel 13 Wbp. De administratieve organisatie en interne controle (AO/IC) en het beveiligingsbeleid van de overheidsorganisatie moeten op basis van al deze regels in de nodige waarborgen voor de betrouwbaarheid en vertrouwelijkheid van de gegevensstromen voorzien. Dit door adequate technische voorzieningen te treffen (bv. voor het loggen van handelingen in een beslisproces) en het verlenen van autorisaties binnen de organisatie.

---

1 Secure identities across borders linked. Zie document D2.3 - Quality authenticator scheme, paragraaf 2.3 en 2.4, te vinden op http://www.eid-stork.eu, onder STORK materials, deliverables approved/public.

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

3 Hieronder worden zowel burgers begrepen als ZZP-ers met de rechtsvorm eenmanszaak



Figuur 2 Relatie tussen Awb en regels inzake informatiebeveiliging

Samengevat is de handreiking dus gericht op de mate van zekerheid die de overheidsdienstverlener moet hebben, gelet op geldende wettelijke vereisten en daarbij spelende belangen, dat de persoon die voor zijn (virtuele) deur staat, daadwerkelijk is wie hij zegt te zijn.

1.3 Aanpak bij ontwikkeling en beheer van deze handreiking

1.3.1 Ontwikkeling

Deze handreiking is tot stand gekomen in een proces van samenwerking tussen verschillende overheidsorganisaties[4], gefaciliteerd door Logius/Bureau Forum Standaardisatie en het programma eHerkenning.
De handreiking is aan het Forum en College Standaardisatie voorgelegd met de vraag of deze toereikend is om een uitspraak te doen over het toepassingsgebied voor standaarden die op identificatie en authenticatie zien. Dit in het licht van een van de aanleidingen voor het ontwikkelen van deze handreiking, nl. de discussie in het Forum Standaardisatie over het op de 'pas toe of leg uit'-lijst van het College Standaardisatie[5] plaatsen van het programma van eisen voor PKIoverheid. Het Forum oordeelde eerder dat het nemen van een besluit daarover niet mogelijk was zolang duidelijkheid over het toepassingsgebied van PKIoverheid (dus over de diensten die het betrouwbaarheidsniveau dat PKIoverheid biedt vereisen) ontbreekt.
De concept-handreiking is op 14 juni 2011 in het Forum Standaardisatie besproken. Het Forum stemde in met de handreiking, en achtte deze geschikt voor het bepalen van het toepassingsgebied van PKIoverheid.[6] Dit oordeel zal worden betrokken bij verdere beoordeling van en besluitvorming over plaatsing van het programma van eisen van PKIoverheid op de 'pas toe of leg uit'-lijst van het College Standaardisatie. Het College Standaardisatie heeft in het najaar van 2011 ingestemd met de handreiking.[7] 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.[8]
De handreiking is voorts digitaal beschikbaar op de sites van Logius (www.logius.nl) en van het programma eHerkenning (www.eherkenning.nl).

1.3.2 Beheer en doorontwikkeling

Deze handreiking is geen statisch product. De verdere ontwikkeling van e-dienstverlening en van

[4] Belastingdienst, KvK, AgentschapNL, IND, Dienst Regelingen, Nictiz, Gemeente Amsterdam, Ministeries van BZK, EL&I en I&M.
[5] Zie hierover http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/.
[6] PM, verwijzing naar verslag van vergadering van Forum op www.open-standaarden.nl.
[7] PM verwijzing naar verslag van vergadering College op www.open-standaarden.nl.
[8] Zie hierover ook paragraaf 2.4.

identificatie- en authenticatiemiddelen, maar ook de ervaringen met toepassing van de handreiking door overheidsorganisaties, zullen aanleiding geven tot aanpassing en aanvulling.
Logius zal het beheer en de doorontwikkeling blijven ondersteunen. Dit sluit aan bij de beheerverantwoordelijkheid die Logius heeft voor verschillende identificatie- en authenticatiemiddelen en – standaarden, zoals DigiD (Machtigen) en PKIoverheid, en met ingang van 2012 ook eHerkenning.

De partijen die betrokken zijn geweest bij ontwikkeling van de handreiking vormen de basis voor een community van gebruikers van de handreiking die Logius wil benutten bij het onderhouden en verder ontwikkelen van de handreiking. Daartoe wordt de handreiking in een wiki-omgeving gepubliceerd, waar gebruikers ervaringen uit hun eigen praktijk en relevante ontwikkelingen in hun domein kunnen delen. Daarnaast zal twee keer per jaar een bijeenkomst worden georganiseerd voor gebruikers, waarin een op grond van de inbreng aangepaste nieuwe versie van de handreiking zal worden besproken en vastgesteld.

1.4 Wijze van gebruik van de handreiking

Het voor inschaling van het betrouwbaarheidsniveau essentiële onderdeel van de handreiking zit in hoofdstuk 3. Daarin is de 'menukaart' opgenomen, aan de hand waarvan overheidsorganisaties eenvoudig kunnen bepalen welk betrouwbaarheidsniveau voor een bepaalde soort dienst aangewezen is. Bij die menukaart zijn ook indicaties opgegeven die tot inschaling op een hoger of lager betrouwbaarheidsniveau zouden kunnen leiden.
Indien de organisatie meent dat een dienst, of de omstandigheden die daarbij aan de orde zijn, tot de conclusie komt dat toepassing van de algemene menukaart niet tot de gewenste uitkomst leidt, dan ligt het voor de hand om een volwaardige risicoanalyse uit te voeren ter bepaling van het betrouwbaarheidsniveau.

Het ligt in de rede dat een overheidsorganisatie in het kader van de openstelling van de elektronische weg bij dienstverlening ingevolge de Algemene wet bestuursrecht (zie hierover bijlage 2) aangeeft welk betrouwbaarheidsniveau geldt en welke identificatie- en authenticatiemiddelen daarvoor beschikbaar zijn.

Voor vragen over toepassing van de handreiking is een aanspreekpunt bij Logius beschikbaar (PM, mailadres of link).

1.5 Leeswijzer

Hoofdstuk 2 van deze handreiking bevat de uitgangspunten die bij de uitwerking van het classificatiemodel zijn gehanteerd.
In hoofdstuk 3 is de menukaart voor inschaling van diensten op het vereiste betrouwbaarheidsniveau opgenomen.
In bijlage 1 wordt het wettelijke kader beschreven waarin verschillende criteria die voor inschaling van diensten op het vereiste betrouwbaarheidsniveau hun grondslag vinden.
Bijlage 2 bevat verschillende illustraties van de wijze waarop wettelijke vereisten en formuleringen zich vertalen naar de elektronische praktijk.
In bijlage 3 is een lijst met veel gebruikte begrippen opgenomen.

2 Uitgangspunten

In dit hoofdstuk worden de uitgangspunten beschreven die bij de uitwerking van de handreiking gevolgd zijn. Deze betreffen:

- de specifieke invulling van de risicobenadering (paragraaf 2.1);
- het streven naar en de mogelijkheid tot standaardisatie van diensten (paragraaf 2.2);
- het hanteren van het STORK-kader als basis voor interoperabiliteit in identificatie- en authenticatievoorzieningen (paragraaf 2.3);
- de verantwoordelijkheid voor het bepalen van het betrouwbaarheidsniveau van diensten (paragraaf 2.4).

2.1 Risico's versus belangen en criteria

In verschillende landen gebeurt het inschalen van betrouwbaarheidsniveaus op basis van risico-analyses.[9] Ook in de VS is deze benadering gekozen; de Office of Management and Budget (onderdeel van de Executive Office of the President) heeft hiervoor in 2006 de E-Authentication Guidance for Federal Agencies vastgesteld.[10] Kort samengevat komt deze richtlijn op het volgende neer:

Het risico wordt gevormd door de dreiging, in casu het schadelijke effect van de dreiging, maal de kans dat deze dreiging zich voordoet. Als dreigingen noemt de Guidance:

- ongemak, onrust, reputatieschade;
- financiële schade of aansprakelijkheid bestuursorgaan;
- negatieve invloed op activiteiten bestuursorgaan of publieke belangen;
- ongeautoriseerde vrijgave van gevoelige informatie;
- persoonlijke veiligheid (= fysieke schade);
- fraude, misbruik en oneigenlijk gebruik van de dienst.

De kans dat de dreiging zich voordoet kan worden ingeschaald op laag, middel of hoog. De aldus bepaalde risico's worden in de Guidance kort omschreven.

Ieder orgaan van de federale overheid dient voor elk afzonderlijk proces of elke dienst, op basis van inschatting van de risico's op al deze variabelen, het benodigde betrouwbaarheidsniveau te bepalen. Op den duur zullen op basis daarvan – zo meldt de Guidance – bepaalde vaste lijnen te onderkennen zijn. Dit vergt uiteraard wel goede documentatie en vastlegging van de analyses.
De nadruk op een risicogebaseerde benadering in deze stukken wordt sterk beïnvloed door de aansprakelijkheidsaspecten, die in de Angelsaksische cultuur een dominante rol spelen.

Gesteld kan worden dat in de Nederlandse situatie:

1. Bepaling van betrouwbaarheidsniveaus bij verschillende overheidsorganisaties tot vergelijkbare resultaten dient te leiden. Daartoe is een zekere standaardisatie vereist.
2. Een volledige risicoanalyse voor het bepalen van betrouwbaarheidsniveaus zijn doel voorbij schiet. Het is kostbaar en kan alsnog tot versnippering en ongerechtvaardigde verschillen leiden. Dit terwijl processen en diensten niet uniek zijn en zelfs veel gemeenschappelijke kenmerken vertonen. Ze zijn onder andere op het wettelijke kader van de Awb gebaseerd.
   Dat laat onverlet dat risicoanalyse aangewezen of verplicht kan zijn op basis van regels inzake informatiebeveiliging (bv. Vir en Vir-BI). Bovendien kan de mate waarin in de back office maatregelen zijn genomen om betrouwbaarheid van gegevens te verzekeren, van invloed zijn op het betrouwbaarheidsniveau dat aan de 'voordeur' wordt gevraagd.

In het licht van het bovenstaande is gezocht naar een systematiek om risico's generiek in te schatten en te ondervangen. Dat kan doordat een inschatting van de te beschermen waarde uit te voeren, aan de hand van een aantal objectieve (of in elk geval objectiveerbare) criteria en belangen. Daarmee is een inschatting van de mogelijke schade mogelijk. 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.
De aanname daarbij is dat de desbetreffende diensten vanuit vergelijkbare online omgevingen worden geleverd en vergelijkbare kwetsbaarheden hebben.
Wel worden in de praktijk geregeld maatregelen getroffen die de kans op verwisselde of vervalste identiteit reduceren, evenals de daarmee samenhangende kans op een geslaagde identiteitsfraude.

---

[9] Zie bv. in Spanje: MAGERIT, Methodology for Information System Risk Analysis and Management, Ministerio de Administraciones Públicas, June 2006, http://www.epractice.eu/document/3215.

[10] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf .

Daarbij kan worden gedacht aan maatregelen als terugkoppeling via een ander kanaal, bijvoorbeeld de brief naar het woonadres zoals opgenomen in de gemeentelijke basisadministratie persoonsgegevens (GBA). Dergelijke maatregelen hebben eveneens een plaats gekregen in deze systematiek.

Het resultaat is een systematiek die een inschatting op hoofdlijnen van de risico's geeft en met betrekkelijk weinig moeite uitvoerbaar is. Daarmee kunnen overheidsorganisaties op eenvoudige wijze het vereiste betrouwbaarheidsniveau voor hun elektronische diensten bepalen.

2.2 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 Algemene wet bestuursrecht, eventueel aangevuld met vereisten uit domeinwetgeving. De relatieve eenvormigheid maakt dat families van diensten te definiëren zijn, ook al verschillen de informatie die bij de afwikkeling van die dienst nodig is (zowel van de klant als van andere overheidsorganisaties) en de (technische) inrichting van de dienst (online portaal, applicatie).
We onderscheiden hier de volgende families:

- Algemene informatie opvragen
- Aanmelden voor/reageren op discussiefora
- Aanmelden voor nieuwsbrieven ed.
- Verzoek tot feitelijk handelen (afvalcontainer, grofvuil ophalen)
- Registreren voor gepersonaliseerde webpagina
- Klacht indienen
- Aanvraag indienen (ten behoeve van een beschikking)
- Persoonsgebonden informatie opvragen/raadplegen (vgl. vooringevulde aangifte)
- Informatie verstrekken/muteren
- Verantwoording afleggen
- Bezwaarschrift indienen

De algemene of specifieke karakteristieken van de dienst bepalen welke mate van zekerheid vereist is over 'wie voor de deur staat'. Algemene karakteristieken zijn bijvoorbeeld de aard van de gegevens (persoonsgegevens vergen meer zekerheid dan niet-persoonsgegevens), specifieke karakteristieken zijn ingegeven door wettelijke vereisten voor een bepaalde dienst (bijvoorbeeld een vereiste van ondertekening).
Deze eenvormigheid van diensten op een hoger abstractieniveau maakt het ook mogelijk om ten algemene een uitspraak te doen over de mate van betrouwbaarheid die vereist is. Dat is een belangrijk uitgangspunt geweest voor de wijze van classificatie van diensten en betrouwbaarheidsniveaus die in deze handreiking is neergelegd.

2.3 STORK-niveaus als basis

Als 'ruggengraat' van een stelsel van betrouwbaarheidsniveaus waaraan enerzijds overheidsdiensten en anderzijds de beschikbare authenticatiemiddelen gekoppeld kunnen worden, wordt het STORK-raamwerk[11] gehanteerd dat in EU-verband is ontwikkeld.
STORK is opgesteld met het oog op het bevorderen van interoperabiliteit van elektronische identificatie en authenticatie in Europa, dus ook bij grensoverschrijdende dienstverlening. 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 vergelijken. Dit heeft geleid tot een raamwerk van Quality Authentication Assurance Levels, ofwel 'betrouwbaarheidsniveaus voor de kwaliteit van authenticatie'.[12]
STORK beperkt zich tot het ondersteunen van uitspraken over de mate van zekerheid dat een authenticatiemiddel van een bepaalde gebruiker daadwerkelijk verbonden is met de natuurlijke persoon die zegt dat middel te gebruiken.

Het STORK raamwerk gaat uit van vier niveaus. Het raamwerk hanteert meerdere stappen om het betrouwbaarheidsniveau van een authenticatiemiddel vast te stellen. De eerste stap is beoordeling van de volgende losstaande aspecten:

[11] Zie www.eid-stork.eu.
[12] In de Nederlandse praktijk wordt ook wel gesproken van zekerheidsniveau. Dat begrip kan worden beschouwd als synoniem voor betrouwbaarheidsniveau.

- De kwaliteit van de identificatie van de persoon bij de registratie tijdens het aanvraagproces voor het middel.
- De kwaliteit van de procedure waarin het middel aan deze gebruiker wordt uitgereikt.
- Kwaliteitseisen ten aanzien 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 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.

In de tweede stap wordt het uiteindelijke betrouwbaarheidsniveau bepaald door een combinatie van deze aspecten. Daarbij is het individuele aspect met het relatief laagste niveau bepalend voor het uiteindelijke niveau: de zwakste schakel telt. In onderstaande figuur is dit verbeeld.

Figuur 3 Bepaling van het betrouwbaarheidsniveau volgens STORK

De vier niveaus die STORK definieert zijn:

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 een authenticatiemiddel worden identificerende kenmerken zonder nadere verificatie overgenomen.
Een voorbeeld is een proces waarin de aanvrager van het middel van de uitgever een e-mail ontvangt met daarin een hyperlink die aangeklikt moet worden om het middel in gebruik te nemen. De enige zekerheid is dat er een dergelijk e-mail adres bestaat op het moment van de aanvraag en dat een verder onbekende in staat is op daarheen verzonden e-mail berichten te reageren.

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 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 vindt echter geen fysieke verschijning plaats in het registratieproces. Een middel met 1-factor[13] authenticatie volstaat.

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 onder overheidstoezicht

[13] Onder 'factor' wordt verstaan een bewijsmiddel voor een geclaimde identiteit, bijvoorbeeld een username-passwordcombinatie, of een door een vertrouwde partij toegezonden unieke code.

staan. Als type middel is 2-factor authenticatie vereist; gedacht kan worden aan 'soft' certificaten of one-time-passwords tokens.

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/EC. 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.

Door de belangen en criteria enerzijds te koppelen aan betrouwbaarheidsniveaus uit STORK en anderzijds aan de kenmerken van diensten(families), kan worden gekomen tot een generieke classificatie van diensten voor wat betreft het vereiste betrouwbaarheidsniveau (zie ook figuur 1 op pag. 6).

2.4 Toepassing van de handreiking: verantwoordelijkheid van de dienstverlener

Deze handreiking kan worden gekwalificeerd als mogelijk uitvoeringsbeleid voor de overheidsdienstverlener bij toepassing van de open normen die de Algemene wet bestuursrecht bevat voor elektronisch verkeer met burgers en bedrijven (zie bijlage 1). De overheidsdienstverlener kan zelf kiezen of hij deze handreiking van toepassing verklaart. Wezenlijk is dat daarbij te realiseren dat de handreiking zelf gebaseerd is op een generieke benadering. De handreiking zal derhalve is het merendeel van de gevallen een adequate bepaling geven van een betrouwbaarheidsniveau, maar uitzonderingen zijn mogelijk. Bij het formuleren van beleid, dat rust op deze handreiking dient hiermee derhalve rekening te worden gehouden.

De dienstverlener is dus ook verantwoordelijk voor een eventuele inschaling van diensten op een ander betrouwbaarheidsniveau dan waar de handreiking logischerwijs toe zou leiden. Dat is niet uitgesloten, maar eventuele verschillen dienen wel verklaarbaar te zijn. Daarom voorziet de handreiking niet alleen in een aantal criteria die leiden tot een generieke inschaling, maar bevat deze tevens een aantal risicoverhogende en verlagende factoren, die de grondslag kunnen vormen voor een afwijkende inschaling. Zo kunnen aanvullende waarborgen in het verdere proces van dienstverlening aanleiding zijn om tot een lagere inschaling te komen.

Het ligt voor de hand dat de dienstverlener de inschaling van het betrouwbaarheidsniveau voor zijn diensten bekendmaakt in een regeling (beleidsregels of algemeen verbindende voorschriften, afhankelijk van de context).[14] In de toelichting daarbij zal de inschaling kunnen worden onderbouwd, zodat dit ook voor gebruikers van de dienst helder is.

Het streven naar uniformiteit door middel van deze handreiking kan niet los gezien worden van het bredere kader van de omschakeling naar elektronische diensten. Uit hun aard van elektronische (via internet) en plaatsonafhankelijke dienstverlening vragen elektronische diensten meer uniformiteit dan diensten die aan een fysiek loket worden afgehandeld
In het verlengde daarvan geldt – zonder afbreuk te doen aan de complexiteit die inherent is aan deze materie – dat het in het belang van de eindgebruiker is te zorgen dat het stelsel van identificatie en authenticatie zo eenvoudig en helder mogelijk is. Ook dit betekent zo min mogelijk differentiatie, in elk geval in de betrouwbaarheidseisen die aan overheidszijde worden gehanteerd. Ook met het oog daarop wordt aangesloten op de vier STORK-niveaus.

[14] Voorbeelden van dergelijke regelingen zijn het Besluit vaststelling niveau DigiD voor Mijnoverheid.nl (Stcrt. 2008, 32) en de Regeling aanwijzing betrouwbaarheidsniveau elektronisch verkeer met de bestuursrechter (Stcrt. 2010, 15000) (hoewel hierin een onderbouwing van de keuze volgens het stramien van deze handreiking uiteraard nog ontbreekt).

3 Classificatie van diensten en betrouwbaarheidsniveaus

Op grond van bovenstaande uitgangspunten is een kader voor de inschaling van betrouwbaarheids-niveaus van diensten geformuleerd, dat als een eenvoudige risicoanalyse is te beschouwen.

De hiervoor gehanteerde systematiek, gerelateerd aan gebruikelijke elementen van risicoanalyse is de volgende:

- Belang, schade.
  De inschatting van het betrouwbaarheidsniveau wordt primair gedicteerd door een aantal criteria. Een belangrijk criterium wordt bijvoorbeeld gevormd door de privacygevoeligheid van de gegevens. De criteria zijn grosso modo gerelateerd aan het belang van de gegevens en, omgekeerd, ook aan de potentiële schade mochten deze gegevens in de handen van onbevoegde derden raken, of ongewenst worden gewijzigd.
- Dreiging, kans.
  Er wordt in de voorgestelde systematiek geen poging gedaan de dreiging of de kans dat een dreiging zich manifesteert te kwantificeren. In plaats daarvan worden aannames geformuleerd over de kwaliteit van de IT beveiliging en relevante kenmerken van het achterliggende proces, waarmee de dienst in kwestie wordt geleverd (het referentiescenario).
- Correctiefactoren.
  Aldus kan via een eenvoudige tabellarische benadering een betrouwbaarheidsniveau worden vastgesteld. Een aantal factoren is benoemd dat de dreiging reduceert ten opzichte van het referentiescenario en ook is een aantal factoren benoemd dat de dreiging verhoogt.

Aldus is een vereenvoudigde risicoanalyse mogelijk. In een aantal gevallen blijft echter een volledige risicoanalyse geboden. Situaties waarin een volledige risicoanalyse is geboden, betreffende de volgende:

- De dienst kent een inherent groot politiek, bestuurlijk of imago-risico.
- Het risico is moeilijk te bepalen omdat er sprake is van beperkte direct aan het incident gerelateerde schade, maar grote potentiële vervolgschade. Een dergelijke situatie komt voor in de tabellen in het geval van muteren op authentieke gegevens in basisregistraties. Hiervoor is het hoogste betrouwbaarheidsniveau aan de orde, tenzij analyses van (gevolg)schade aantonen dat er sprake is van een lager risico dan impliciet daarmee aangenomen.
- Situaties met ketenmachtigingen. In dergelijke situaties verdient het risico, voortvloeiend uit deze machtigingssituaties, een aparte (risico)analyse.
- 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.

3.1 Aannames over de betrouwbaarheid van de informatieverwerkende processen en systemen

De tabelmatige benadering van het betrouwbaarheidsniveau is een goede benadering bij een bepaalde kwetsbaarheid van proces en IT. Hiertoe zijn de hieronder de aannames over die kwetsbaarheid expliciet gemaakt, ze vormen als het ware het *referentiescenario*. Een aantal veel voorkomende afwijkingen ten opzichte van dit scenario zijn vervolgens onderkend en zijn vormgegeven als correctiefactoren. Dat wil zeggen dat ze (kunnen) leiden tot een bijstelling van het tabelmatig bepaalde betrouwbaarheidsniveau.

Aannames betreffende de scope.

- Het gaat om interactieve, on-line, diensten voor burgers en/of bedrijven.
- Burgers nemen diensten voor zichzelf af, werknemers nemen diensten af voor de onderneming waar ze voor werken.
- Machtiging is goed geregeld (elders).
- Er is sprake van een duidelijke afbakening wat voor soort regeling en wat voor dienstverlenend proces het betreft.

Aannames betreffende de beheersing van IT beveiliging en privacy

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

Aannames betreffende het proces dat de regeling afhandelt/de dienst voorbrengt

- 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; extra controles waarbij aan de gebruiker gevraagd wordt aanvullende zekerheden over de identiteit te verstrekken, worden verondersteld niet aanwezig te zijn.
- Bij diensten die een besluit van een bestuursorgaan omvatten, wordt het besluit steeds teruggekoppeld aan tenminste de belanghebbende en eventueel de betrokkene. Dit mag, maar hoeft niet per se, plaats te vinden via een ander kanaal als waarlangs de dienst oorspronkelijk is aangevraagd.
- Bij diensten die wel rechtsgevolg hebben, maar niet noodzakelijk een besluit van een bestuursorgaan, worden handelingen niet standaard teruggekoppeld aan de belanghebbende / betrokkene.

3.2 Criteria

De volgende criteria zijn relevant bij het inschalen van betrouwbaarheidsniveaus:

1 Rechtsgevolg

- De dienst leidt al dan niet tot rechtsgevolg.
  Als de dienst zijn grondslag vindt in wetgeving zal deze leiden tot rechtshandelingen van de overheidsorganisatie (bv. een voor beroep vatbaar besluit nemen) en dus op rechtsgevolg gericht zijn. In andere gevallen is sprake van feitelijk handelen (bv. het verstrekken van inlichtingen) en dus niet op rechtsgevolg gericht.[15]
- Indien sprake is van een dienst die leidt tot rechtsgevolg: voor het proces of de dienst geldende wettelijke eisen worden in acht genomen.

In dit instrument hanteren we twee mogelijke waarden: geen rechtsgevolg, wel rechtsgevolg.

2 Formeelrechtelijke vereisten

- Schriftelijkheid kan zijn vereist.
- Ondertekening kan worden vereist, ten behoeve van authenticatie of ter bevestiging van wilsuiting.
- In specifieke gevallen kan expliciet een geavanceerde of gekwalificeerde elektronische handtekening worden vereist, afhankelijk van de vereiste bewijskracht.

De aanname is dat schriftelijkheid in alle gevallen van elektronische dienstverlening is geregeld.
In dit instrument hanteren we de volgende mogelijke waarden: slechts algemene eisen betreffende betrouwbaarheid en vertrouwelijkheid zijn gesteld; ondertekening door of namens belanghebbende is vereist; ondertekening is vereist, tevens zijn nadere vormvereisten zijn gesteld aan de ondertekening.

3 Opgeven van persoonsgegevens door de betrokkene

- Bij de dienstverlening worden al dan niet persoonsgegevens verwerkt.
  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 alle gegevensverwerkingen van verzamelen tot en met vernietigen. Hiervan zijn in contact met de burger met name het zelf opgeven door de burger van persoonsgegevens en het op een website of in een bericht verstrekken van persoonsgegevens aan een burger relevant. Daarnaast zijn er de wijzigingen van persoonsgegevens, die worden ingegeven door burger of bedrijf.
  Als een persoon zelf persoonsgegevens op een website opgeeft, dan kan daarvoor een lager betrouwbaarheidsniveau aan de orde zijn dan voor de verstrekking vanuit de overheid van diezelfde soort gegevens. Ongeoorloofde kennisname door derden is immers bij opgave door de betrokkene niet aan de orde, terwijl dat bij verstrekking door de overheid (tonen op een overheidswebsite b.v.) wel aan de orde is. Zeker de kans dat dit op enige schaal gebeurt is het dominante risico bij verstrekking van persoonsgegevens op grote schaal. 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 dezelfde risicoklasse, is een hoger

[15] 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 uitgeven registreren van afvalcontainers op naam en adres, waarbij deze gegevens ook de basis kunnen vormen voor handhaving (bv. op het juiste moment aanbieden van huisvuil). Voor de inschaling van het betrouwbaarheidsniveau is dit van belang.

betrouwbaarheidsniveau vereist. Hierbij is gewerkt met de indeling in risicoklassen die het College Bescherming Persoonsgegevens heeft gemaakt (zie bijlage 2, onderdeel 3).

- Helaas is de indeling naar risicoklassen die het CBP maakt in het document Achtergrondstudies en Verkenningen (AV) nr. 23[16] niet geheel eenduidig. Ook is het criterium 'complexe verwerking' lastig hanteerbaar. Het element van de complexe verwerking is reeds voldoende afgedekt middels het expliciete referentiescenario en middels de differentiatie die is gemaakt tussen zelf invoeren van persoonsgegevens en het tonen van persoonsgegevens.
- We hanteren de volgende receptuur voor de bepaling van de risicoklasse:
  Stap 1. Doe een initiële inschatting van de risicoklasse aan de hand van de aard van de gegevens, volgens onderstaande tabel.
  Stap 2. Bepaal of er verzwarende factoren zijn. Is er sprake van een grote hoeveelheid naar aard (veel verschillende gegevens van een enkel persoon) of omvang (veel personen), dan kan van een verzwarende factor worden gesproken.
  Stap 3. Indien er sprake is van een of meer verzwarende factoren, ga dan 1 risicoklasse omhoog. Een uitzondering hierop vormen de financieel-economische gegevens, waar geen verzwaring voor aan de orde is (altijd risicoklasse II).

Klasse	**Aard van de gegevens**
Geen persoonsgegevens	De gegevens zijn niet te herleiden tot geïdentificeerde of identificeerbare persoon.
Risicoklasse 0	Publiek. Openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures en publieke internetsites.
Risicoklasse 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.
Risicoklasse II	Verhoogd risico. Bijzondere persoonsgegevens als genoemd in artikel 16 Wbp, of financieel-economische gegevens in relatie tot de betrokkene.
Risicoklasse 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.

In dit instrument hanteren we de volgende waarden voor dit criterium:
- er is geen sprake van verwerking van persoonsgegevens;
- risicoklasse 0;
- risicoklasse I;
- risicoklasse II;
- risicoklasse III.

4 Tonen van persoonsgegevens, anders dan in zelfde sessie door gebruiker opgegeven

- Zie voor toelichting het bovenstaand criterium.

In dit instrument worden de volgende waarden gehanteerd:
- geen persoonsgegevens in aanvulling op zelf opgegeven;
- risicoklasse 0;
- risicoklasse I;
- risicoklasse II;
- risicoklasse III.

5 Verwerking van het BSN

- In het verlengde van de discussie over aggregatie van persoonsgegevens dient ook het BSN te worden gezien. Het BSN is bij uitstek een sleutel, die dergelijke aggregatie binnen organisaties en over organisaties heen vereenvoudigt. Het BSN, hoewel het zelf niet die aggregatie van gegevens vormt, is wel een opmaat naar de koppelbaarheid.

[16] 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.

In dit instrument worden de volgende waarde gehanteerd: 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 gebruik 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 dergelijke gegevens als 'de waarheid' worden behandeld.
- Onderscheid wordt daarbij wel gemaakt naar mutaties op niet-authentieke gegevens en mutaties op de authentieke gegevens.

In dit instrument worden de volgende waarden gehanteerd:
- er is geen sprake van muteren van een basisregistratie op basis van opgegeven gegevens;
- mutaties van niet-authentieke gegevens in basisregistraties;
- mutaties 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 omvang) of het uitlekken van koersgevoelige informatie.

De volgende waarden worden daarbij gehanteerd:
- 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 euro.
- 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 euro.

8 Publiek belang

- Dit belang vormt in feite het spiegelbeeld van het risico op schending van collectief economisch belang, collectieve veiligheid, schokken van de rechtsorde ed. Onderscheid wordt gemaakt naar publicitair en maatschappelijke ontwrichting.
  In dit instrument worden de volgende waarden gehanteerd:

a) Publicitair, publiek vertrouwen in dienstverlening. Laag = klachten, krantenberichten; Midden = ombudsman bemoeit zich ermee, Kamervragen etc; Hoog = Minister valt.
b) Maatschappelijke ontwrichting. Laag = verstoringen, die binnen de middelen van een enkele organisatie opgelost kunnen worden; Midden = verstoringen die gecoördineerd optreden van meerdere organisaties, veelal publiek en privaat vragen; Hoog = noodtoestand; verstoringen die noodmaatregelen vereisen buiten de normale juridische, financiële etc. kaders.

3.3 Koppeling criteria aan betrouwbaarheidsniveaus

In onderstaande tabel worden de gedefinieerde criteria afgezet tegen de gedefinieerde betrouwbaarheidsniveaus. Van elk van de 7 benoemde criteria bepaalt men het laagste toepasselijke betrouwbaarheidsniveau. Het hoogste van de aldus verkregen betrouwbaarheidsniveaus is het toepasselijke betrouwbaarheidsniveaus.

Criteria	**Betrouwbaarheidsniveau**
- geen rechtsgevolg - algemene eisen aan betrouwbaarheid en vertrouwelijkheid - opgave door betrokkene van publieke persoonsgegevens (risicoklasse 0) - geen tonen van persoonsgegevens door overheidsdienstverlener	0 (geen eisen aan authenticatie)

- geen verwerking BSN - geen mutaties basisregistratie - economisch belang nihil - publiek belang nihil	
- geen rechtsgevolg - algemene eisen aan betrouwbaarheid en vertrouwelijkheid - opgave van persoonsgegevens, maximaal risicoklasse I[17] - tonen van persoonsgegevens, maximaal risicoklasse 0 - geen verwerking BSN - geen mutaties basisregistratie - economisch belang nihil - publiek belang nihil	1
- al dan niet rechtsgevolg - wettelijke eisen omtrent ondertekening - opgave van persoonsgegevens in maximaal risicoklasse II - Tonen van persoongegevens betreft max risicoklasse 1 - BSN wordt verwerkt, opgave door gebruiker, evt via DigiD - Geen mutatie basisregistratie - economisch belang gering - publiek belang gering	2
- rechtsgevolg - wettelijke eisen omtrent ondertekening of wilsuiting - opgeven persoonsgegevens maximaal risicoklasse III - tonen persoonsgegevens risicoklasse II - BSN wordt verwerkt, al dan niet opgave door gebruiker - mutatie niet-authentieke gegevens basisregistraties - economisch belang gemiddeld - publiek belang gemiddeld	3
- rechtsgevolg - wettelijke eisen aan ondertekening, nadere vormeisen - verwerking van persoonsgegevens van risicoklasse III - tonen van persoonsgegevens risicoklasse 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 groot	4

[17] Voor een toelichting op de genoemde risicoklassen zie bijlage 2, onderdeel 3.

3.4 Correctiefactoren

De bovengeschetste aannames (het *referentiescenario*) en de daarmee samenhangende tabellarische bepaling van het betrouwbaarheidsniveau geven niet onder alle omstandigheden een juiste uitkomst. Met name kunnen er specifieke aspecten zijn in het proces die als risicomitigerende factor werken. Risicoverzwarende 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. Dit zijn alle indicatoren voor het uitvoeren van een volledige risicoanalyse.

Risicomitigerende factoren zijn veelal in het achterliggende proces gelegen. Voorbeelden zijn:
- Aanvullende zekerheid over de identiteit van de betrokkene wordt verkregen;
- Aanvullend bewijsmateriaal dat de grondslag voor te verrichten dienst versterkt wordt ingewonnen;
- Mutaties van gegevens worden schriftelijk teruggekoppeld (na elektronische mutatieopgave);
- Maatregelen worden getroffen om ongebruikelijke patronen vroegtijdig te detecteren, teneinde fraude ofwel te voorkomen ofwel in een vroeg stadium tegen te houden.

De risicomitigerende factoren worden hieronder nader uitgewerkt.

Als een risicomitigerende factor van toepassing is, dan is onder omstandigheden verlaging van het resulterende betrouwbaarheidsniveau met 1 stap mogelijk. Echter, waar wettelijke eisen het betrouwbaarheidsniveau bepalen (bijvoorbeeld vormeisen aan ondertekening), is verlaging niet aan de orde. Ook is verlaging van betrouwbaarheidsniveau 1 naar 0 niet toegestaan.

Risicomitigerende factoren

De volgende risicomitigerende factoren worden onderkend:

1. In het vervolgproces bevindt zich een processtap waarin de belanghebbende zich fysiek moet melden zodanig dat opgemerkt wordt wanneer een ander in plaats van deze belanghebbende en zonder dat deze daartoe toestemming heeft gegeven de dienst heeft afgenomen en het proces in gang gezet.
2. In het vervolgproces bevindt zich een processtap waarin de belanghebbende natuurlijk persoon zich fysiek meldt en zich moet legitimeren met een ID-document en het BSN geverifieerd wordt met het in het proces vastgelegde BSN.
3. Terugkoppeling van mutaties of (voorgenomen) besluiten vindt plaats, via een ander kanaal dan het oorspronkelijke elektronische.
4. 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.
5. 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.
6. 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.

3.5 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.

Voorbeelden van diensten	**Vereiste 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.)	2

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 vergunningvoorschriften particulieren Inzien WOZ waardering	
Belastingaangifte particulieren; ophalen of muteren vooringevulde aangifte (tonen persoonsgegevens risicoklasse 2) Aanbestedingsdocumenten Omgevingsvergunning ondernemingen, verblijfsvergunning arbeids/kennismigranten officiële documenten (VOG, paspoort, rijbewijs ed.) Belastingaangifte ondernemingen Financiële aanspraak ondernemingen (subsidie) Naleving voorschriften ondernemingen (jaarrekening ed.)	3
Aangifte (geboorte) Raadplegen medisch dossier Aangifte (delicten, zwaar) Octrooiaanvragen	4

Bijlage 1 Relevante wet- en regelgeving

1. Algemene wet bestuursrecht

Met de Wet elektronisch bestuurlijk verkeer (Webv)[18] is een afdeling 2.3 toegevoegd aan de Algemene wet bestuursrecht (Awb). Deze afdeling bevat algemene regels betreffende 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.[19]

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 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

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

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 dus niet snel aan elektronisch verkeer 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 enkele 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, terinzageleggingen) 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, dan wel 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.

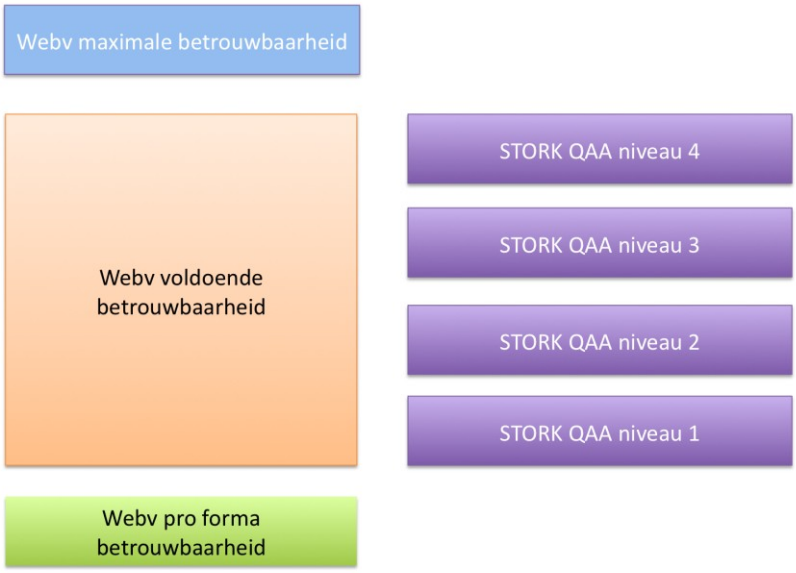
Het derde lid van artikel 2:14 refereert aan een ander belangrijk uitgangspunt van de Wet elektronisch bestuurlijk verkeer, namelijk **betrouwbaarheid en vertrouwelijkheid**. Indien een bestuursorgaan een bericht elektronisch verzendt, dan dient dit op een voldoende betrouwbare en vertrouwelijke manier 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 maximaal (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'.[20]

De wetgever beoogt met de eis van betrouwbaarheid en vertrouwelijkheid uitdrukking te geven aan de zogenaamde *algemene beginselen van behoorlijk IT-gebruik*.[21] Hieronder worden verstaan de beginselen van authenticiteit, integriteit, onweerlegbaarheid, transparantie, beschikbaarheid, flexibiliteit en vertrouwelijkheid. Concreet kunnen deze beginselen bijvoorbeeld worden gewaarborgd met techniek waarmee een elektronische handtekening kan worden gezet, met een tijdsstempel of met behulp van cryptografische technieken.

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 acht 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 een adequate invulling van de open norm uit de Awb. In onderstaande figuur wordt deze relatie geïllustreerd.

[20] Kamerstukken II 2001/02, 28 483, nr. 3, p. 16-17.
[21] 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.



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 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.[22] 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 spiegelbeeld van artikel 2:14, eerste lid, is opgenomen in het eerste lid van artikel 2:15. Dit lid regelt dat ook het bestuursorgaan moet hebben aangegeven elektronisch bereikbaar te zijn. Deze **kenbaarmaking 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.
Deze 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.[23]
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

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

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 zich beperkt 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 worden hier op 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.
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 controle meer heeft. Als het bestuursorgaan en de geadresseerde gebruikmaken van hetzelfde systeem voor gegevensverwerking, is dit het moment waarop het toegankelijk wordt voor de geadresseerde.
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[24] (hierna: Weh) is de Europese richtlijn over een gemeenschappelijk kader voor elektronische handtekeningen geïmplementeerd.[25] 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 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.

[24] Stb. 2003, 199.
[25] 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.

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.[26]

Deze definitie is behoorlijk ruim. Ook een ingescande handgeschreven handtekening kan hiermee als elektronische handtekening worden aangemerkt.[27] 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 enkele 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, wil men een elektronische handtekening gelijk 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 tenslotte dat partijen een hoger of lager betrouwbaarheidsniveau dan dat van lid 2 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.[28]
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 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

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

een verklaring.[29]

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:
- uitdrukkelijke toestemming van degene van wie gegevens worden verwerkt;
- de verwerking vindt plaats ter uitvoering van publiekrechtelijke taken;
- 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.
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 de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking (artikel 23).

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) onderkent op basis van artikel 13 Wbp vier **risicoklassen** met betrekking tot persoonsgegevens. Deze klassen zijn uitgewerkt in Achtergrondstudies en Verkenningen (AV) nr. 23 van het Cbp.[30] Hoewel dit normatieve advies stamt uit 2001 is het nog steeds relevant en bruikbaar als norm voor het bepalen van de toepasselijke risicoklassen.

AV nr. 23 hanteert drie criteria om een risicoklasse te bepalen. Het eerste criterium is de aard van de gegevens. Daarbij wordt onderscheid gemaakt naar openbare gegevens, 'gewone' persoonsgegevens, bijzondere persoonsgegevens zoals benoemd in de Wbp, art. 16, financieel-economische gegevens en tenslotte gegevens waar een bepaalde wettelijke geheimhoudingsplicht op rust (bijvoorbeeld gegevens van inlichtingendiensten, beroepsgeheim, DNA-banken). Het tweede criterium is de hoeveelheid gegevens, naar aard en omvang. Veel personen impliceert veel gegevens. Veel persoonsgegevens van weinig personen impliceert veel gegevens. Het derde criterium is de complexiteit van de verwerking, dit wordt gezien als een factor die duidt op een grotere kans dat er met de verwerkingen iets ongewenst gebeurd (bijvoorbeeld ongeoorloofde kennisname door een derde).
In het hoofddocument is een methode gegeven om op basis van deze criteria te komen tot een indeling in een risicoklasse. Voor een nadere toelichting op de criteria zij verwezen naar AV nr. 23.

Zoals hierboven al opgemerkt geldt op basis van artikel 13 Wbp een beveiligingsplicht voor degene die verantwoordelijk is voor de verwerking van persoonsgegevens. Wat volgens het Cbp verstaan moet

[29] Zie hierover ook R. van Esch, Electronic data interchange (EDI) en het vermogensrecht, Deventer 1999, pag. 139-141.
[30] 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.

worden onder een "passende technische en organisatorische maatregelen" in de zin van artikel 13 Wbp is eveneens uitgewerkt in AV nr. 23.
Het beveiligingsadvies hangt direct samen met de toepasselijke risicoklasse waarin een bepaald persoonsgegeven valt. De verantwoordelijke dient de classificatie te bepalen op basis van een risicoanalyse. Deze dient toetsbaar te zijn en de verantwoordelijke moet hierover verantwoording kunnen afleggen, bijvoorbeeld bij een audit, indien het Cbp of de rechter daarom vraagt.

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.
Deze 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 paragraaf 1.2 van de handreiking is nader op de afbakening tussen informatiebeveiligingsbeleid (VIR, VIR-BI) en elektronisch verkeer (Awb) ingegaan.

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.

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 **geclassificeerde informatie**. Dat is informatie die als Staatsgeheim is gerubriceerd, of als departementaal vertrouwelijk.

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. De Wet algemene bepalingen burgerservicenummer geeft regels over oa. uitgifte en gebruik van dit nummer.

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

Ten aanzien van BSN geldt een **vergewisplicht**, wat 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, doordat aan de beheervoorziening langs elektronische weg de vraag kan worden gesteld of aan een bepaalde persoon een burgerservicenummer is toegekend en zo ja welk burgerservicenummer aan die persoon is toegekend. Op deze wijze kan het burgerservicenummer van een bepaalde persoon worden nagetrokken. Aan de beheervoorziening kan voorts 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.[31]
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 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.[32] 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. De reden hiervoor is dat hij geen invloed heeft op de keuze van het hulpmiddel (CD-rom, USB stick) waarop degene ten behoeve van wie de akte bewijs oplevert, de akte opslaat.

Voor de ondertekening van elektronische onderhandse akten wordt in het algemeen een elektronische handtekening als bedoeld in artikel 3:15a 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

[31] Ontleend aan memorie van toelichting Wabb.
[32] Stb. 2006, 475, laatstelijk gewijzigd in *Stb*. 2006, 706.

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 betreffende de totstandkoming van overeenkomsten en artikel 1021 Rv betreffende de arbitrageovereenkomst. Artikel 156a Rv voorziet er slechts in voor onderhandse akten te bepalen onder welke voorwaarden die op een andere wijze dan schriftelijk kunnen worden opgemaakt.

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

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

1. Verzenden van elektronische berichten

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

Voorbeelden zijn:
- Versturen en ontvangen van een faxbericht of e-mail met inhoudelijke informatie.
- Geautomatiseerde berichtuitwisseling (bijvoorbeeld een fiscale aangifte of jaarrekening in XBRL).
- 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 dienst 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).[33]
- 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.

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 hierboven)).
- Een chat met een ambtenaar (vergelijkbaar met telefoongesprek).
- Een telefoongesprek, ook al gaat dat in vergelijkbare berichten over internet (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

[33] De MvT bij het wetsvoorstel voor de Webv geeft overigens aan dat een sms in het algemeen niet zal voldoen aan de eis van voldoende betrouwbaar en vertrouwelijk (Kamerstukken II 2001/02, 28 483, nr. 3, p. 7).

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 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, echter dat is strikt genomen geen bewijs dat 'het bericht het systeem van het bestuursorgaan heeft bereikt', zoals artikel 2:17 Awb vereist. Hiertoe zou eerder een gewaarmerkt bericht, van een tijdsstempel voorzien, toegepast dienen te 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.[34] 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.[35]

3. 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 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.[36] 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.[37] 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[38]; in beide gevallen blijft ook de elektronische weg openstaan.

b. Vormvoorschriften die zich tegen elektronisch verkeer verzetten

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:	De eis "in persoon" te

[34] Kamerstukken II 2001/02, 28 483, nr. 3, p. 13.
[35] Openstelling elektronische bestuurlijk verkeer met de belastingdienst, 27 april 2005, nr. CPP 2004/2807M, Stcrt. 87, p. 12.
[36] CBB 4 juni 2008, LJN BD4039 (Aanvraag MEP-subsidie).
[37] 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.
[38] Dit voorbeeld is overigens inmiddels achterhaald, nu de Staatscourant sinds 2009 niet meer op papier verschijnt.

	"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.	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.

4. 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.

Formuleringen in wet- en regelgeving met analogie voor elektronisch verkeer		
Formulering wetstekst	**Voorbeeld**	**Elektronische analogie**
schriftelijk indienen	Artikel 5 Grondwet MvT Wet elektronisch bestuurlijk verkeer (Awb)	Een geschrift is iedere drager van verstaanbare lettertekens die – in onderling verband – een gedachte-inhoud vertolken. Daaruit volgt dat onder geschrift ook een elektronisch te lezen stuk is te verstaan. Een e-mail is in deze optiek schriftelijk.
met gebruikmaking van het origineel van een ondertekend formulier	Regeling MEP-subsidies	Het invullen van een formulier op een website wordt geacht schriftelijk te zijn. Indien dit gebeurt na te zijn ingelogd is de identificatie van de verzender van hetzelfde betrouwbaarheidsniveau als de inlogmethode, aannemende dat de verbinding tenminste op datzelfde niveau beveiligd is.
ondertekening, ondertekend…	zie artikel 2:16 Awb	Een 'natte' handtekening kan vervangen worden door een

		elektronische handtekening. Het soort elektronische handtekening (gewoon, geavanceerd, gekwalificeerd) is afhankelijk van de aard van het bericht, het doel waarvoor het gebruikt wordt en de omstandigheden van het geval.
… schriftelijke klacht, ondertekend, ten minste bevattend: naam en adres indiener, dagtekening …	Awb artikel 9:4	Een met enige vorm van door ontvanger te valideren elektronische handtekening ondertekende e-mail waarin naam en adres vermeld zijn. Naar analogie van Awb art 2.17 kan het daar gedefinieerde tijdstip als dagtekening gebruikt worden.
aanvraag tot het geven van een beschikking, ondertekend, ten minste bevattend: naam en adres indiener dagtekening …	Awb art 4.2 lid 1	Uit art 4.3a Awb (Het bestuursorgaan bevestigt de ontvangst van een elektronisch ingediende aanvraag) blijkt dat een dergelijke aanvraag elektronisch kan zijn. Een gewone e-mail kan aan de vereisten voldoen, met uitzondering van de ondertekening.
overlegging of toezending van bescheiden en andere gegevensdragers of de inhoud daarvan	artikel 7, Algemene wet inzake rijksbelastingen	Maakt elektronisch equivalent van 'aangiftebiljet' mogelijk.

5. 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.

6. Ondertekening van berichten

Indien ondertekening van een bericht is vereist, wordt daarvoor ingevolge artikel 2:16 Awb een elektronische handtekening gebruikt.
Hieronder 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	Kopie van ondertekend document, print van document met gescande handtekening, elektronisch bestand die een gescande handtekening bevat.

	als zodanig door partijen geaccepteerd wordt.	
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 veelvoorkomende begrippen in de handreiking gedefinieerd. De begrippen zijn in alfabetische volgorde geplaatst.
Voor een uitgebreide lijst van begrippen op het terrein van identificatie en authenticatie wordt verwezen naar de begrippenlijst die in het kader van eHerkenning is ontwikkeld.[39]

Authenticatie: de controle (het staven) van de (een) geclaimde identiteit van een partij en de set van zijn geclaimde attributen op een bepaald betrouwbaarheidsniveau.

Belanghebbende: degene wiens belang rechtstreeks bij een besluit is betrokken (artikel 1:2 Awb). De belanghebbende is dus de persoon waarop de rechtsgevolgen van een overheidsdienst direct betrekking hebben. De belanghebbende kan een natuurlijke persoon of een niet-natuurlijke persoon.

Bericht: een uiting, overgebracht in de vorm van elektronische communicatie of elektronisch verkeer.

Betrouwbaarheidsniveau: een niveau van zekerheid waarmee de door een belanghebbende geclaimde identiteit in het kader van het verrichten van een dienst kan worden vastgesteld (authenticatie). Dit begrip moet worden onderscheiden van zekerheidsniveau (assurance level) of beveiligingsniveau. Dit betreft het geheel aan beveiligingsmaatregelen dat nodig is om een dienst betrouwbaar uit te voeren en de vertrouwelijkheid van de daarbij behorende gegegevensuitwisseling te borgen. Bij dat geheel horen ook andere maatregelen dan met betrekking tot de authenticatie van de gebruiker.

Conventioneel verkeer (communicatie, berichten): verkeer waarbij berichten op papier worden verzonden en ontvangen, door persoonlijke bezorging of door tussenkomst van een postdienstverlener.

Dienst: een dienst die door een overheidsorganisatie in het kader van aan hem toebedeelde taak wordt aangeboden aan een natuurlijke of niet-natuurlijke persoon. Een dienst kan een (op rechtsgevolg gericht) besluit van de desbetreffende overheidsorganisatie betreffen, of feitelijk handelen door die overheidsorganisatie (het verstrekken van goederen, informatie ed.).

Elektronisch verkeer (elektronische communicatie, elektronische berichten): 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.

Gegeven: een eenheid van informatie die in een dienst verwerkt wordt. Het begrip is niet beperkt tot gegevens die de gebruiker expliciet zelf opgeeft of beschikbaar heeft. Het tijdstip waarop een dienst gestart en het IP-adres waarvandaan een browser een dienst opvraagt zijn bijvoorbeeld ook gegevens.

Identificatie: het noemen van attributen van een entiteit om deze in een bepaalde context uniek aan te duiden.

Middel: een set van attributen op basis waarvan een gebruiker zich kan laten authenticeren, gevat in een bepaalde elektronische toepassing.
Dit kan een combinatie van gebruikersnaam en wachtwoord zijn of een in software, op een smartcard of in andere specifieke hardware opgeslagen certificaat.

Natuurlijke persoon: een individueel menselijk wezen en subject van rechten en drager van plichten.

Niet-natuurlijke persoon: een organisatie, al niet met rechtspersoonlijkheid.

Persoon: een natuurlijke persoon of een niet-natuurlijke persoon.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon.

[39] Zie http://www.eherkenning.nl/sites/default/files/20100906-eherkenning-algemene-introductie-versie-1.0-final.pdf.