FS-20110614.04A

Handreiking

Classificatie van overheidsdiensten en bepaling van het daarvoor vereiste betrouwbaarheidsniveau

concept 0.91

Colofon

Auteur
Logius
Project

Organisatie
Logius
Titel
Classificatie van overheidsdiensten ten aanzien van vereiste betrouwbaarheidsniveau

Status
Concept
Datum
3 feb 2011

Versie
0.9

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

Distributielijst

Datum	Distributie	Versie
5-2-2011	Deelnemers workshop	0.6b
25-2-2011	Deelnemers workshop	0.7d
4-5-2011	Deelnemers workshop	0.8

Goedkeuring

Datum	Naam	Versie

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 e-dienstverlening in het STORK-project.[1] 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.
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 en collectieve koppeling van (soorten) diensten en betrouwbaarheidsniveaus bevat. Daarachter zit de 'receptuur' waarmee de menukaart is samengesteld. Daarin zijn de factoren beschreven waarop de generieke en collectieve inschaling is gebaseerd en die de grondslag kunnen vormen voor een afwijkende inschaling door de overheidsdienstverlener.

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 beperkt tot degene die een dienst voor zichzelf afneemt, dus niet voor machtigingssituaties, niet omdat deze 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 meerdere diensten aanbiedt met verschillende betrouwbaarheidsniveaus dan zal hij met gebruikmaking van de handreiking wel kunnen bepalen of voor deze diensten 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.

[1] Secure identities across borders linked, zie www.eid-stork.eu.

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 kan voor vergelijkbare diensten toch een verschillend betrouwbaarheidsniveau 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

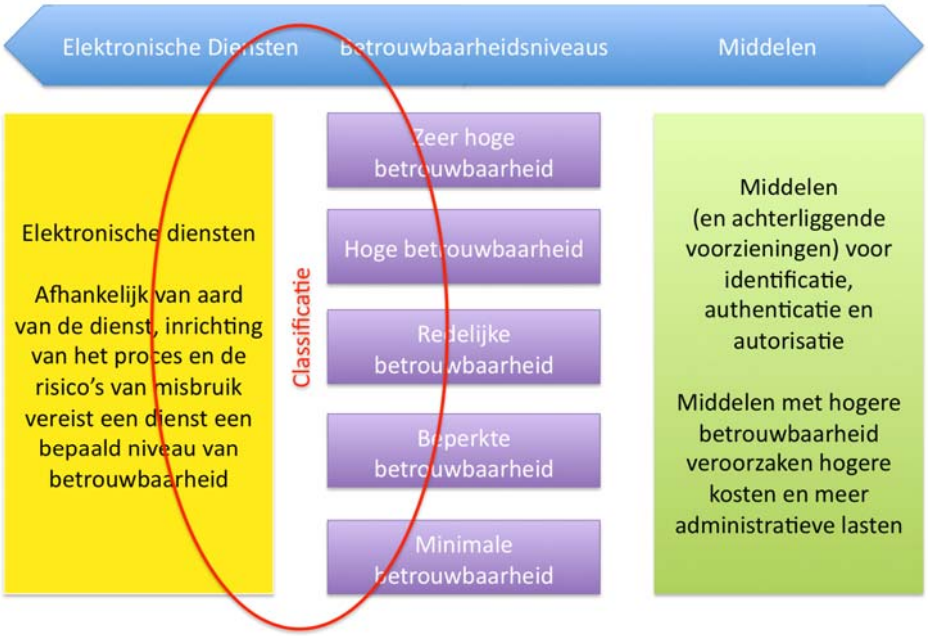
De handreiking bedient verschillende doelgroepen. Enerzijds biedt hij de basis voor de dialoog tussen beleidsmakers, (proces)architecten en informatiebeveiligers bij het inrichten van e-diensten en back office processen. Anderzijds biedt hij bestuurders inzicht in de afwegingen die aan het bepalen van 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 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 kan zijn dat zij met de juiste persoon te maken heeft.

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 is 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 “grootste gemene deler” oplossing. Deze zou te duur en ingewikkeld zijn voor het ene geval of te slecht beveiligd voor het andere. Indeling van de middelen op basis van betrouwbaarheidsniveaus is de oplossing daarvoor. Ieder van die betrouwbaarheidsniveaus geeft een niveau van afweging weer op basis van een 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.



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 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 de grondslag van deze handreiking liggen algemene en specifieke wettelijke voorschriften voor elektronisch verkeer tussen overheid en burgers. Daarnaast haakt het kader aan op het raamwerk dat in Europees verband voor classificatie van identificatie en authenticatiemiddelen is ontwikkeld, STORK[2]. 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 een aan 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 ziet op 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.[3]

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.[4]
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. Deze handreiking ziet niet specifiek op de vraag hoe daarmee omgegaan moet worden, maar is wel bruikbaar om te bepalen of het aantal niveaus beperkt kan worden. Risicoverhogende en – verlagende aspecten rond de dienstverlening of de afnemers kunnen daarbij een rol spelen, evenals de aard van de doelgroep van de diensten.

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 veelal ISO27002 of NEN 7510. 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.

PM Plaatje relatie Awb en VIR

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

---

2 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.

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

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

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[5], gefaciliteerd door Logius en het programma eHerkenning.
De handreiking is in juni 2011 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[6] 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 dat het betrouwbaarheidsniveau dat PKIoverheid biedt vereist) ontbreekt.
PM weergave besluiten Forum en College Standaardisatie.[7]

Na accordering door het College Standaardisatie is de handreiking 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 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 of meer van deze indicaties aan de orde zijn, kan hij met behulp van het classificatiemodel in bijlage 3 een uitgebreide analyse maken van de karakteristieken van de dienst en mogelijke risicoverhogende en verlagende factoren, en op basis daarvan een op de situatie toegespitst betrouwbaarheidsniveau vaststellen.

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).

---

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

1.5 Leeswijzer

Hoofdstuk 2 van deze handreiking bevat de uitgangspunten die bij 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.

Bijlage 3 bevat vervolgens het uitgebreide classificatiemodel, aan de hand waarvan beoordeeld kan worden of voor een bepaalde dienst een van de menukaart afwijkende inschaling nodig of wenselijk is.

In bijlage 4 is een lijst met veel gebruikte begrippen opgenomen.

2 Uitgangspunten

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

- de specifieke invulling van de gebruikelijke risicobenadering;
- het streven naar en de mogelijkheid tot standaardisatie van diensten;
- het hanteren van het STORK-kader als basis voor interoperabiliteit in identificatie- en authenticatievoorzieningen;
- de verantwoordelijkheid voor het bepalen van het betrouwbaarheidsniveau van diensten.

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 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 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.

Geconstateerd kan worden dat een zo fijnmazig systeem in de Nederlandse context niet nodig en niet wenselijk is. De nadruk ligt in de risicogebaseerde stelsels voor het bepalen van betrouwbaarheidsniveaus sterk op aansprakelijkheidsaspecten, wat in het licht van de overheersende cultuur in de VS (maar ook in andere landen) begrijpelijk is. Daarnaast is de vraag of het efficiënt is om iedere overheidsorganisatie aparte risico-analyses te laten verrichten, aangezien processen en diensten niet uniek zijn en zelfs veel gemeenschappelijke kenmerken vertonen. Ze zijn onder andere op het wettelijke kader van de Awb gebaseerd.
Individuele risico-analyse aangaande het aspect authenticatie van gebruikers (per bestuursorgaan en per dienst) is dan niet nodig, het is kostbaar en kan alsnog tot versnippering en ongerechtvaardigde verschillen leiden. 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 voorgaande is gezocht naar een mechanisme om risico's collectief in te schatten en te ondervangen. Dat kan door te werken met het spiegelbeeld van risico's, nl. objectieve (of in elk geval objectiveerbare) criteria en belangen. Daarbij kan men denken aan 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.

2.2 Families van diensten

Zoals hiervoor is opgemerkt zijn de processen die achter e-overheidsdiensten zitten vaak gelijksoortig van aard en opbouw. De informatie die nodig is, zowel van de klant als van andere overheidsorganisaties (denk aan basisregistraties) verschilt per domein. De relatieve eenvormigheid maakt dat families van

[9] Zie bv. het Magerit-kader in Spanje (PM zie links in STORK-documenten)
[10] PM vindplaats

diensten te definiëren zijn. Het gaat om 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. ook 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. Eerst worden losstaande aspecten beoordeeld. Vervolgens 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.

De aspecten die STORK in ogenschouw neemt zijn:

- 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.
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

[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.

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 authenticatimiddel verificatie plaats van de door de gebruiker geclaimde identiteit door controle op basis van een door een Staat afgegeven document (bv. 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 staan. Als type middel is 2-factor authenticatie vereist gebaseerd op certificaten.

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 families van diensten, 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 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 collectieve en generieke benadering zal in het merendeel van de gevallen (uitgegaan is van de 80-20 regel) voldoen voor een adequate bepaling van het betrouwbaarheidsniveau voor een dienst. De verantwoordelijkheid voor toepassing ervan ligt dan ook bij de dienstverlener.
Dat betekent dat hij ook verantwoordelijk is 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. Dat is de reden waarom de handreiking niet alleen voorziet in een ‘menukaart’ op basis waarvan in het algemeen het betrouwbaarheidsniveau vastgesteld zal kunnen worden, maar ook van de achterliggende ‘receptuur’. Die wordt gevormd door een uitsplitsing van de factoren waarop de generieke en collectieve inschaling is gebaseerd, en een aantal risicoverhogende en verlagende factoren, die grondslag kunnen vormen voor een afwijkende inschaling.

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. Deze uitsplitsing vormt tevens de inhoudelijke verantwoording over de relevantie en betekenis van de gekozen criteria en belangen (vanuit oogpunt van auditing).

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

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

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

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.

3 Classificatie van diensten en betrouwbaarheidsniveaus

Op grond van bovenstaande uitgangspunten is het volgende kader voor inschaling van betrouwbaarheids-niveaus van diensten geformuleerd.

3.1 Relevante criteria en belangen

De volgende criteria en belangen zijn relevant bij het inschalen van betrouwbaarheidsniveaus:

- 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.
- Een aan de dienst verbonden transactie vereist een ondertekening, al dan niet bij wijze van wilsuiting.
- Bij de dienstverlening worden al dan niet persoonsgegevens verwerkt.
  Daarbij zijn de aard van en de hoeveelheid persoonsgegevens die verwerkt worden relevant. Het College bescherming persoonsgegevens heeft hiervoor een indeling in risicoklassen gemaakt (zie hierover bijlage 2, onderdeel 3). Bij persoonsgegevens die relateren aan de persoonlijke integriteit (bijvoorbeeld medische gegevens) zijn de belangen veelal groter dan bij eenvoudige NAW-gegevens.
- Er is een individueel economisch belang.
  Dit belang vormt in feite het spiegelbeeld van het risico op fraude, misbruik of oneigenlijk gebruik of schade als gevolg van oneerlijke concurrentie. In het kader is ook relevant of bij de dienstverlening concurrentie-, koersgevoelige of anderszins economisch gevoelige gegevens worden verwerkt.
- Er is een 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. De impact van schending van het belang is groot.

3.2 Families van diensten en koppeling aan betrouwbaarheidsniveaus

In onderstaande tabel worden de in hoofdstuk 2 gedefinieerde families van diensten gekoppeld aan betrouwbaarheidsniveaus, op basis van de voor die diensten relevante criteria en belangen.

Diensten / processen	**Criteria**	**Vereiste betrouwbaarheidsniveau**
Aanmelden voor/reageren op discussiefora (online community) *Aanmelden voor nieuwsbrieven*	-	0 (geen eisen)
Algemene informatie opvragen *Verzoek tot feitelijk handelen* *Klacht indienen*	- geen rechtsgevolg - geen wilsuiting of wettelijke eisen omtrent ondertekening - verwerking van persoonsgegevens in maximaal risicoklasse I[16] - economisch belang nihil - publiek belang nihil	1
Registreren voor gepersonaliseerde webpagina	- al dan niet rechtsgevolg - wilsuiting of wettelijke eisen omtrent	2

[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.

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

Aanvraag indienen *Informatie opvragen/raadplegen* *Informatie verstrekken* *Verantwoording afleggen* *Bezwaarschrift indienen* *Beroepschrift indienen*	- verwerking van persoonsgegevens in maximaal risicoklasse I - economisch belang gering - publiek belang gering	
Informatie opvragen *Informatie verstrekken* *Aanvraag indienen* *Verantwoording afleggen*	- rechtsgevolg - wilsuiting of wettelijke eisen omtrent ondertekening - verwerking van persoonsgegevens in maximaal risicoklasse II - verwerking van concurrentiegevoelige, koersgevoelige of anderszins economisch gevoelige gegevens - verwerking leidt tot mutatie van gegevens in basisregistratie - economisch belang gemiddeld - publiek belang gemiddeld	3
Informatie opvragen *Informatie verstrekken* *Aanvraag indienen*	- rechtsgevolg - wilsuiting of strenge wettelijke eisen omtrent ondertekening in verband met onweerlegbaarheid - verwerking van persoonsgegevens van risicoklasse III - verwerking van concurrentiegevoelige, koersgevoelige of anderszins economisch gevoelige gegevens - verwerking gegevens leidt tot muteren of creëren authentiek gegeven in basisregistratie - economisch belang groot - publiek belang groot	4

3.3 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**
bezoeken overheidswebsites	0 (geen eisen)
gemeentelijke diensten (melden gebreken in de openbare ruimte, aanvragen afvalcontainers)	1
registreren voor mijnoverheid.nl, mijnbelastingdienst.nl etc. 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 naleving vergunningvoorschriften particulieren	
fiscaal (ophalen of muteren vooringevulde aangifte) 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?) octrooien	4

3.4 Indicaties voor een ander betrouwbaarheidsniveau en bepaling van het niveau

Er zullen omstandigheden kunnen zijn waardoor het ‘standaard’ betrouwbaarheidsniveau dat voortvloeit uit het model in de vorige paragraaf voor een bepaalde dienst niet voldoende zekerheid biedt of juist te zwaar uitvalt. In dat geval kan een toetsing van de dienst plaatsvinden aan de hand van het uitgebreide classificatiemodel in bijlage 4.

Indicaties voor toepassing van het model in de bijlage kunnen zijn dat in het proces van dienstverlening (in de back office) waarborgen zijn ingebouwd (bijvoorbeeld door verificatie van gegevens bij andere overheidsorganisatie of bij basisregistraties, of doordat in de software waarmee de dienst wordt aangevraagd al controlefunctionaliteiten zijn ingebouwd) die de mogelijkheden van fraude, misbruik of oneigenlijk gebruik door het malverseren met identiteiten tot een minimum beperken.
Ook kunnen ervaringsgegevens over verlening van soortgelijke diensten (neergelegd in risico- of handhavingsprofielen) een indicatie geven over de wenselijkheid van een hoger of lager niveau.

Bijlage 1 Relevante wet- en regelgeving

1. Algemene wet bestuursrecht

Met de Wet elektronisch bestuurlijk verkeer (Webv)[17] 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.[18]

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. Voor de uitzonderingen zie § ….
- 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

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

niet. Wel wordt een aantal gevallen genoemd waarin vormvoorschriften die tot gebruik van papier lijken te leiden, ook elektronische 'verzending' toelaten, zoals 'per brief' (kan ook via de mail) of 'aanplakken' (kan ook door publicatie op een site). Deze uitzondering zal 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'.[19]

De wetgever beoogt met de eis van betrouwbaarheid en vertrouwelijkheid uitdrukking te geven aan de zogenaamde *algemene beginselen van behoorlijk IT-gebruik*.[20] 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 de relatie tussen niveaus en middelen geïllustreerd.

Fout! Objecten kunnen niet worden gemaakt door veldcodes te bewerken.

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

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

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.[21] 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.[22]
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 betreffen. Ze zijn dan ook vaak niet in een besluit of regeling van het bestuursorgaan vastgelegd. Indien een bestuursorgaan het beginsel van nevenschikking hanteert, en het elektronisch berichtenverkeer een aanvulling vormt op de conventionele weg, kunnen de eisen gezien worden als beleidsinvulling. Indien een burger of bedrijf zich daaraan niet wil conformeren, heeft hij de keuze om van de conventionele (schriftelijke) weg gebruik te maken.

Waar het elektronisch berichtenverkeer expliciet verplicht is gesteld, met uitsluiting van de conventionele, papieren weg, ligt het in de rede om deze nadere eisen in algemeen verbindende voorschriften op te nemen. Het verplichte karakter, en de consequenties die eventueel aan niet naleving van die verplichtingen verbonden worden, rechtvaardigen een wettelijke grondslag.

Dezelfde lijn kan worden gevolgd ten aanzien van betrouwbaarheidseisen aan de elektronische weg. Als deze 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 bepaalt de tijdstippen van verzending en ontvangst van een elektronisch bericht. Hierop wordt, gelet op de geringe betekenis van dit artikel voor dit kader, niet verder ingegaan.

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

2. Wet elektronische handtekeningen (Weh)

Met de Wet elektronische handtekeningen[23] (hierna: Weh) is de Europese richtlijn over een gemeenschappelijk kader voor elektronische handtekeningen geïmplementeerd.[24] 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.

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.[25]

Deze definitie is behoorlijk ruim. Ook een ingescande handgeschreven handtekening kan hiermee als elektronische handtekening worden aangemerkt.[26] 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

[23] Stb. 2003, 199.
[24] 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.
[25] Kamerstukken II 2001/02, 28 483, nr. 3, p. 15.
[26] Kamerstukken II 2000/01, 27 743, nr. 3, p. 2.

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.

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. Tevens zijn telefoonnummers, kentekens van auto's, postcodes met huisnummers en het BSN, persoonsgegevens.

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.[27] Hoewel dit normatieve advies stamt uit 2001 is het nog steeds relevant en bruikbaar als norm voor het bepalen van de toepasselijke risicoklassen.

Klasse	**Aard van de gegevens**
Geen persoonsgegevens	De gegevens zijn niet te herleiden tot geïdentificeerde of identificeerbare persoon.

[27] 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

Risicoklasse 0	Openbare persoonsgegevens waarvan algemeen aanvaard is dat deze geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures en publieke internetsites.
Risicoklasse I	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	Bijzondere persoonsgegevens als genoemd in artikel 16 Wbp, financieel-economische gegevens in relatie tot de betrokkene, grote hoeveelheid persoonsgegevens uit lagere risicoklasse.
Risicoklasse III	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.

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 worden 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. Het toepassen van deze handreiking kan gezien worden als een onderdeel van dit beleid.
De secretatis-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.[28]
Door het burgerservicenummer te koppelen aan DigiD, kan de burger zich op een betrouwbare manier elektronisch kenbaar maken aan de overheid.

6. Wetboek van Burgerlijke Rechtsvordering

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

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

Artikel 156a
1. Onderhandse akten kunnen op een andere wijze dan bij geschrift worden opgemaakt op zodanige wijze dat het degene ten behoeve van wie de akte bewijs oplevert, in staat stelt om de inhoud van de akte op te slaan op een wijze die deze inhoud toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de akte 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**

[28] Ontleend aan memorie van toelichting Wabb.

drager in de Wet op het financieel toezicht.[29] Duurzame drager wordt in artikel 1:1 van die wet gedefinieerd als: een hulpmiddel dat een persoon in staat stelt om aan hem persoonlijk gerichte informatie op te slaan op een wijze die deze informatie toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de informatie kan dienen, en die een ongewijzigde reproductie van de opgeslagen informatie mogelijk maakt.
Deze eis gaat niet zo ver dat degene die de akte opmaakt een ongewijzigde reproductie van de opgeslagen informatie moet garanderen. 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 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.

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

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).[30]
- 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

PM nog uitwerken: paragraaf over tijdstip van verzending en ontvangst, wat wordt van burger gevergd aan zorg dat het bericht ook ontvangen wordt, wat te doen als systeem van het bestuursorgaan in storing is, wat te doen bij gebruik van generieke faciliteiten (bv. Digipoort).

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

[30] 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).

adres nog niet betekent dat daarmee voor alle mogelijke handelingen de elektronische weg openstaat.[31] Dit vereist een actieve kenbaarmaking door de overheidsorganisatie, bijvoorbeeld door middel van:

- Een brochure.
- Een mededeling in een huis-aan-huis-blad of op een website, waarin wordt aangegeven waar op het internet aanvragen voor bepaalde vergunningen kunnen worden gedaan, klachten kunnen worden ingediend, etc.
- Een openstellingsbesluit, zoals de Belastingdienst destijds heeft vastgesteld.[32]

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.[33] In het verlengde daarvan zal waarschijnlijk ook een definitie van 'schriftelijk' die zich uitdrukkelijk beperkt tot 'schrifttekens op papier' niet als expliciete uitsluiting van elektronisch verkeer gelden.[34] De MvT bij de Wet elektronisch bestuurlijk verkeer onderstreept dit: "Vormvoorschriften staan dus niet zonder meer aan elektronisch verkeer in de weg." Als voorbeeld noemt de wetgever de vereisten van een brief of publicatie in de Staatscourant; 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: "zijn verblijf in persoon te melden …" Zie ook art. 71 en artikel 74, tweede lid. Boek 1 BW, art. 43, derde lid, over ondertrouw. Kentekenregeling art. 25a, tweede lid. Waterschapsreglement art. 50.2, eerste lid.	De eis "in persoon" te verschijnen is een voorbeeld van een vormvoorschrift dat afhandeling op basis van een elektronisch bericht verhindert conform artikel 2.13, tweede lid, onderdeel b, Awb.
Waarmerken	Regeling LNV subsidies, Bijlage bij artikel 1:14e	Dit gebruik in de papieren wereld is vergelijkbaar met de cryptografische koppeling van een elektronische handtekening aan hetgeen getekend wordt op basis van een hash.
verifieert identiteit van de persoon door middel van visuele controle	Besluit elektronische handtekening art. 2, eerste lid, onderdeel g	De verplichtingen aangaande de uitgifte van een gekwalificeerd certificaat (STORK niveau 4), waarbij iemand in persoon (face tot face) moet worden geïdentificeerd zijn een evident voorbeeld van een

[31] Kamerstukken II 2001/02, 28 483, nr. 3, p. 13.
[32] Openstelling elektronische bestuurlijk verkeer met de belastingdienst, 27 april 2005, nr. CPP 2004/2807M, Stcrt. 87, p. 12.
[33] CBB 4 juni 2008, LJN BD4039 (Aanvraag MEP-subsidie).
[34] Zie artikel 1 van de Pensioenwet. Overigens is de MvT bij deze wet ook niet geheel eenduidig in de mate waarin deze definitie aan elektronisch verstrekken van informatie in de weg staat.

		vormvereiste dat toepassing van een elektronisch proces verhindert.
PM aanvullende input van de gebruikers met betrekking tot wet- en regelgeving in hun domein		

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 leestekens 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. Het e-mail adres van de verzender bevat echter voor een overheidsdienst geen betrouwbare gegevens om vast te stellen wie de verzender is op basis van een basisregistratie en een e-mail is veelal niet ondertekend (met een elektronische handtekening in de zin van art … [ongeacht of deze gekwalificeerd is of niet]). Een e-mail waarin verzender zijn naam en adres vermeldt staat dus gelijk aan een niet ondertekend schriftelijk stuk. Antwoord kan alleen gegeven worden aan de verzender op diens e-mail adres indien hij of zij heeft aangegeven elektronisch bereikbaar te zijn of aan het in de e-mail vermelde andere adres. In geval dat de authenticatie onvoldoende is voor het behandelen van de ingediende zaak kan aan de verzender middels antwoord op de e-mail verzocht worden zich nader via een ander middel te laten authenticeren. Een overheidsdienst zal binnenkomende e-mail van burgers en bedrijven even goed moeten archiveren als andere

		schriftelijk ontvangen stukken en deze archieven voldoende moeten beveiligen.
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

PM
elektronische aangifte voor ondernemers
andere 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 als zodanig door partijen geaccepteerd wordt.	Kopie van ondertekend document, print van document met gescande handtekening, elektronisch bestand die een gescande handtekening bevat.
Geavanceerd	Alleen indien er duidelijke gronden zijn anders dan de in BW boek 3 art 15a derde lid uitgesloten gronden om deze handtekening onvoldoende betrouwbaar te vinden zijn de rechtsgevolgen niet gelijk aan de handgeschreven handtekening	In de papieren situatie wordt een ondertekening met pen op papier met eventueel paraaf op iedere pagina gehanteerd, waarbij de "vasthechting" versterkt kan worden door de handtekening deels over de gedrukte tekst te plaatsen.
Gekwalificeerd	Rechtsgevolgen zijn gelijk aan handgeschreven handtekening voor dezelfde situatie	Idem als boven met extra waarborgen zoals een notaris die een handtekening valideert tegen het reisdocument en de GBA gegevens.

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

Wettelijke formulering	functie van de handtekening	soort elektronische handtekening
… wordt ondertekend…	identificatie van de zender	gewone of geavanceerde
…	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 Uitgebreid classificatiemodel

1 Inleiding

Indien in een specifiek geval twijfel bestaat over het uit de menukaart in hoofdstuk 3 voortvloeiende betrouwbaarheidsniveau of er indicaties zijn om een nader niveau te kiezen, kan met behulp van het uitgebreide classificatiemodel in deze bijlage een specifieke inschaling worden gemaakt.
Deze inschaling wordt opgebouwd door van een dienst eerst de onderstaande losstaande aspecten te bekijken en per aspect vast te stellen in welke van de geformuleerde categorieën deze past. Vervolgens kan worden bepaald – met behulp van de tabel in onderdeel 4 van deze bijlage – welke (combinaties van) categorieën tot welke minimaal vereiste betrouwbaarheidsniveaus leiden en waarop die minimale vereisten gebaseerd zijn. Het beschouwen van losstaande aspecten reduceert de complexiteit en leidt ertoe dat duidelijk zichtbaar wordt welke aspecten van een dienst een bepaalde eis aan het betrouwbaarheidsniveau stellen.
De aspecten zijn ook uitgesplitst omdat verschillende combinaties van aspecten tot hetzelfde betrouwbaarheidsniveau kunnen leiden. Een lagere score op het ene aspect kan bijvoorbeeld gecompenseerd worden door een hogere scoren op een ander aspect. Ook in STORK wordt deze benadering gevolgd.

2 Voor classificatie te beoordelen aspecten

A. Wie is de betrokkene?
Dit aspect beoordeelt of de dienst voor breed publiek is of dat het een dienst betreft die aan een belanghebbende (in de zin van de Awb) geleverd wordt. De code IP staat voor Informatie over de betrokken Persoon.

Criteria	IP1	IP2	IP3	IP4
A1. De Betrokkene is een willekeurige gebruiker.	●			
A2. De betrokkene is zelf tevens Belanghebbende en wordt ergens in het proces waar de Dienst betrekking op heeft geïdentificeerd.	●	●		

Voorbeelden	
A1	Iemand die met een browser een webpagina opvraagt of iemand die een e-mail verzendt in de situatie dat het e-mailadres waarvandaan verzonden is geen enkele rol speelt en ook niet gebruikt hoeft te worden om na afronding van de Dienst een antwoord te mailen.
A2	Een elektronische aangifte inkomstenbelasting. De gegevens in de aangifte worden in het vervolgproces gekoppeld aan de gegevens die de Belastingdienst over de persoon met het desbetreffende BSN bezit.

B. Identificatie van belanghebbende
Het gaat hier om de vraag hoe belangrijk het is om zeker te weten aan welke belanghebbende de dienst geleverd wordt. Hoe ernstig is het als deze niet getraceerd kan worden of een ander zich namens de belanghebbende heeft uitgegeven? De code IB staat voor Identificatie van de Betrokkene of Belanghebbende.

Criteria	IB1	IB2	IB3	IB4	IB5
B1. Er is geen sprake van een belanghebbende of betrokkene die geïdentificeerd moet worden op basis van gegevens in een basisregistratie. Mogelijk is sprake van identificatie van de betrokkene op basis van IP-adres, cookie of andere soortgelijke technieken die werken zonder expliciete acties van betrokkene en die slechts beperkte identificatie geven.	●				
B2. Als B1 waarbij daarnaast een identificatie plaats vindt die wel expliciete actie van de betrokkene vraagt, bijvoorbeeld het kiezen van een eigen gebruikersnaam in een portal of het opvragen van een	●	●			

inlogcode via een e-mailadres waaraan geen verdere eisen worden gesteld (en dat dus een min of meer anoniem webmailadres kan zijn).					
B3. De belanghebbende wordt geïdentificeerd op basis van persoonsgegevens, niet zijnde het BSN (maximaal risicoklasse I en beperkte hoeveelheid). Authenticatie hiervan is niet noodzakelijk binnen de dienstafname.	●	●	●		
B4. De belanghebbende wordt geïdentificeerd op basis van een pseudoniem waarvan alleen achteraf, op basis van vermoeden van misbruik of fraude, de relatie met BSN of andere identificerende persoonsgegevens gelegd kan worden.	●	●	●		
B5. De belanghebbende wordt binnen de dienstafname geïdentificeerd op basis van BSN. Mocht het een natuurlijk persoon betreffen die (nog) geen BSN heeft dan wordt het BSN vervangen door een als uniek identificerende combinatie van persoonsgegevens die in basisregistratie zijn (of worden) opgenomen en op basis van derde bron geverifieerd worden in het proces.	●	●	●	●	
B6. Als B5 waarbij de dienstafname een expliciete wilsuiting vergt en de belanghebbende zijn wilsuiting met een handtekening bevestigt	●	●	●	●	●

Voorbeelden	
B1	Iemand die met een browser een webpagina opvraagt (als A1) of iemand die een e-mail verzendt in de situatie dat het e-mailadres waarvandaan verzonden is geen enkele rol speelt en ook niet gebruikt hoeft te worden om na afronding van de Dienst een antwoord te mailen.
B2	Een gepersonaliseerd webportal waarvoor iemand een zelfgekozen gebruikersnaam aanmaakt en waarbij onder die naam zijn gebruikersinstellingen worden opgeslagen. Als de gebruikersnaam kwijt is, kan gewoon een nieuwe aangemaakt worden met als enige gevolg dat de gebruikersinstellingen opnieuw ingevuld moeten worden.
B3	Een webformulier voor het maken van een afspraak waarin iemand zijn voornaam, achternaam en het telefoonnummer waar hij of zij te bereiken is, invult.
B5	Een webformulier waarop het eigen BSN wordt ingevuld en waarbij vervolgens de bijbehorende NAW gegevens uit de GBA opgehaald worden.
B6	*nog goed voorbeeld zoeken, inschrijven Handelsregister lijkt een voorbeeld*

C. Aard van de gegevens die de betrokkene verstrekt in kader van de dienstafname
Dit aspect beoordeelt de gegevens die door de betrokkene in het kader van het afnemen van de dienst verstrekt worden. Indien het een elektronische dienst betreft is dit inclusief de gegevens die in het kader van elektronische authenticatie verstrekt worden. Gegevens die eerder verstrekt zijn, bij een eerdere dienstafname en die in te zien zijn vallen onder aspect D. Er wordt van uitgegaan dat verbindingen dusdanig beveiligd zijn dat alleen de betrokkenen zelf deze gegevens ziet. De code GI staat voor Gegeven Input.

Criteria	**GI1**	**GI2**	**GI3**	**GI4**	**GI5**
C1. Er worden geen gegevens verstrekt die direct tot de persoon te herleiden zijn, of alleen van Wbp risicoklasse 0, of ten hoogste gegevens die voortkomen uit normaal elektronisch verkeer zoals IP-adres, cookie-gegevens e.d.	●				
C2. Er worden gegevens verstrekt die tot een persoon te herleiden zijn zoals een adres, een persoonlijk e-mailadres, naam of telefoonnummers. Het betreft gegevens die in het algemeen ook gemakkelijk via andere kanalen te achterhalen zijn. Deze gegevens zijn praktisch noodzakelijk voor het uitvoeren van het proces (bijvoorbeeld bezorgadres van nieuwe vuilniscontainer). Het betreft Wbp risicoklassen 0 en I.	●	●			

C3. Het BSN of een combinatie van persoonsgegevens die betrokkene uniek identificeert wordt verstrekt.	●	●	●		
C4. Er worden gegevens verstrekt van categorie C3 met daarbij gegevens die in combinatie met redelijk zekere identificatie van de betrokkene de privacy schenden of concurrentiegevoelige, koersgevoelige of andere economisch gevoelige gegevens betreffen. Nota bene dit geldt zowel in de context van privépersonen als in de context van bedrijven en instellingen.	●	●	●	●	
C5. Er worden gegevens van Wbp risicoklasse II of hoger verstrekt of vergelijkbaar.	●	●	●	●	
C6. Er worden gegevens over verblijfplaats op een bepaald tijdstip verstrekt. Dit kan bijvoorbeeld interessante informatie voor inbrekers opleveren …	●	●	●	●	
C7. Risicoklasse III. Buiten scope.	●	●	●	●	●

Voorbeelden bij criteria	
C1	De gegevens die (voor gewone gebruikers ongemerkt) verstrekt worden wanneer men met een browser een webpagina opvraagt (als A1). Dit zijn onder andere: - IP-adres - Kenmerken van de gebruikte computer (hardware en software) - Geïnstalleerde browser plugins - Vorige websites die bezocht zijn (zie whattheinternetknowsaboutyou.com) - Favorieten - Cookies - Varianten op cookies die moeilijker te verwijderen zijn (bv. Flash cookies) Nota bene: dit is zoveel informatie dat het bij normaal gebruik veelal voldoende is om een gebruiker uniek te herkennen, het zijn echter geen persoonsgegevens. Gebruikers die persoonsgegevens die ingevuld zijn op eerdere websites opslaan in hun browser stellen deze wel bloot aan het achterhalen door andere website van persoonsgegevens.
C2	Er wordt een formulier ingevuld met daarop een e-mail adres dat eigen naam bevat (persoonsgegevens).
C3	Als B4. Een webformulier waarop het eigen BSN wordt ingevuld en waarbij vervolgens de bijbehorende NAW gegevens uit de GBA opgehaald worden, of een webformulier waarop iemand naam, adres, woonplaats, geboortedatum en geboorteplaats invult.
C4	Economisch gevoelige gegevens betreffen bv. het feit dat iemand een vergunning aanvraagt, bepaalde goederen exporteert, bepaalde medische voorzieningen gebruikt, cliënt is van de reclassering. Concurrentie- en koersgevoelige gegevens kunnen aan de orde zijn in aanbestedingsprocedures.
C5	Uit de aard van de dienst volgt een risicoklasse II verband, bijvoorbeeld een aanvraag voor schuldsanering gepaard gaand met identificatie op BSN.
C6	Voorbeelden van dergelijke diensten zijn nog niet voorhanden; het aspect anticipeert op de risico's van informatielekken bij locatie- en tijdgebonden diensten.

D. Aard van de gegevens die na toegang getoond worden

Dit aspect betreft de gegevens die getoond worden nadat de identificatie en authenticatie van de betrokkene of belanghebbende heeft plaatsgevonden. Het gaat dus ook over de aard van de gegevens die in handen van de verkeerde persoon vallen indien de authenticatie omzeild kan worden. De code GO staat voor Gegeven Output.

Criteria	**GO1**	**GO2**	**GO3**	**GO4**	**GO5**
D1. Het betreft algemene openbare gegevens. Iedere betrokkene krijgt exact dezelfde gegevens te zien. Het kan zijn dat deze gegevens een geldigheidsdatum hebben, of gelden voor een bepaald gebied of een andere inperking, deze inperking is echter op geen enkele manier afhankelijk van wie de betrokkene is.	●				

D2. Het betreft gespecificeerde openbare gegevens. Ten behoeve van deze specificatie heeft de betrokkene gegevens verstrekt die niet als persoonsgegevens beschouwd kunnen worden en waarover niet zeker is dat ze waar zijn of betrekking hebben op de betreffende betrokkene.	●	●			
D3. De gegevens die getoond worden zijn tot een persoon of een zeer beperkte groep personen te herleiden (conform criteria Wbp beperkte hoeveelheid en risicoklasse I of lager) of gepersonaliseerd weergegeven op basis van door de betrokkene verstrekte persoonsgegevens.	●	●	●		
D4.De gegevens die getoond worden zijn eigendom van een derde, zijn niet openbaar gepubliceerd of vallen onder een licentie of ander recht. Overheidsorganisaties dienen vanuit algemene zorgvuldigheid toegang tot deze gegevens door personen die geen reden (vanuit een overheidstaak of wet) hebben om deze gegevens in te zien af te schermen.	●	●	●		
D5. Tenminste één van de getoonde gegevens valt in Wbp risicoklasse II of hoger of betreft concurrentiegevoelige, koersgevoelige of andere economisch gevoelige gegevens. Inzage van deze gegevens door een derde,hetzij door een fout (onopzettelijk), hetzij door bewuste poging deze gegevens te bemachtigen is een privacy inbreuk en kan leiden tot bezwaar bij of schadevergoeding door de veroorzaker. De werkelijke onmiddellijke schade bij één geval van onterechte inzage is beperkt.	●	●	●	●	
D6. Tenminste één van de getoonde gegevens valt in Wbp risicoklasse III. Inzage van deze gegevens door een derde, hetzij door bewuste poging deze gegevens te bemachtigen, hetzij door een fout is een ernstige inbreuk.	●	●	●	●	●

Voorbeelden bij criteria	
D1	De gegevens op een algemene informatieve website, bijvoorbeeld www.denhaag.nl of http://www.denhaag.nl/home/bewoners/loket/to/Grofvuil-of-afval-wegbrengen.htm
D2	Algemene informatie voor een bepaalde door de gebruiker opgegeven categorie, bijvoorbeeld op de website van de KvK, indien daar op basis van postcode een regio gekozen wordt: http://www.kvk.nl/?postcode=6522
D3	Gegevens die na inloggen beschikbaar zijn op sites als mijndenhaag.nl of mijnoverheid.nl.
D4	In het kader van milieu-inspecties verstrekte gegevens over bedrijfssystemen.
D5	De gegevens voor de vooringevulde aangifte van de inkomstenbelasting die opgevraagd worden door het aangifteprogramma.
D6	Medische gegevens (in een elektronisch patiëntendossier bij zorgverlener, of regionaal).

E. Gebruik van verstrekte gegevens binnen de dienstafname

Dit aspect beoordeelt wat de rol is in het vervolgproces van (identificerende) gegevens die expliciet door de betrokkene worden versterkt als onderdeel van het afnemen van de dienst en tevens wat de rol is van gegevens die impliciet worden verstrekt als onderdeel van een elektronische authenticatie. De code GG staat voor Gebruik Gegevens.

Criteria	**GG1**	**GG2**	**GG3**	**GG4**	**GG5**
E1. Er worden geen identificerende gegevens gebruikt binnen de dienstafname.	●				

E2. Identificerende gegevens worden enkel gebruikt ten opzichte van de eigen registratie, c.q. binnen de dienst zelf en leiden niet tot bevraging van of wijzigingen in andere systemen of organisaties.	●	●			
E3. Identificerende gegevens wordt gebruikt om niet-authentieke gegevens van een reeds in basisregistratie opgenomen object te wijzigen	●	●	●		
E4. Identificerende gegevens worden gebruikt om authentieke gegevens in een basisregistratie te wijzigen, maar niet om een nieuw object te creëren dat authentieke gegevens bevat of een bestaand object met authentieke gegevens te beëindigen (waaronder samenvoeging met ander object)	●	●	●	●	
E5. Identificerende gegevens worden gebruikt om nieuwe objecten met authentieke gegevens aan te maken in een basisregistratie (of bestaande objecten te beëindigen of samen te voegen met ander object)	●	●	●	●	●

Voorbeelden bij criteria	
E1	Het zoeken naar een bepaalde zoekterm in de actuele versie van Nederlandse wet- en regelgeving op www.overheid.nl
E2	Het zoeken op handelsnaam in het gratis en openbare deel van het Handelsregister op www.kvk.nl of het via www.rdw.nl opvragen van voertuiggegevens op basis van kenteken.
E3	Het doorgeven aan het Handelsregister van een wijziging van de functie van een bestuurder van een BV.
E4	Het doorgeven van de verhuizing van een vestiging aan het Handelsregister, doorgeven adreswijziging van natuurlijk persoon in de GBA.
E5	Het inschrijven van een eenmanszaak in het Handelsregister of het doen van een aangifte van geboorte door één van de ouders.

F. Aard van het vervolgproces
Dit aspect beoordeelt wat nadat de dienst is afgenomen aan mogelijke vervolgstappen wordt gezet. De code VP staat voor Vervolg Proces.

Criteria	**VP1**	**VP2**	**VP3**	**VP4**	**VP5**
F1. Er is geen vervolgproces. Uit de dienstafname volgt geen rechtsgevolg noch enig vervolgproces of statuswijziging.	●				
F2. In het vervolgproces is het wenselijk dat de betrokkene bereikt kan worden met een mededeling over statusvoortgang, onverwachte wijzigingen of andere vervolgstappen. Indien de betrokkene niet daadwerkelijk en/ of niet voor een bepaald tijdstip bereikt wordt op het vastgelegde adres of nummer dan zijn de gevolgen daarvan gering en leidt dit niet tot rechtsgevolg.	●	●			
F3. Het vervolgproces leidt tot feitelijk handelen: er wordt een bezoek afgelegd, iets wordt fysiek bezorgd, er wordt een afspraak ingepland.	●	●	?		
F4. Het vervolgproces is administratief en vereist zekerheid omtrent BSN van de betrokkene en leidt tot rechtsgevolgen voor de betrokkene	●	●	●		
F5. Het vervolgproces heeft rechtsgevolgen die verder gaan dan een enkele dienstafname maar het functioneren van de belanghebbende betreffen.	●	●	●	●	

Voorbeelden bij criteria	
F1	Als E2 (of E1). Het betreft enkel het zoeken naar en opvragen van informatie die vervolgens elektronisch verstrekt wordt. Als E3 waarbij de betaling onderdeel is van het afnemen van de dienst doordat een creditcard of IDEAL transactie gedaan wordt voorafgaand aan daadwerkelijke levering van het gevraagde product.
F2	Als E3 waarbij er na de levering in separaat proces een factuur gestuurd wordt (en waarbij het totale bedrag beperkt is). Bijvoorbeeld de aanvraag van een nieuwe GFT container (de schade van het incidenteel bezorgen op verkeerde adres is gering). Een dienst waarbij de persoon in kwestie nadien bereikt moet kunnen worden, bijvoorbeeld het indienen van een klacht.
F3	Het inplannen van een afspraak bij het kantoor van de gemeente, het inplannen van een bezoek van iemand die een reparatie komt uitvoeren, het bezorgen van een vuilcontainer.
F4	De aangifte inkomstenbelasting of de tenaamstelling van een voertuig op naam van een rechtspersoon.
F5	Van deze situatie is nog geen concreeet voorbeeld te geven. Gedacht kan worden aan een voorziening voor het elektronische aanvragen van ontslag door een werkgever, waarbij de gevolgen van het aanvragen van ontslag voor de verkeerde persoon aanzienlijk zijn.

3 Risicoverhogende en – verlagende aspecten

Voordat op basis van bovenstaande classificatie per aspect een vaststelling van het betrouwbaarheidsniveau volgt, worden aspecten bekeken die het risico verhogen of verlagen. Deze kunnen globaal spelen of op een specifiek aspect betrekking hebben.

Risicoverhogende aspecten

Risicoverhogende factoren moeten niet te lichtvaardig worden toegepast. Het ligt het voor de hand dat aan het in aanmerking nemen van risicoverhogende aspecten een argumentatie ten grondslag ligt die voortvloeit uit een afhankelijkheden en kwetsbaarheidsanalyse (A&K-analyse). Deze lijn wordt ook gehanteerd in het VIR.

Als risicoverhogende aspecten zijn in het algemeen te definiëren:

- RH1. Bestuurlijk risico
  PM toelichten
- RH2. Imago
  PM toelichten
- RH3. Risico dat slechte beveiliging leidt tot problemen in ander overheidsproces (slechte info in basisregistratie heeft netwerkeffect etc.)
- RH4. Herhaalfactor
  Het gaat hier om de situaties dat de schade indien het één keer verkeerd gaat beperkt is, maar bij herhaling (die met een elektronische dienst vaak in korte tijd, op afstand en in een groot aantal gevallen mogelijk is) grote schade veroorzaakt.

Risicoverlagende aspecten

Per aspect of in het algemeen gesproken kunnen er omstandigheden zijn of maatregelen zijn ingericht die het risico in de praktijk kleiner maken. Deze maatregelen kunnen ertoe leiden dat een lager betrouwbaarheidsniveau volstaat.

LO1. 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.

LO2. 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.

LO3. 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.

LO4. Er is sprake van voortdurende en actieve monitoring waarmee voorkomen wordt dat een dienst in korte tijd heel vaak benaderd wordt door dezelfde betrokkene. Ook het bijhouden van risico- of handhavingsprofielen kan hieronder worden geschaard.
Dit verlaagt het risico op aspect F3 en op het op grote schaal beschikbaar komen van vertrouwelijke gegevens.

aspectscore	verlaging	resultaat aspectscore
IB3	LO1 fysieke melding	IB2
IB4	LO2 fysieke melding met ID	IB3
IB4	LO4 actieve monitoring	IB3
GI3	LO2 fysieke melding met ID	GI2
GG4	LO2 fysieke meldeing met ID	GG3
GG4	LO4 actieve monitoring	GG3
IB5	LO3 bewijsstukken	IB4
GG5	LO4 actieve monitoring	GG4

4 Vereiste betrouwbaarheidsniveaus voor diensten

Op basis van de boven gedefinieerde aspecten kan van een dienst bepaald worden hoe deze geclassificeerd wordt op deze punten. Het totaal van deze aspecten bepaalt het betrouwbaarheidsniveau dat vereist wordt. Voor deze betrouwbaarheidsniveaus (aangeduid als D1 tot en met D4) is aangesloten bij de vier betrouwbaarheidsniveaus als gedefinieerd in STORK. In hoofdstuk 2 zijn de STORK-niveaus toegelicht.

De classificatie in de onderstaande tabel kan als volgt gehanteerd worden. Voor een bepaalde dienst wordt gekeken of er tenminste één aspect is dat onder betrouwbaarheidsniveau 4 (D4) valt (c.q. in de meest rechtse kolom staat). Zo ja, dan is ten minste betrouwbaarheidsniveau 4 vereist. Zo nee, dan wordt gecontroleerd of er tenminste één aspect is dat onder betrouwbaarheidsniveau 3 valt enzovoorts.

Criterium	geen	D1 Minimaal	D2 Beperkt	D3 Redelijk	D4 Hoog
Wie is de betrokkene?	IP1	IP2			
Identificatie van belanghebbende	IB1	IB2	IB3 IB4	IB4	IB5
Aard van de gegevens die de betrokkene verstrekt in kader van de dienstafname	GI1	GI2	GI3	GI4	GI5
Aard van de gegevens die na toegang getoond worden	G01	GO2	GO3	GO4	GO5
Gebruik van identificerende gegevens binnen de dienstafname	GG1	GG2	GG3	GG4	GG5
Aard van het vervolgproces	VP1	VP2	VP3	VP3	VP4

Bijlage 4 Begrippenkader

Elektronisch verkeer (Elektronische communicatie, elektronische berichten)

Conventioneel verkeer (communicatie, berichten)

Identificatie

Authenticatie

Autorisatie

Toegang verlenen

Dienst: Een dienst is in de context van deze handreiking een dienst die door een overheidsdienstverlener in het kader van een bepaalde overheidstaak wordt aangeboden.

De volgende eigenschappen van diensten zijn daarbij van belang:

- Een dienst betreft een interactie tussen een welgedefinieerde overheidsinstantie (de dienstaanbieder) en een welgedefinieerde andere persoon (de dienstafnemer).
- Een dienst is een uitvloeisel van een overheidstaak conform wet- en regelgeving
- Als begin en eind van de dienst wordt genomen al hetgeen hoort bij één onafgebroken transactie met de dienstafnemer. Indien de dienstafnemer voordat de volgende stap genomen wordt zodanig lang moet wachten dat hij of zij tussentijds andere zaken doet (uren, werkdagen, weken) dan is het vervolg een andere dienst.
- Een dienst kan leiden tot een vervolgproces of tot afname van andere diensten.
- Diensten kunnen onderling gerelateerd zijn
- Er zijn situaties waarin dienstafnemers meerdere diensten afnemen om een bepaald samenhangend resultaat te bereiken.

Betrouwbaarheidsniveau: Een betrouwbaarheidsniveau is een niveau van zekerheid dat de geclaimde beveiliging van een bepaald product ook daadwerkelijk wordt geboden.

Deze algemene definitie geldt evenals zekerheidsniveau als vertaling van assurance level zoals gebruikt in relatie tot de Common Criteria (zie Informatiebeveiliging onder controle, O. Overbeek e.a., ISBN 978-90-430-0962-7). In deze handreiking wordt het begrip specifieker afgebakend.

Er is sprake van een "vereist betrouwbaarheidsniveau": een bepaalde dienst vereist een bepaald betrouwbaarheidsniveau. Waar hiervoor kortweg gesproken wordt van "betrouwbaarheidsniveau van een dienst" dient dit niet verward te worden met het geheel aan beveiligingsmaatregelen dat nodig is om betreffende dienst zorgvuldig uit te voeren, bij dat geheel horen immers ook andere maatregelen dan maatregelen aangaande de authenticatie van de gebruiker. Waar in wet- en regelgeving sprake is van afhankelijkheden en kwetsbaarheidsanalyses of risicoanalyses wordt in het algemeen dit bredere geheel aan maatregelen bedoeld. Soms wordt voor dat geheel gesproken van beveiligingsniveau. Het betrouwbaarheidsniveau zoals hier gebruikt en zoals in STORK gebruikt is dan een aspect daarvan.

Bij DigiD en DigiD machtigingen wordt de term zekerheidsniveau gehanteerd als synoniem voor betrouwbaarheidsniveau. In het PvE PKI overheid komt de term betrouwbaarheidsniveau voor zonder expliciete definitie. In wet- en regelgeving komen beide termen voor. In alle gevallen worden deze termen gebruikt als vertaling van authentication assurance level zoals dat in STORK wordt gehanteerd. Het betreft derhalve specifiek het niveau van zekerheid aangaande een authenticatie met een bepaald authenticatiemiddel dat op bepaalde manier is uitgegeven.

In STORK en andere raamwerken wordt naast "assurance level" de term "trust level" gehanteerd om niveaus weer te geven die op grond van een risicoanalyse of classificatie vereist worden en dus voorafgaand aan een praktische toepassing bepaald worden, terwijl "assurance levels" altijd de resultante zijn van in praktijk optredende factoren. Dit op zich relevante onderscheid is in deze handreiking alleen terug te vinden doordat — waar dit voor duidelijkheid gewenst is — gesproken wordt van "vereiste betrouwbaarheidsniveaus".

Middel Een authenticatiemiddel of in de context van deze handreiking kortweg middel is een set van attributen op basis waarvan een gebruiker zich kan laten authenticeren gevat in een technische vorm van een bepaald type.

Dit kan een gebruikersnaam - wachtwoord combinatie zijn, een in software opgeslagen certificaat, maar ook een op een smartcard of andere specifieke hardware opgeslagen certificaat.

Persoon: Hetzij een natuurlijk persoon, hetzij een niet natuurlijk persoon.

Natuurlijk persoon: Een individueel menselijk wezen en subject van rechten en drager van plichten.

Wilsverklaring:

Bericht: De term bericht wordt in deze handreiking zeer breed opgevat zodat vrijwel iedere vorm van elektronisch verkeer een bericht kan zijn.

Gebruiker: een gebruiker is een natuurlijk persoon die direct zelf een elektronische dienst afneemt

Belanghebbende: De belanghebbende is de persoon waarop de rechtsgevolgen van een dienst betrekking hebben. Dit is hetzij een natuurlijk persoon, hetzij een niet natuurlijk persoon.

Vertegenwoordiging: De rechtsfiguur die inhoudt dat de rechtsgevolgen van een door een bepaalde partij (de vertegenwoordiger of gemachtigde) in naam van een andere partij (de vertegenwoordigde) met een derde verrichte handeling aan de vertegenwoordigde worden toegerekend. De bevoegdheid tot het verrichten van vertegenwoordigingshandelingen vloeit voort uit hetzij de wet hetzij een volmacht (privaatrecht) hetzij uit een machtiging (bestuursrecht). Zo'n bevoegdheid kan eventueel ingeperkt zijn tot bepaalde rechtshandelingen, of een bepaalde relevante omvang ten aanzien van rechtshandelingen. In privaatrechtelijke context wordt naast het begrip vertegenwoordiger, agent of gevolmachtigde gehanteerd in plaats van gemachtigde.

Gegeven: Een gegeven is een samenhangend stukje informatie dat in een dienst verwerkt wordt. De term wordt hier zeer algemeen gebruikt en is niet beperkt tot gegevens die de gebruiker expliciet zelf opgeeft of inzichtelijk heeft. Het tijdstip waarop een dienstafname gestart wordt is bijvoorbeeld ook een gegeven, of het IP-adres waarvandaan een browser een dienst opvraagt.

Persoonsgegevens: zie Wbp.

Toegang: onder toegang wordt in deze handreiking verstaan de beslissing van de dienstverlener om een gebruiker in het kader van de afname van een bepaalde dienst tot bronnen en zaken toegang te geven. Toegang onderscheidt zich van autorisatie, autorisatie betreft het verleende recht om op enig moment toegang te krijgen op grond van het voldoen aan bepaalde eisen.

Vervolgproces