Een handreiking voor overheidsorganisaties

Betrouwbaarheidsniveaus voor digitale dienstverlening

Versie 5 (2024)

Forum Standaardisatie

Forum Standaardisatie

De overheid wisselt veel digitale gegevens uit. Dit moet betrouwbaar, eenduidig en veilig gebeuren en dat lukt het beste met open ICT standaarden. Het Forum Standaardisatie heeft als taak de overheid hierover te adviseren. Daarnaast stimuleert het Forum samenwerkingsinitiatieven rond standaardisatie. Zo draagt het Forum Standaardisatie bij aan waardengedreven digitalisering.

Het Forum Standaardisatie is een adviescommissie met deskundigen uit diverse overheidsorganisaties, het bedrijfsleven en de wetenschap. Het Forum doet voorstellen aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) en is ook een adviserend orgaan van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, en de minister van Economische Zaken. Het Forum Standaardisatie is ingesteld door het Ministerie van BZK in afstemming met het Ministerie van EZK.

Het Bureau Forum Standaardisatie is het secretariaat van het Forum Standaardisatie. Dit bureau is gehuisvest bij Logius, de dienst digitale overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Voorwoord

Sinds de vorige versie van de Handreiking Betrouwbaarheidsniveaus voor de digitale dienstverlening van de overheid zijn er zeven jaar verstreken. In die tijdsspanne is de digitale wereld enorm veranderd en tegelijk lijkt de tijd te hebben stil gestaan. Vergelijken we de laatste rapportages en conclusies van de nationale commissaris voor de digitale overheid met die van de regeringscommissaris voor de informatiehuishouding van het Rijk, waartussen die zeven jaar ligt, dan lijkt de overheid met dezelfde uitdagingen te worstelen. Zo blijft er in de aanpak sprake van defragmentatie en is een sterkere regie wenselijk. Ook zijn er nog steeds bindende afspraken nodig, die het digitale overheidshandelen vastleggen. En tegelijkertijd is er een enorme ontwikkeling geweest, en hebben de grote techbedrijven een digitale platform economie ontwikkeld en zorgen algoritmes, kunstmatige intelligentie in relatie tot gigantische beschikbare data voor ongekende mogelijkheden. Ten goede en ten kwade zo blijkt uit enkele uit de hand gelopen toepassingen ervan.

De sleutel bij veel van het overheidshandelen ligt in een tweetal zaken: betrouwbare identificatie en authenticatie zijn cruciaal en daarnaast betrouwbare en toegankelijke digitale dienstverlening. Deze nieuwe versie van de Handreiking Betrouwbaarheidsniveaus is belangrijk om hierin de goede weg te vinden. Het Forum Standaardisatie is erin geslaagd om de nodige actualisatie vorm te geven. Het past in de veranderingen, die juridisch zijn gestold in de Wet digitale overheid, de Wet open overheid en de Europese eIDAS verordening. Maar, en dat is mijn vaste overtuiging, er wordt veel meer gevraagd van de overheid. Om het vertrouwen van de burgers niet kwijt te raken zal de overheid zich transparanter en eenduidiger moeten opstellen. Het zou mooi zijn als het nog eens zal komen tot een eigen digitaal platform onafhankelijk van de dominante "*global four*". Ondertussen moet (!) naast transparantie betrouwbaarheid voorop staan. Deze handreiking is een noodzakelijk hulpmiddel daarvoor.

Bas Eenhoorn,
voormalig Digicommissaris

Inhoud

1 Inleiding

Waarom deze handreiking?

1.1 Zorgvuldig het betrouwbaarheidsniveau kiezen

Deze handreiking gaat over betrouwbaarheidsniveaus. Dit document dient in samenhang met de Wet digitale overheid (Wdo) en de Regeling Betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (Regeling) te worden gelezen. De Regeling schrijft voor welk betrouwbaarheidsniveau vereist is voor de verschillende elektronische overheidsdiensten.
De Wdo en de Regeling geven op Nederlands niveau verder invulling aan de Europese eIDAS-verordening. Deze handreiking herhaalt niet wat er al in de wet- en regelgeving staat.

Wel helpen we u met deze handreiking een heldere en transparante keuze te maken voor het betrouwbaarheidsniveau van uw diensten die via een onlinekanaal worden aangeboden, via een vereenvoudigde risicoanalyse. In het bijzonder richten we ons in deze handreiking op digitale identificatie- en authenticatievraagstukken. In mindere mate richten we ons ook op vertrouwensdiensten.

In bijlage 1 is de voor deze handreiking relevante wet- en regelgeving nader toegelicht, zoals de (U)AVG, de Wdo, eIDAS 1.0 en eIDAS 2.0 en de aankomende Elektronische Identiteit Wallet, de NIS2-Richtlijn, het wetsvoorstel voor de Cyberbeveiligingswet en de Wet modernisering elektronisch bestuurlijk verkeer.

1.2 'One size fits all' bestaat niet

Geen hoog of laag niveau

Er zijn veel verschillende digitale overheidsdiensten met verschillende eisen aan de betrouwbaarheid van identificatie en authenticatie. Het is niet mogelijk en wenselijk om voor al die diensten één uniform inlogmiddel vast te stellen voor identificatie, authenticatie en autorisatie.

Algemeen inzetbare oplossingen

Burgers en bedrijven zullen zoals gezegd met verschillende betrouwbaarheidsniveaus te maken krijgen bij verschillende diensten. De rijksoverheid werkt aan algemeen inzetbare oplossingen om gebruikers daarbij te helpen. Voorbeelden daarvan zijn DigiD en eHerkenning.

1.3 Maak uw keuze kenbaar in een regeling

Het is wenselijk om - bijvoorbeeld op uw website - kenbaar te maken wat voor een bepaalde dienst het vastgestelde betrouwbaarheidsniveau is. In de toelichting daarbij onderbouwt u uw keuze, zodat die ook voor gebruikers van de dienst helder is.

1.4 Hoe is deze handreiking tot stand gekomen?

Handreiking vanaf 2011

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

De handreiking is geen statisch product. Sinds de eerste versie wordt de ontwikkeling van e-dienstverlening en van identificatie- en authenticatiemiddelen gevolgd. Bovendien zijn ervaringen van overheidsorganisaties met de handreiking uiterst welkom. Die worden steeds meegenomen in volgende versies. Forum Standaardisatie blijft het beheer en de doorontwikkeling ondersteunen. Het voornemen is om vanaf deze versie 5 deze handreiking met een kortere regelmaat te actualiseren.

In deze geactualiseerde handreiking (versie 5) is alle relevante nieuwe wet- en regelgeving meegenomen. Zo was de Algemene verordening gegevensbescherming (AVG) nog niet van toepassing (2018) op het moment van verschijnen van de vorige Handreiking. En dat geldt ook voor de Baseline Informatiebeveiliging Overheid (BIO) die per 1 januari 2020 de verschillende baselines informatieveiligheid voor diverse groepen overheden verving.

De Klankbordgroep Handreiking Betrouwbaarheidsniveaus houdt handreiking up-to-date

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

Wijzigingen in versie 5

In de huidige versie 5 staat de uitwerking van de eIDAS-verordening in de Wdo en de Regeling centraal. Daarnaast hebben we een geactualiseerde uitwerking gegeven van de verschillende onderwerpen uit de vorige handreiking en enkele nieuwe onderwerpen toegevoegd. Bovendien zijn de bijlagen over wet- en regelgeving en de casuïstiek geactualiseerd.

1.5 Leeswijzer

Hoofdstuk 2-4: de kern

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

Hoofdstuk 5-9: specifieke diensten

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

Bijlagen: Juridisch kader, bronvermelding, en afkortingen en begrippen

Bijlage 1 beschrijft het actuele juridisch kader (relevante wet- en regelgeving). In bijlage 2 vindt u Bronvermelding Verordeningen, wetten en documentatie m.b.t. wetgevingsproces (incl. conceptwetgeving). In bijlage 3 bevat een lijst met veel gebruikte afkortingen en begrippen opgenomen.


XLE10-10M1

2 Afbakening en context

Waar gaat deze handreiking over?

De betrouwbaarheid van de digitale dienstverlening van de overheid is een groot en complex domein. Immers, de taken van verschillende delen van de overheid verschillen essentieel van elkaar. We kunnen dit domein onmogelijk geheel binnen één handreiking behandelen. In dit hoofdstuk maken we duidelijk waarop we ons wel en niet richten.

Bij de ontwikkeling en het gebruik van elektronische diensten zijn er ook meer onderwerpen van belang dan de eIDAS-verordening beschrijft. Daarbij gaat het bijvoorbeeld om machtigingen, applicatie¬applicatieverkeer en eenmalig inloggen. Hiervoor zijn nauwelijks algemeen geaccepteerde standaarden voorhanden voor een indeling in betrouwbaarheidsniveaus. In deze handreiking geven we daar een nadere invulling aan.

Binnen deze 'afbakening' gaan we ook kort in op relevante trends en ontwikkelingen. Definities van begrippen vindt u in bijlage 3.

2.1 Afbakening

2.1.1 Om welke diensten gaat het?

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

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

2.1.2 Alleen voor individuele diensten

Met deze handreiking helpen we vast te stellen wat het vereiste betrouwbaarheidsniveau is voor één bepaalde dienst. Natuurlijk kunt u meer diensten aanbieden. Daarvoor komt u wellicht conform de risicoanalyse in deze handreiking uit op verschillende betrouwbaarheidsniveaus. Het toepassen van risico mitigerende maatregelen in uw dienst kan aanknopingspunten bieden om het aantal betrouwbaarheidsniveaus voor uw organisatie te beperken.

2.1.3 Onderscheid tussen publiek en privaat vervaagt

Zowel digitale diensten als digitale identificatie- en authenticatiemiddelen zijn niet meer strak in te delen in publieke of privaat. Steeds meer overheidstaken worden uitgevoerd door private partijen, waardoor het voor de burger steeds vaker niet duidelijk is met wie gegevens worden gedeeld en wie bescherming zou moeten bieden. Het actualiseren van deze handreiking leidde tot het inzicht dat het klassieke onderscheid tussen publiek en privaat niet meer voldoet.

Voor de praktijk leidt dit bijvoorbeeld tot vraagstukken omtrent persoonlijke gezondheidsomgevingen, de *user experience* bij *single sign-on* (SSO) en het onderscheid tussen het Burger Service Nummer (BSN) domein en het niet-BSN-domein. In de navolgende hoofdstukken komen deze vraagstukken aan de orde.

3 Uitgangspunten

Vereenvoudigde risicoanalyse

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

- De eIDAS-verordening, en daarmee
  - de eIDAS-betrouwbaarheidsniveaus voor inlogmiddelen;
  - de eIDAS-vertrouwensdiensten.
- De Wet digitale overheid (Wdo) en de Regeling Betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (Regeling) (meer uitleg over de Wdo en de Regeling in relatie tot deze handreiking vindt u in de hoofdstukken 1 (Inleiding) en 2 (Afbakening en context) evenals bijlage 1 (juridisch kader).

3.1 De Wet digitale overheid en de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening

De Wet digitale overheid regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een substantiële of hoge mate van betrouwbaarheid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De wet stelt daarnaast open standaarden verplicht. Hiermee implementeert Nederland de Europese richtlijn over toegankelijkheid van overheidswebsites en apps. De eerste tranche (deel) van Wdo gaat over veilig inloggen op dienstverlening bij (semi-) overheidsinstanties, en toepassing van standaarden zoals informatieveiligheidsstandaarden.

De regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening geeft regels voor de bepaling van het vereiste betrouwbaarheidsniveau van authenticatie voor de verlening van elektronische diensten.

3.2 De eIDAS-verordening

Vanaf 1 juli 2016 is de Europese eIDAS-verordening van kracht. eIDAS legt criteria vast voor de betrouwbaarheidsniveaus van elektronische authenticatiemiddelen. Met de eIDAS-verordening is er een kader om betrouwbaarheidsniveaus te bepalen voor digitale overheidsdiensten (zoals dat in Nederland in de Wdo is geregeld). eIDAS richt zich op de authenticatie van burgers en bedrijven en dan vooral als het gaat om het gebruik van webportalen.

Op 20 mei 2024 is eIDAS versie 2 van kracht geworden. Versie 2 is een revisie op versie 1. In 2026 moet eIDAS 2.0 in Nederland zijn ingevoerd en zijn uitgewerkt in nationale wetgeving via een uitvoeringswet. Het voornemen is om in diezelfde periode een nieuwe actualisatie van deze Handreiking Betrouwbaarheidsniveaus (versie 6) te publiceren die zal zijn gebaseerd op de praktische uitwerking van eIDAS 2.0 die dan beschikbaar zou moeten zijn. Deze handreiking is daarom in deze min of meer overgangsperiode gebaseerd op versie 1 van eIDAS. Bijlage 1 (Juridisch kader) gaat alvast kort in op de impact van eIDAS 2.

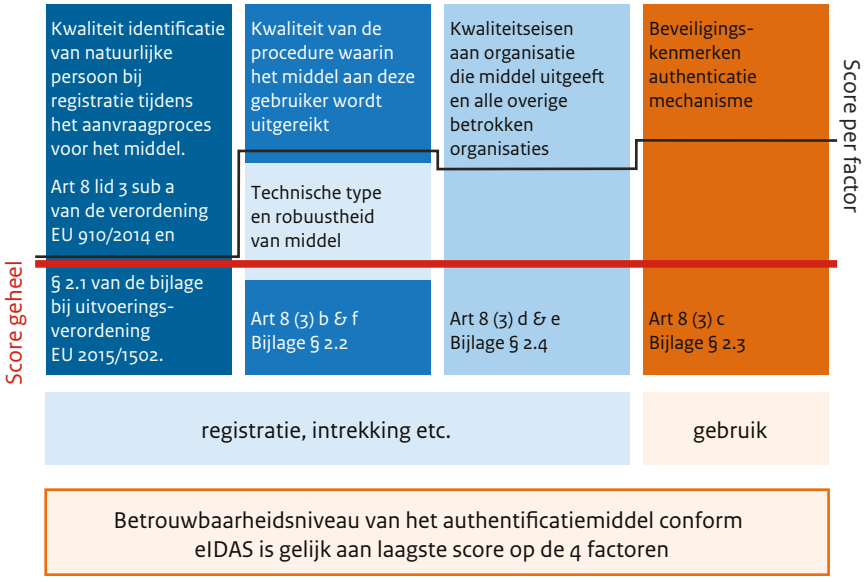
3.3 Betrouwbaarheidsniveaus

eIDAS onderkent drie betrouwbaarheidsniveaus: laag, substantieel en hoog. Om het betrouwbaarheidsniveau te bepalen hanteert eIDAS minimumeisen per niveau. eIDAS stelt daarbij de volgende vragen:

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

Deze factoren worden eerst los beoordeeld. Vervolgens wordt het uiteindelijke betrouwbaarheidsniveau van het authenticatiemiddel bepaald door de laagste score voor de individuele factoren. In onderstaande figuur is dit verbeeld. Voor alle helderheid, een Authenticatiemiddel behaalt een betrouwbaarheidsniveau als het aan alle eisen voldoet die bij dat niveau van toepassing zijn.

Figuur 1: *eIDAS geeft vier factoren om een authenticatiemiddel op te scoren. De laagste score bepaalt het uiteindelijke niveau van het authenticatiemiddel.*



Naast de genoemde eisen stelt eIDAS ook eisen aan (voor een complete uitleg van de eisen verwijzen we naar eIDAS (EU) 2015/1502):

- de minimale reeks van persoonsgegevens die voor de identificatie gebruikt moet worden;
- de gebruikersvoorwaarden;
- de vernieuwing van het middel;
- de informatiebeveiliging;
- (onafhankelijke) audits;
- de aansprakelijkheid.

Niveau 1: eIDAS laag

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

Voor eIDAS laag volstaat een **middel** met éénfactorauthenticatie. Denk bijvoorbeeld aan een combinatie van een gebruikersnaam en wachtwoord of een unieke code die de gebruiker ontvangt van een vertrouwde partij. In Nederland zijn er ook middelen voor twee factor authenticatie in gebruik die zich, gezien de inrichting van het uitgifteproces ervan, niet kwalificeren als substantieel.

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

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

Niveau 2: eIDAS substantieel

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

Voor het niveau substantieel is (minimaal) een **middel** met tweefactorauthenticatie vereist. Het middel moet zo ontworpen zijn dat het alleen onder controle van de gebruiker gebruikt kan worden. Het mag niet mogelijk zijn dat het per ongeluk of ongemerkt door een ander kan worden gebruikt.

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

Voorbeelden van middelen op het niveau van eIDAS substantieel zijn de *tokens* van banken (mits die conform het daarvoor bestemde proces zijn aangevraagd en verstrekt).

Niveau 3: eIDAS hoog

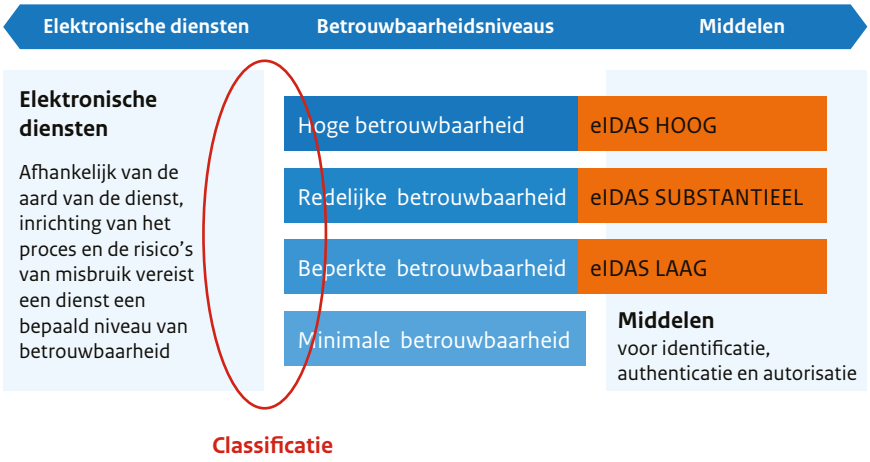
Voor eIDAS hoog moet in aanvulling op de eisen bij niveau substantieel moet in het uitgifteproces **de identiteit van de gebruiker** ten minste een maal fysiek vastgesteld worden.

Verder moet het **middel** goed beschermd zijn tegen misbruik door anderen. Denk bijvoorbeeld aan een cryptografisch token, dat ook nog een PIN-code vereist, voordat het gebruikt kan worden. Deze PIN-code biedt een extra bescherming tegen misbruik door derden (de eisen zijn bijna net zo streng als die voor middelen voor gekwalificeerde elektronische handtekeningen. Echter, anders dan bij het eerder gehanteerde STORK, is eIDAS hoog niet gelijkgesteld aan de gekwalificeerde elektronische handtekening c.q. de daarbij gehanteerde techniek).

3.4 Relatie middelen en elektronische diensten

Onderstaande figuur maakt de relatie tussen elektronische diensten en middelen inzichtelijk, rekening houdend met de betrouwbaarheidsniveaus die eIDAS onderkent.

Figuur 2: *Relatie tussen elektronische diensten en middelen*



3.5 Handreiking in relatie tot eIDAS, de Wdo en de Regeling

Bij de ontwikkeling en het gebruik van elektronische diensten zijn er meer onderwerpen van belang dan de eIDAS-verordening beschrijft. Daarbij gaat het bijvoorbeeld om machtigingen, applicatieapplicatieverkeer en eenmalig inloggen. Hiervoor zijn nauwelijks algemeen geaccepteerde standaarden voorhanden voor een indeling in betrouwbaarheidsniveaus. In deze handreiking geven we daar echter wel een nadere invulling aan.

De Wdo en de Regeling geven op Nederlands niveau verder invulling aan de eIDAS-verordening. BZK verzorgt de communicatie hierover. Deze handreiking richt zich alleen op onderwerpen die niet in deze communicatie aan de orde komen.

4 Inschaling van diensten

Hoe kiest u het juiste betrouwbaarheidsniveau?

In hoofdstuk 3 hebben we uitgangspunten geformuleerd voor een classificatiemodel om e-overheidsdiensten in te schalen op de verschillende betrouwbaarheidsniveaus. In eerdere versies van deze handreiking is hiervoor in dit hoofdstuk een model geïntroduceerd dat als de 'kern' van de handreiking kan worden gezien. Zoals in hoofdstuk 3 is aangegeven, is dit een model dat te zien is als een eenvoudige risicoanalyse.

Met de inwerkingtreding van de Wet digitale overheid (Wdo) en de daarbij behorende Regeling betrouwbaarheidsniveaus per 1 juli 2023, is een dergelijk model als wettelijk kader geformuleerd. Daarmee is het gebruik van dit model verplicht voor dienstaanbieders.

Dit hoofdstuk is niet bedoeld om nadere toelichting te geven op de tekst van de Regeling. Dit is reeds gebeurd met de publicatie in de Staatscourant.

In essentie maakt de Regeling gebruik van dezelfde criteria om het vereiste betrouwbaarheidsniveau voor de dienst, en daarmee het niveau van authenticatie en machtiging, te bepalen als in eerdere versies van de handreiking. Voor de leesbaarheid nemen we de tabel uit de Regeling (bijlage 2 bij de Regeling) hieronder over.

Aspecten van de dienst	**Criteria betrouwbaarheidsniveaus**		
	Niveau laag	**Niveau substantieel**	**Niveau hoog**
Persoonsgegevens (behoudens het BSN): aard gegevens en aard en omvang van de verwerking	• Geen bijzondere categorieën van persoonsgegevens • Geen persoonsgegevens van strafrechtelijke aard, geen gegevens uit antecedentenonderzoek en geen politiegegevens • Kleinschalige verwerking	• Bijzondere categorieën van persoonsgegevens • Persoonsgegevens van strafrechtelijke aard, gegevens uit antecedentenonderzoek en politiegegevens • Gevoelige persoonsgegevens niet zijnde bijzondere categorieën van persoonsgegevens, persoonsgegevens van strafrechtelijke aard, gegevens uit antecedentenonderzoek of politiegegevens • Grootschalige verwerking	• Persoonsgegevens die: * stigmatiserend kunnen werken * reputatieschade kunnen opleveren * tot uitsluiting kunnen leiden * schade kunnen opleveren aan de gezondheid, of * chanteerbaarheid kunnen opleveren • Gegevens die onder het medisch beroepsgeheim vallen

Aspecten van de dienst	Criteria betrouwbaarheidsniveaus		
	Niveau laag	**Niveau substantieel**	**Niveau hoog**
Risico's indien de gegevens in verkeerde handen vallen	Geen of nauwelijks risico op identiteitsfraude en/of misbruik van de betreffende dienst	Reëel risico op identiteitsfraude en/of misbruik van de betreffende dienst	Groot risico op identiteitsfraude en/of misbruik van de betreffende dienst
Aard van de gegevens van ondernemingen en rechtspersonen	Algemeen bekende gegevens van ondernemingen en rechtspersonen	Gevoelige gegevens van ondernemingen en rechtspersonen	Geen criteria
Aard van de verwerking van het BSN	• BSN van degene aan wie de dienst wordt verleend, van zijn gemachtigde, of van een derde wordt door dienstverlener niet verstrekt	• BSN van degene aan wie de dienst wordt verleend, van zijn gemachtigde of van een derde wordt door de dienstverlener tijdens het proces van dienstverlening verstrekt • NB: wanneer dienstverlener reeds opgegeven BSN terugkoppelt: minimaal niveau laag met 2-factor authenticatie nodig	• BSN in combinatie met andere persoonsgegevens
Gevolgen voor de gegevens in de basisregistraties	• Geen criteria	• Controle op de verwerking van gegevens	• Geen controle op de verwerking van gegevens
Economisch belang	• Niet of nauwelijks ingrijpend voor economische positie burgers/ondernemingen en rechtspersonen in de doelgroep, waarbij als richtsnoer geldt: * De directe schade voor burgers is lager dan € 1.000,– * De directe schade voor bedrijven tot 250 werknemers is lager dan € 125.000,– * De directe schade voor grotere bedrijven is lager dan € 500.000,–	• Ingrijpend voor economische positie burgers/ ondernemingen en rechtspersonen in de doelgroep, waarbij als richtsnoer geldt: * De directe schade voor burgers is hoger dan € 1.000,– * De directe schade voor bedrijven tot 250 werknemers is hoger dan € 125.000,– * De directe schade voor grotere bedrijven is hoger dan € 500.000,–	• Zodanig ingrijpend voor economische positie burgers/ondernemingen en rechtspersonen dat ongewijzigd welstandsniveau of voortbestaan onmogelijk is

De regels, zoals gedefinieerd in de Regeling, zijn voor uw geval ook eenvoudig te bepalen middels de Regelhulp Betrouwbaarheidsniveaus. Deze is geactualiseerd en aangepast op de Regeling Betrouwbaarheidsniveaus.

Analoog met eerdere versies van deze handreiking, zijn ook in de Regeling uitzonderingsbepalingen opgenomen op het aldus via deze tabel te bepalen betrouwbaarheidsniveau , in de vorm van:

- risicoverlagende factoren,
- risicoverhogende factoren en het tijdelijk toestaan van een lager authenticatieniveau.

De Regeling bepaalt alleen iets omtrent het vereiste niveau van authenticatie en machtiging. Dat laat veel vragen van dienstaanbieders omtrent het betrouwbaar aanbieden van elektronische diensten onbeantwoord. Daarom zijn overige hoofdstukken van de handreiking nog steeds relevant, met onderwerpen als machtigen, retourstromen, applicatie-applicatieverkeer, eenmalig inloggen en ondertekenen. Wellicht door de toenemende digitaliseringsgraad zelfs relevanter dan ooit.

Met de behandeling in de komende hoofdstukken wordt niet alleen beoogd een uiteenzetting van de verschillende aspecten van de digitale dienstverlening te geven. Het is ook de intentie om dienstaanbieders op die aspecten van een handelingsperspectief te voorzien, juist ook op die plaatsen waar vaste (wettelijke) regels nog niet zijn uitgekristalliseerd.

5 Machtigingen

Welk betrouwbaarheidsniveau hoort erbij?

5.1 Waar gaat het eigenlijk over?

In veel situaties laten burgers of bedrijven zich vertegenwoordigen door iemand anders. Zo'n vertegenwoordiger is gemachtigd om te handelen namens die burger of dat bedrijf. Een machtiging heeft in principe geen invloed op het betrouwbaarheidsniveau van een individuele dienst: de aard van de dienst verandert er namelijk niet door.

Rond machtigingen is sprake van twee situaties:

- een belanghebbende geeft vrijwillig een machtiging af aan een (beoogd) gemachtigde.
- de gemachtigde is de wettelijk vertegenwoordiger van de belanghebbende (daarbij gaat het om curatele en bewindvoering). Hierbij is geen sprake van vrijwilligheid.

Daarnaast kan rond machtigen sprake zijn van attribuutverstrekking, waarbij specifieke afwegingen en controles worden gevraagd waar we in de context van deze handreiking niet verder op ingaan.

De achtergrond bij wettelijke vertegenwoordiging en attribuutverstrekking is dat hier sprake is van specifieke wettelijk geregelde situaties, de handreiking geeft geen nadere uitleg over wet- en regelgeving. Dit hoofdstuk gaat daarom over machtigingen in algemene zin.

Het is verder belangrijk om machtigingssituaties zonder twijfel te herkennen. U wilt immers niet dat gemachtigden inloggen met de eigen inloggegevens van burgers of bedrijven. Het is dan namelijk alsof zij die burgers of bedrijven zelf zijn. Ook zouden die gemachtigden die inloggegevens ook voor andere zaken kunnen gebruiken, terwijl dit niet de bedoeling was, wat een direct risico op fraude met zich meebrengt.

Het is daarom van belang dat machtigingen expliciet vastgelegd en herkenbaar zijn. Dat betekent dat machtigingen (in lijn met het in de Wdo gestelde) vastgelegd moeten zijn in een machtigingsregister dat onderdeel uitmaakt van de Generieke Digitale Infrastructuur (GDI). In zo'n register is opgeslagen welke handelende partij bevoegd is welke handelingen te doen namens welke burger of welk bedrijf en tot hoever die handelingsbevoegdheid strekt.

Een machtigingsregister zoals hiervoor bedoeld verstrekt bevoegdheidsverklaringen. Dit gebeurt via digitale berichten waarin staat dat de handelende partij (die al is geauthenticeerd) daadwerkelijk bevoegd is de elektronische dienst in kwestie af te nemen namens die burger of dat bedrijf. Dit betekent niet automatisch dat de bevoegdheid ook met voldoende waarborgen tot stand is gekomen.

5.2 Regeling betrouwbaarheidsniveaus

De Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (Regeling) geeft een aantal algemene kaders voor de registratie van machtigingen en het gebruik ervan binnen elektronische diensten. De Regeling is gebaseerd op twee belangrijke uitgangspunten:

- De registratie van afgifte, verstrekking en intrekking van machtigingen vindt elektronisch plaats (waarbij de afgifte en intrekking zelf zowel elektronisch als niet-elektronisch kan plaatsvinden).
- Het is mogelijk machtigingen te registreren met authenticatie op hetzelfde betrouwbaarheidsniveau als het niveau dat vereist is voor de elektronische dienst waarvoor de machtiging is bedoeld.

In aanvulling daarop stelt de Regeling het volgende:

- Bij de registratie van een machtiging, die niet of niet geheel langs elektronische weg is afgegeven, bepaalt het bestuursorgaan of de aangewezen organisatie of de betrouwbaarheid van de machtiging gewaarborgd is.

Bij DigiD machtigen is het proces niet (volledig) elektronisch wanneer:

- de beoogd gemachtigde de machtiging aanvraagt en een brief met machtigingscode naar de machtiginggever wordt gestuurd.
- de machtiginggever de machtiging telefonisch aanvraagt (ook dan gaat er een brief met machtigingscode naar de machtiginggever).

- Het bestuursorgaan of de aangewezen organisatie kan bepalen dat de betrouwbaarheid van een machtigingsregistratie lager mag zijn dan het betrouwbaarheidsniveau dat voor de authenticatie van de dienst vereist is, mits adequate aanvullende maatregelen in het proces van dienstverlening of toegangsverlening worden getroffen.

In de praktijk blijkt dat deze uitgangspunten niet altijd volledig van toepassing zijn. Dat vindt mede zijn oorzaak in de inrichting van de bestaande voorzieningen. Daarnaast zijn er andere factoren die de betrouwbaarheid van de machtiging beïnvloeden. In de volgende paragraaf is een nadere uitwerking van de problematiek rond machtigen opgenomen.

5.3 Nadere analyse van de problematiek

Betrouwbaarheidsniveau van de machtiging

De betrouwbaarheid waarmee een machtiging wordt geregistreerd hangt samen met de betrouwbaarheid waarmee de authenticatie moet plaatsvinden indien er géén sprake is van een machtigingssituatie. Immers, de waarborgen omtrent de identiteit die worden geboden in de situatie dat iemand een elektronische dienst zelf afneemt, zijn maatgevend voor de situatie waarin er sprake is van een machtiging. Gestreefd moet worden naar equivalente betrouwbaarheid in beide situaties. Zwaardere dan equivalente waarborgen leiden tot ongewenste drempels bij het registreren van een machtiging, wat elektronische dienstverlening onnodig belemmert. Lichtere dan equivalente waarborgen leiden ertoe dat machtigingen het 'afvoerputje' worden: als men wil frauderen met identiteiten, is het eerste dat men dan doet het registreren van een machtiging (op een lager betrouwbaarheidsniveau). Dit kan los van de (soms verstrekkende) gevolgen voor individuele burgers leiden tot verlies van vertrouwen in elektronische dienstverlening in het algemeen en in machtigingen in het bijzonder.

Verder is van belang dat de procedures voor met name het afgeven van een machtiging in veel gevallen niet (geheel) elektronisch zijn. Vooral in het maatschappelijk belangrijke segment van belanghebbenden die niet digitaal vaardig zijn, wordt de belanghebbende primair betrokken via *face-to-face* machtigingsdienstverlening (een helpende hand) en/of via papier. Van de niet-digitale processen voor het afgeven van een machtiging is thans niet duidelijk wat het betrouwbaarheidsniveau is.

Onderkend dient ook te worden dat de waarborg in het geval van een machtiging niet alleen de identiteit van de belanghebbende betreft, maar tevens de identiteit van de gemachtigde en de wilsuiting van de belanghebbende. In geval van elektronische dienstverlening zonder machtiging, betreffen de waarborgen slechts de identiteit van de belanghebbende en diens wilsuiting.

Machtigingen die langs niet-elektronische weg tot stand komen

Er zijn verschillende factoren die relevant zijn voor het bepalen van het betrouwbaarheidsniveau van een machtiging. Dat zijn:

- Het kanaal of de kanalen waarlangs de machtiging wordt afgegeven
  Dienstverleners moeten kanalen waarbinnen de identiteitsverificatie en -controle van de wilsuiting / ondertekening kan plaatsvinden expliciet benoemen. In de praktijk betekent dit *face-to-face* (balie) dienstverlening of dienstverlening door een videoproces. Van machtigingen die via een papieren proces tot stand komen is het moeilijker om de juiste ondertekening te verifiëren. Het verdient dus de voorkeur om dergelijke papieren processen zo mogelijk te vermijden. Hoewel er theoretisch wel een hoge betrouwbaarheid aan toegekend moet worden, is aanvullend bewijs nodig. Combinatie met een schriftelijke feedback naar de belanghebbende met expliciete opt-in en/of opt-out mogelijkheid is een overweging bij het gebruik van een schriftelijk proces.
  De dienstaanbieder bepaalt zelf, aan de hand van de aard van de dienst, of hij deze mogelijkheid wil toepassen.

- Kenbaarheid van de wil van de belanghebbende
  Het is van cruciaal belang dat de wil van de belanghebbende omtrent de machtiging kenbaar is. Het beste is als er sprake is van een expliciete wilsuiting die bovendien als wilsuiting voorhanden is, denk aan een ondertekende verklaring of een op video opgenomen verklaring. Hoewel dit niet is opgenomen in de Regeling is een dergelijke praktijk feitelijk noodzakelijk voor het niveau Substantieel en Hoog. Dat laat onverlet dat dit in de huidige praktijk lastig te realiseren is.

  In sommige gevallen kan voor het niveau Laag worden volstaan met ‘bijkomend bewijs’ aan de hand waarvan kan worden aangenomen dat de machtiging overeenkomt met de wil van de belanghebbende. Hierbij kan worden gedacht aan codes die zijn verstrekt aan belanghebbende en die deze aan de gemachtigde heeft gegeven. Bij de wilsuiting moet de belanghebbende op een voldoende betrouwbare wijze zijn geïdentificeerd. Regels die die ETSI recent heeft geformuleerd in ETSI TS 119 461 (identity proofing) zijn hiervoor relevant.

- Omstandigheden waaronder de belanghebbende zijn wil kenbaar heeft gemaakt
  De belanghebbende dient zijn wil tot het afgeven van een machtiging zonder dwang of drang te kunnen uiten. In het geval van een *face-to-face* proces zijn hier de omstandigheden het gunstigst voor. In een videoproces waarbij belanghebbende en gemachtigde beiden aanwezig

zijn, zijn hier al meer twijfels bij denkbaar. Het is een overweging om machtigingen die op een wijze tot stand komen waarbij er twijfels mogelijk zijn, de registratie van de machtiging schriftelijk te laten bevestigen, met opt-out mogelijkheid. Verder is aan te bevelen een termijn aan te geven voordat de machtiging ingaat. Overigens kan ook in situaties waarin alleen de belanghebbende aanwezig is tot twijfels leiden: de belanghebbende kan bijvoorbeeld buiten het directe video-zicht onder druk worden gezet. Wellicht kan inspiratie worden opgedaan bij richtlijnen voor online proctoring (zie bijvoorbeeld 'Aanbevelingen online proctoring onderwijs').

- Specificiteit van de machtiging

  Vrijwillige machtigingen dienen heel specifiek te worden afgegeven:
  - met eenduidig bepaalde identificerende gegevens van de gemachtigde;
  - met een eenduidig bepaald bereik ten aanzien van diensten waar de machtiging betrekking op heeft en de geldigheidstermijn.

  Dienstaanbieders moeten daarom expliciet aandacht geven aan de indeling van hun diensten, de granulariteit en de begrijpelijkheid daarvan. Alleen op die manier kunnen belanghebbenden gericht hun keuze bepalen voor de omvang van de door hen af te geven machtiging.

  Daar waar de gemachtigde een machtiging laat vastleggen in een elektronisch register op basis van een voorafgaande schriftelijke machtiging (bijvoorbeeld een notariële volmacht) wordt hier een specifieke machtiging voor een of meer elektronische diensten van afgeleid. Ook in dit geval is een schriftelijke bevestiging aan de belanghebbende aan te bevelen. Overigens bestaat het risico dat wanneer afnemers het proces van machtigen als (te) ingewikkeld ervaren, men te veel zaken in één keer uit handen geeft, om dat proces in de toekomst maar niet nog een keer door te hoeven. Bij ketenmachtigingen binnen eHerkenning wordt zo bijvoorbeeld (te) vaak een "alle machtiging" verstrekt.

5.4 Aanvullende maatregelen in het dienstverleningsproces

De nadere analyse maakt duidelijk dat de Regeling niet alle situaties afdekt die in de praktijk voorkomen. Dat noopt dienstaanbieders tot het nemen van aanvullende maatregelen voor die situaties die niet (geheel) afgedekt zijn door de Regeling. In zijn algemeenheid gaat het om de volgende situaties:

- Het authenticatieniveau waarop de machtiging is geregistreerd is lager dan het authenticatieniveau dat vereist is voor toegang tot de digitale dienst.
- Het is onbekend op welk authenticatieniveau de machtiging is geregistreerd.
- Het (brief)proces van het vaststellen van de wilsuiting biedt (bij DigiD Machtigen) te weinig zekerheid. Dit is met name het geval voor digitale diensten een "gevoelig karakter" hebben en/of onomkeerbaar zijn.

Er zijn drie typen maatregelen mogelijk, waarbij dienstverleners zelf bepalen welke maatregelen zij inzetten:

- Baliemachtigen
- Aanvullende maatregelen in het dienstverleningsproces zelf
- Aanvullende maatregelen in het proces van toegangsverlening zelf

In de volgende paragrafen komt een nadere uitwerking van deze maatregelen aan de orde.

5.4.1 Baliemachtigen

Een baliemachtiging is bedoeld om de betrouwbaarheid van een machtiging te verhogen door deze vast te laten leggen of nader te laten controleren aan de balie van de dienstaanbieder, waarbij belanghebbende en gemachtigde beiden aanwezig zijn.

De Belastingdienst biedt deze mogelijkheid bijvoorbeeld aan voor HUBA's (HUBA = hulp bij aangifte). De medewerker van de Belastingdienst stuurt daarbij een brief met machtigingscode naar de belanghebbende. Aan de balie kan de medewerker de machtiging met deze code activeren. Bepalend voor het betrouwbaarheidsniveau is hoe aan de balie de identiteit van de belanghebbende en de beoogd gemachtigde is vastgesteld.

Naast de baliemachtiging kent de Belastingdienst ook de mogelijkheid dat een nabestaande met een verklaring van erfrecht een machtiging regelt. Een medewerker van de Belastingdienst kan deze machtiging rechtstreeks registreren in DigiD machtigen (zie voor meer informatie de notitie Baliemachtigen dd. 7 mei 2020 (opgesteld binnen het programma Machtigen van Logius); deze notitie is op 13 juli 2021 vastgesteld in de toenmalige Program Board Vertegenwoordiging; de Program Board heeft de uitwerking van de kaders voor Baliemachtigen opgenomen op zijn "long list".).

Een ander voorbeeld van baliemachtigen is te vinden in de zorg, waarbij de belanghebbende en de gemachtigde zich beiden fysiek bij een zorgaanbieder melden, veelal in verband met te verlenen zorg aan de belanghebbende.

Het beeld is dat baliemachtigen een nuttig instrument is, waarmee dienstaanbieders alsnog machtigingen met de juiste betrouwbaarheid kunnen realiseren. Echter, bovenstaande punten tezamen maken dat er een behoefte ontstaat aan generieke balies, waar machtigingen kunnen worden afgegeven en geregistreerd voor een verscheidenheid aan dienstverleningsprocessen. Daarom gaat er onderzoek plaatsvinden naar de beleidsvraag of en zo ja op welke wijze generieke balies belegd moeten worden (vastgesteld in de program board Vertegenwoordiging van 13 juli 2021). Kortom, er is bij baliemachtigingen echter een aantal kanttekeningen te zetten:

- Veel dienstaanbieders hebben als beleid om hun dienstverlening minder langs het fysieke kanaal aan te bieden. Voor deze partijen is een baliemachtiging van weinig praktisch nut (met name omdat de registratie van de baliemachtiging veelal plaatsvindt in het verlengde van de af te nemen (fysieke) dienst).
- Baliebezoek is arbeidsintensief voor de aanbieder van de balie, *in casu* de dienstaanbieder. Daarnaast werkt baliebezoek ook drempelverhogend voor belanghebbende en gemachtigde.
- In situaties dat iemand als gemachtigde gaat optreden voor een belanghebbende in meerdere dienstverleningsprocessen, moeten belanghebbende en mogelijk ook gemachtigde meerdere balies afgaan. Dat heeft als reden dat de baliemachtiging alleen betrekking heeft op de diensten die de organisatie zelf aanbiedt. Dit versterkt de drempelwerking.

Waar machtigingen decentraal aan een balie worden afgegeven en geregistreerd, is het nog wel zaak in welk systeem deze vervolgens worden vastgelegd. Volgt men de route om deze machtigingen of aanvullende registraties in centrale voorzieningen vast te leggen, dan dienen die voorzieningen hier geschikt voor te zijn. Volgt men de route om deze machtigingen decentraal vast te leggen, dan werkt dat prima voor deze specifieke dienstverleningssituatie, maar de informatie over de machtiging is dan feitelijk geïsoleerd en komt dan bijvoorbeeld niet voor in landelijke overzichten.

5.4.2 Aanvullende maatregelen in het dienstverleningsproces zelf

Zoals gezegd moet het betrouwbaarheidsniveau van de authenticatie bij de registratie een machtiging (in beginsel) gelijk zijn aan het niveau van betrouwbaarheid dat voor de authenticatie op een dienst is vereist. Dat impliceert dus logischerwijs ook dat het verlenen van een dienst aan een gemachtigde niet is toegestaan als het betrouwbaarheidsniveau van de authenticatie bij de registratie van de machtiging niet hoog genoeg is. Een wezenlijke vraag is in hoeverre er kan worden afgeweken van het vereiste betrouwbaarheidsniveau van de authenticatie en zo ja, onder welke omstandigheden.

Voor een aantal van de elektronische diensten die de overheid aanbiedt is het logischerwijs niet toegestaan om op een lager authenticatieniveau te machtigen. Daarbij gaat het met name om diensten die een "gevoelig karakter" hebben en/of onomkeerbaar zijn. We kunnen bijvoorbeeld denken aan het inzien van privacygevoelige gegevens, zoals medische gegevens of het inzien van contracten met concurrentiegevoelige informatie. Een onterechte verstrekking van (privacygevoelige) gegevens is immers niet ongedaan te maken. Ook kan een dienstaanbieder, al dan niet in samenspraak met de wetgever, besluiten dat diensten een zodanig karakter hebben dat hij geen machtigingen wil accepteren of besluiten bepaalde diensten niet aan te bieden via een elektronisch kanaal. Daarbij kan het bijvoorbeeld gaan om de aanvraag van een identiteitsbewijs of om verzoeken tot verstrekking van hulpmiddelen in het kader van de Wet maatschappelijke ondersteuning (Wmo).

Voor andere diensten die langs elektronische weg geboden worden en die of minder gevoelig zijn of tot goed omkeerbare gevolgen leiden, is het echter mogelijk om een lager authenticatieniveau bij de registratie van de machtiging toe te staan, mits mitigerende maatregelen zijn genomen (een interessante bron van dergelijke maatregelen is de Handreiking voorziening machtigen van de VNG, die mede is samengesteld op basis van de gemeentelijke uitvoeringspraktijk). In de praktijk komen de volgende maatregelen voor:

- Controleren van aanvraag aan de hand van andere registraties
  In dit geval toetst de dienstaanbieder de gegevens op de aanvraag aan de hand van andere registraties. Voorbeelden:
  - controle van de gegevens van een onderneming aan de hand van het Handelsregister.
  - controle op het opgegeven bankrekeningnummer (is dat van de belanghebbende).
- Contacteren van de belanghebbende vanuit het (digitale) primaire proces
  Het primaire proces kent stappen waarin contact met de belanghebbende tot stand komt, zoals bijvoorbeeld:
  - vragen om aanvullende gegevens;
  - informeren over een genomen besluit/verleende vergunning.
- Uitstellen van het gevraagde besluit/wachttijd inbouwen
  Door het gevraagde besluit later in de tijd te nemen krijgt de dienstaanbieder ruimte om aanvullende verificaties uit te voeren (in bijvoorbeeld publieke registers). Bij twijfel verleent de dienstaanbieder geen toegang tot de dienst (ten onrechte weigeren heeft namelijk minder negatieve gevolgen dan ten onrechte toegang verlenen).

- "Terugdraaien van de dienst"
  Als blijkt dat een gemachtigde ten onrechte een dienst heeft afgenomen "draait" de dienstaanbieder de dienst "terug", in die zin dat de dienstaanbieder de genomen beslissing en de daaruit resulterende gevolgen ongedaan maakt.
- Notificeren van het gebruik van de machtiging aan de belanghebbende
  In dit geval stuurt de dienstaanbieder de belanghebbende een kennisgeving van het gebruik van de machtiging.
- Gebruik maken van vertrouwde tussenpersonen
  De dienstaanbieder accepteert in dit geval alleen aanvragen en verzoeken die afkomstig zijn van een vertrouwde partij. Daarbij kan het bijvoorbeeld gaan om een notaris (die zelf de identiteit van de aanvrager/verzoeker controleert). De voorwaarden die partijen tot een vertrouwde partij maken zijn tot nu toe niet nader gedefinieerd, hier zijn landelijke richtlijnen voor nodig.
- Vastleggen van het gebruik van de machtiging
  De dienstaanbieder legt vast welke persoon gebruik heeft gemaakt van een machtiging. Dit maakt het mogelijk bij oneigenlijk gebruik van de machtiging achteraf verhaal te halen bij de gemachtigde.

Specifiek voor het ondernemersdomein zijn nog twee aanvullende maatregelen mogelijk:

- Soms is de doelgroep voor een regeling zo beperkt dat de medewerkers van de dienstaanbieder de leden van de doelgroep "persoonlijk" kennen (denk bijvoorbeeld aan de aanvraag voor subsidie voor vissersschepen).
- In sommige sectoren waarin sprake is van inhoudelijk complexe regelingen is sprake van een beperkt aantal intermediairs die namens ondernemingen in die sectoren optreden. Dat maakt het mogelijk deze intermediairs te vertrouwen op basis van een zogenoemde zelfverklaring. Echter, vanaf het niveau substantieel zijn zelfverklaringen ingevolge de Wdo niet toegestaan.

Het moge helder zijn dat dienstaanbieders deze maatregelen ook kunnen toepassen in gevallen waarin de machtiging wel op het juiste niveau is geregistreerd.

5.4.3 Aanvullende maatregelen in het proces van toegangsverlening

Naast aanvullende maatregelen in het dienstverleningsproces zelf, zoals uiteengezet in de vorige paragraaf, is er de mogelijkheid om in het proces van toegangsverlening aanvullende maatregelen te treffen. Daarbij gaat het om:

- Persoonlijk contact met de belanghebbende
  In persoonlijk contact met de belanghebbende kan de dienstaanbieder expliciet vaststellen of de gemachtigde daadwerkelijk namens hem of haar mag handelen. Een voorbeeld hiervan is het keukentafelgesprek in het kader van de Wmo. Daarbij is wel de vraag hoe deze aanvullende check wordt vastgelegd en of daar inzage en herstel op mogelijk is.
- Beperken van de acceptatie van machtigingen
  Deze maatregel komt erop neer dat de dienstaanbieder alleen machtigingen accepteert die bijvoorbeeld niet langer geleden dan een vooraf bepaalde termijn zijn uitgegeven, of die juist 'voor' een bepaalde datum zijn aangegaan. Stel dat iemand dement is geraakt, dan zou een (malafide) gemachtigde misbruik van die situatie kunnen maken.

5.5 Resterende (nog op te lossen) problemen

Met de hiervoor beschreven maatregelen hebben dienstaanbieders mogelijkheden om de problematiek rond (de betrouwbaarheid van) machtigingen te mitigeren. Dat laat onverlet dat er problemen resteren die (al langer) om een gerichte oplossing vragen.
Die problemen doen zich voor bij

- het vastleggingsproces van machtigingen;
- het beschikbaar stellen van informatie over het betrouwbaarheidsniveau van de machtiging;
- het betrouwbaarheidsniveau van niet-digitale processen rond digitaal vastleggen van machtigingen.
- het bepalen onder welke voorwaarden een partij als vertrouwde partij kan worden gezien;
- ketenmachtigingen;
- wettelijke vertegenwoordiging.

5.5.1 Het vastleggingsproces van machtigingen

Het uitgangspunt in de Wdo en daarmee ook in deze handreiking is dat bij gebruik van een machtiging de betrouwbaarheid van de vastlegging daarvan gelijk moet zijn aan het betrouwbaarheidsniveau dat de dienstaanbieder vereist bij identificatie en authenticatie van een belanghebbende.
Het vaststellen van het betrouwbaarheidsniveau van de registratie is relatief eenvoudig als de belanghebbende de machtiging digitaal registreert.
Echter, niet alle machtigingen worden direct digitaal geregistreerd. Dat heeft als oorzaak dat de belanghebbenden vaak minder of niet digitaal vaardig zijn. De registratie van een machtiging kan in verband daarmee bijvoorbeeld gebaseerd zijn op telefonisch contact met de belanghebbende, een brief van de belanghebbende of een formele verklaring van een notaris.

Er is geen normenkader beschikbaar waarmee het mogelijk is de betrouwbaarheid van deze (deels) handmatige registratieprocessen vast te stellen (de eIDAS-verordening besteedt in het algemeen geen aandacht aan de betrouwbaarheidsniveaus van machtigingsregistraties). Dat betekent dat dienstaanbieders geen zekerheid kunnen krijgen over de betrouwbaarheid van de vastgelegde machtigingen.

5.5.2 Het beschikbaar stellen van informatie over het betrouwbaarheidsniveau van de machtiging

De huidige machtigingsvoorziening DigiD Machtigen legt geen informatie vast over de betrouwbaarheid waarmee een machtiging is vastgelegd, ze kunnen deze informatie daardoor ook niet aan dienstaanbieders verstrekken. De consequentie daarvan is dat dienstaanbieders de betrouwbaarheid van de machtiging op het laagste niveau (moeten) inschalen. In het geval de dienst een hoger betrouwbaarheidsniveau vereist kan de dienstaanbieder een dergelijke machtiging accepteren, mits hij aanvullende mitigerende maatregelen neemt (zie bijvoorbeeld Handreiking voorziening machtigen).

5.5.3 Ketenmachtigingen

Ketenmachtigingen zijn machtigingen die verder gaan dan een enkelvoudige machtiging tussen twee partijen. Het gaat daarbij om verschillende situaties, zoals:

- Een burger die een andere burger machtigt waarna de gemachtigde een andere burger machtigt (al dan niet voor een afgebakend onderdeel van de oorspronkelijke machtiging). Een voorbeeld hiervan is een situatie waarin een ouder zijn of haar kind machtigt om zaken met de Belastingdienst te doen, waarbij het kind iemand anders machtigt voor het onderdeel Toeslagen.
- Een burger die een organisatie machtigt om namens hem of haar zaken te doen met de overheid waarna de organisatie een van zijn medewerkers machtigt om de hiervoor benodigde activiteiten uit te voeren. Een voorbeeld hiervan is de situatie waarin een ondernemer een accountantskantoor machtigt voor fiscale aangelegenheden en subsidies, waarbij het accountantskantoor een van zijn medewerkers machtigt namens het kantoor de hiervoor nodige activiteiten uit te voeren.

Het lastige is dat de bestaande machtigingsvoorzieningen alleen geschikt zijn voor het registreren van enkelvoudige machtigingen. Dat betekent dat in geval van ketenmachtigingen andere oplossingen nodig zijn, zoals het vastleggen van machtigingen op papier of een belanghebbende die van geval tot geval toestemming geeft om bepaalde handelingen door een andere persoon te laten uitvoeren.

5.5.4 Wettelijke vertegenwoordiging

Bij wettelijke vertegenwoordiging gaat het zowel om mentorschap, curatele en bewindvoering als om ouderlijk gezag. Het uitgangspunt is dat de betrouwbaarheid van deze registraties hoog is en dat wettelijke vertegenwoordiging daarmee een hoog niveau van betrouwbaarheid heeft.

Er doen zich desondanks nog verschillende problemen voor, zoals:

- Het was tot voor kort voor dienstaanbieders lastig om het juiste inzicht te krijgen over mentorschap, curatele of bewindvoering. De registraties waarin deze zaken zijn vastgelegd waren namelijk niet of niet effectief digitaal te raadplegen. De introductie van de Bevoegdheidsverklaringdienst biedt hier een oplossing voor. Daarnaast was er sprake van vertraging in de registratie van rechterlijke uitspraken. De Raad voor de Rechtspraak heeft samen met de Rechtbanken in de afgelopen jaren hard gewerkt aan het versnellen van deze registratie.
- Voor het ouderlijk gezag is de Basisregistratie Personen (BRP) de voor de hand liggende bron. Echter, in de BRP is sprake van inconsistenties in relaties tussen personen. RvIG werkt hard aan het verbeteren van de kwaliteit van deze registraties. Het gebruik van de bedoelde gegevens door afnemers heeft een aanjagende werking op de kwaliteit ervan (omdat door het gebruik onjuistheden vaker en sneller aan het licht komen).
  Daarnaast kan sprake zijn van complicerende factoren, zoals in de situatie waarin gescheiden ouders allebei het ouderlijk gezag willen uitoefenen. In voorkomende gevallen doet de rechter hier uitspraak over, tot dat moment is voor de dienstaanbieder niet helder welke ouder het gezag heeft.

6 Applicatie-applicatieverkeer

Wat doet u met dienstverlening zonder menselijke tussenkomst?

6.1 Waar gaat het eigenlijk over?

Steeds vaker komt er bij digitale dienstverlening geen mens meer aan te pas. Zo kan een geautomatiseerd systeem een dienst afnemen bij een ander geautomatiseerd systeem. Dit wordt applicatie-applicatieverkeer genoemd. Een voorbeeld hiervan is Digipoort (centrale voorziening waar gestructureerd berichtenverkeer voor de overheid afgehandeld wordt).

De volgende eigenschappen zijn kenmerkend voor applicatie-applicatieverkeer:

- Het betreft applicaties die diensten (en gegevens) leveren aan andere applicaties. Die afnemende applicaties moeten als de afnemer van de dienst worden beschouwd. Bijvoorbeeld omdat het juridisch zo geregeld is en/of omdat er niet een specifiek natuurlijk persoon als afnemer van de dienst is aan te merken.
- In deze interactie is er in deze interactie tussen de verschillende applicaties geen menselijke tussenkomst.
- Vaak gaat het om complexe interactiepatronen en aanzienlijke volumes.

De scheidslijn tussen een interactieve applicatie zoals een webapplicatie of een portaal aan de ene kant versus applicatie-applicatieverkeer aan de andere kant is niet altijd hard te trekken. Zo is het goed mogelijk dat het startsein voor de interactie tussen applicaties nog steeds een verzoek van een mens is. Maar het is ook mogelijk dat daar bijvoorbeeld een batchproces aan ten grondslag ligt. Dan is het van belang om terug te keren naar de vraag: wie is hier de afnemer? Gaat dat om een organisatie of een organisatiedeel, of is dat de natuurlijke persoon?

In deze zin past het gebruik van *apps* op mobiele telefoons dan ook niet in de karakterisering van applicatie-applicatieverkeer. Het gaat daar weliswaar om een applicatie op de mobiele telefoon, die interacteert met een applicatie bij de dienstaanbieder, maar daar houdt de match met de bovenstaande criteria op. De interactie tussen de applicatie wordt geheel en al bepaald door de handelingen van de natuurlijke persoon en wordt deze interactie ook uitgevoerd ten behoeve van deze natuurlijke persoon.
In het algemeen zullen complexiteit en volume ook laag zijn.

6.2 Manieren van beveiliging

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

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

In tabel 1 staan enkele kenmerkende verschillen tussen kanaalbeveiliging en inhoudsbeveiliging, waar het vooral de plek betreft, waar cryptografische mechanismes worden toegepast.

Tabel 1. *Kanaalbeveiliging versus beveiliging van de inhoud*

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

Digitale certificaten zijn feitelijk altijd de basis voor cryptografische beveiliging, zowel op kanaal- als inhoudsniveau. Vaak worden ze in combinatie gebruikt. Digitale certificaten verschaffen meer zekerheid dan andere vormen van beveiliging, zoals met wachtwoorden. Landelijke voorzieningen kennen feitelijk zowel kanaalbeveiliging ((M)TLS o.b.v. PKIo) als inhoudsbeveiliging (bv. autorisatiebesluit dat de op te vragen informatie beperkt).

In de toepassing van elk grootschalig systeem worden echter meer beveiligingsmechanismes toegepast dan de bovengenoemde cryptografische mechanismes. Denk bijvoorbeeld aan autorisatiebesluiten en logische toegangsbeveiliging.

Beveiligd verkeer met digitale certificaten

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

Communicatie met basisregistraties
Overheidsinstanties hebben typisch tientallen van deze certificaten en vaak unieke certificaten per verbinding in gebruik voor de communicatie met de verschillende basisregistraties, welke verloopt via Digikoppeling (Digikoppeling is een set van standaarden, die logistieke afspraken bevat voor elektronisch berichtenverkeer tussen (overheids)organisaties). Hierbij wordt er gebruik gemaakt van een PKIoverheid-certificaat.

6.3 Wat betekent dit voor toepassing van het classificatiemodel?

Voor applicatie-applicatieverkeer is de differentiatie naar betrouwbaarheidsniveau van diensten zoals gehanteerd in de Regeling en in deze handreiking minder zinvol. In de praktijk gebruikt u hiervoor namelijk digitale certificaten. De vraag is dan wel hoe betrouwbaar die certificaten moeten zijn. In de praktijk kiest u bij voorkeur voor PKIoverheid services server certificaten, zowel voor de beveiliging van het kanaal als voor de versleuteling van de inhoud. Hoewel de Baseline Informatiebeveiliging Overheid (BIO) over de toepassing van digitale certificaten minder helder is dan voorgaande richtlijnen voor informatiebeveiliging, blijven voor deze soort toepassing PKIoverheid services certificaten de gouden standaard.

Aandachtspunten voor digitale certificaten

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

- Zorg dat u voor kritische toepassingen reservecertificaten van alternatieve certificaatdienstverleners beschikbaar heeft;
- Zorg dat u in uw organisatie meer dan één gemachtigd certificaatbeheerder heeft aangewezen. Dat is een gemachtigde die namens uw organisatie bijvoorbeeld nieuwe certificaten van verschillende certificatenverleners kan aanvragen en oude certificaten kan intrekken.
- Zorg voor een actuele en sluitende administratie van de certificaten die u toepast en de momenten waarop die verlopen, zodat u niet overvallen wordt door het verlopen van certificaten.
- Voorkom een *single-point-of-failure* om te vooromen dat er bij falen een heel proces of een hele keten tot stilstand komt.

De opkomst van apps en het mobiele ecosysteem

Zoals in de inleiding in dit hoofdstuk gesteld dient het gebruik van apps nadrukkelijk niet gelijkgeschakeld te worden met applicatie-applicatieverkeer. Maar hoe is dit dan wel te duiden?

In het algemeen is het gebruiken van een app om toegang te krijgen tot de diensten van u als dienstaanbieder het beste te vergelijken met het inloggen door een gebruiker op het portaal waarop u die dienst aanbiedt. In die gevallen zijn dan ook dezelfde eisen aan de betrouwbaarheid van de authenticatie van toepassing te verklaren, ongeacht de formele juridische situatie. Dan zijn dus ook dezelfde niveaus voor authenticatie en machtiging van de gebruiker aan de orde.

Een bijzonderheid is echter dat op de smartphone een geheel eigen ecosysteem ontstaat en de vraag ontstaat of dat nog specifieke overwegingen vraagt. Immers, een smartphone met onder meer een lock-out timer en gebruik van PIN of biometrie om het toestel te ontgrendelen, biedt een redelijk veilige omgeving om digitale diensten in te leveren.

Dit ecosysteem biedt kansen om diensten te leveren waarbij:

- Voor de authenticatie van de gebruiker wordt vertrouwd op de voorzieningen van het mobiele ecosysteem;
- Ook andere beveiligingsaspecten zoals het combineren van de diensten van meerdere dienstaanbieders en veilige lokale opslag van gegevens een goede beveiliging gelijke pas houdt met een goede gebruikerservaring.

In dat verband is het aan te bevelen om:

- Te bezien in hoeverre formeel toegelaten authenticatiemiddelen ook goed zijn in zetten ten behoeve van de authenticatie van gebruikers in relatie tot de interacterende app en applicatie.
- Waar dat niet zo is, maar er de facto wel een vergelijkbaar authenticatieniveau kan worden geboden, is te overwegen hier flexibel mee om te gaan. Het feit dat apps formeel genomen niet onder de Wdo en de eIDAS verordening vallen, biedt de mogelijkheid om hier flexibel mee om te gaan.

API's en betrouwbaarheidsniveaus

De laatste jaren kenmerken zich doordat elektronische diensten steeds vaker worden aangeboden via API's. Steeds meer overheidsdienstaanbieders omarmen API's en goede authenticatie van API's is dan ook van groot belang, temeer omdat er via API's in toenemende mate ook persoonsgegevens worden ontsloten.

In dit verband is het goed om te wijzen op de verschillende beveiligingsrichtlijnen en -standaarden die in het kader van de NL API strategie zijn of worden ontwikkeld. Het gaat hierbij bijvoorbeeld om het gebruik van de open standaard OAuth 2.0 voor authenticatie voor zowel situaties dat er sprake van een natuurlijke persoon die een applicatie bedient, maar ook situaties die meer in lijn zijn met het formele applicatie-applicatieverkeer zoals bedoeld in dit hoofdstuk. Momenteel wordt de Digikoppeling-standaard ook uitgebreid voor het veilig aansluiten op API's.


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

7 Retourstromen

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

7.1 Waar gaat het eigenlijk over?

Burgers, ondernemingen en rechtspersonen hebben het recht om u digitale berichten te sturen. Dat recht is nu nog relatief beperkt, de Wet modernisering elektronisch berichtenverkeer die per 1 januari 2026 in werking treedt zorgt voor uitbreiding naar formeel berichtenverkeer.

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

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

7.2 Wat betekent dit voor een individuele dienst?

In de Algemene wet bestuursrecht (Awb), afdeling 2.3, staan bepalingen over digitaal verkeer. Deze bepalingen zijn met betrekking tot formeel berichtenverkeer recentelijk aangevuld en geactualiseerd via de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv).

De Awb stelt dat u maatregelen moet nemen die ertoe bijdragen dat het gebruik van de elektronische weg niet tot onverwachte problemen leidt. U moet een betrouwbaar en veilig medium regelen, u moet de burger of het bedrijf notificeren met betrekking tot verzonden berichten en de burger of het bedrijf moet zelf zijn post controleren.

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

- Verzend een notificatie voor ieder verzonden bericht.
- Zorg dat het bericht of document de geadresseerde bereikt. Dit vereist in ieder geval dat als een elektronisch verzonden bericht of een notificatie niet kan worden bezorgd, dit bericht ten minste eenmaal elektronisch opnieuw moet worden verzonden. Voor een notificatie mag de verzender direct een alternatieve weg kiezen.

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

De Awb laat het aan de burger of het bedrijf over of zij via de digitale weg willen communiceren. Kiezen ze daarvoor, dan moeten ze via die weg ook bereikbaar zijn.

Met andere woorden: in de Awb zijn de gewone post en het elektronische kanaal nevengeschikt (wat betekent dat beide kanalen naast elkaar bestaan en dat burgers en ondernemers (behoudens wettelijke uitzonderingen) keuzevrijheid hebben. Het elektronische verkeer is echter op een aantal punten inmiddels verplicht en de verwachting dat deze verschuiving nog verder zal voortgaan. Daarnaast krijgen burgers en ondernemers met de Wmebv het recht om hun formele berichten elektronisch in te zenden, daarmee ontstaat de plicht voor publieke dienstverleners om dat te faciliteren.

Zie voor meer informatie het (verder in de tekst opgenomen) kader 'Verschuivingen met juridische gevolgen' in paragraaf 7.3 'Wat betekent dit voor toepassing van het classificatiemodel?'. Verder kunnen er formeelrechtelijke verplichtingen zijn waar het gaat om de beveiliging en betrouwbaarheid van die berichten, zie ook paragraaf 9.3.1 'Moet ik een elektronische handtekening ondersteunen en zo ja, welke?'.

E-mail

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

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

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

Webportaal en Berichtenbox

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

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

De keuze voor het betrouwbaarheidsniveau Laag voor beide berichtenboxen heeft als consequentie dat een bestuursorgaan zelf een afweging maakt ten aanzien van de aard van de berichten die zij in de berichtenboxen plaats (de berichtenboxen zijn minder geschikt voor (zeer) vertrouwelijke berichten).

Zwak punt blijft verder dat u afhankelijk bent van de beschikbaarheid van een actueel e-mailadres of 06-nummer om de burger of het bedrijf over nieuwe berichten te notificeren. Uiteraard heeft de burger zelf ook een belang bij een goede registratie van dergelijke bereikbaarheidsinformatie, niettemin is het een aandachtspunt. Een alternatief kan gelegen zijn in het schriftelijk notificeren over nieuwe berichten.

Applicatie-applicatieverkeer

Als u een retourbericht rechtstreeks naar de betrokken organisatie stuurt, zorgt de kanaalbeveiliging voor de gewenste zekerheden. Omdat voor applicatie-applicatiekoppelingen de bereikbaarheid van de geadresseerde

inherent goed is geregeld, is de kans groot dat het bericht ook daadwerkelijk aankomt. De kanaalbeveiliging verzekert bovendien dat buitenstaanders geen toegang kunnen krijgen tot het bericht. Een applicatie-applicatiekoppeling kan dus zeer betrouwbaar zijn.

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

7.3 Wat betekent dit voor toepassing van het classificatiemodel?

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

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

Verschuivingen met juridische gevolgen

Van breng- naar haalverplichting

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

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

Van optioneel naar verplicht kanaal

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

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

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

Belangrijk: waarmerk uw documenten

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

Zegels en tijdstempels

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

Het gaat om:

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

Eisen vanuit eIDAS

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

Hoog betrouwbaarheidsniveau

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

Standaardformaten
Voor de interoperabiliteit is het verstandig om voor het ondertekenen van documenten te werken met de standaardformaten PAdES, XAdES, CAdES en ASiC. Deze formaten zijn ook vastgelegd in het Besluit EU 2011/130 en het Uitvoeringsbesluit (EU) 2015/1506. Ze zijn in de Dienstenrichtlijn aangemerkt als de formaten die u als overheidsinstantie in ieder geval moet accepteren. Daarnaast zijn ze onder de noemer AdES Baseline Profiles verplicht aan de overheid ('Pas toe of leg uit'-verplichting) via de 'Pas toe of leg uit'-lijst van Forum Standaardisatie.

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

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


Shift

8 Gebruikservaring en eenmalig inloggen

Wat betekent gebruiksgemak voor veiligheid en betrouwbaarheid?

8.1 Gebruiksgemak in digitale dienstverlening

In het complexe Nederlandse en Europese landschap van authenticatievoorzieningen, machtigingsvoorzieningen en een breed aanbod van elektronische diensten, ligt de focus logischerwijs vooral op een goede beveiliging. Dat maakt het belang van een goede gebruikservaring echter niet minder groot. Immers, als de gebruiker door de bomen het bos niet meer ziet of met oplossing wordt geconfronteerd die minder goed werkbaar is, is de kans groot dat die gebruiker afhaakt of om te beginnen al niet gaat meedoen in de digitaliseringsgolf.

Wat zijn mogelijke bronnen van onnodige complexiteit of praktische ergernissen, die we zouden willen vermijden? En wat kunt u als dienstaanbieder daaraan doen?

Allereerst is het goed om te onderkennen dat er een aantal trends is:

- Bij het inloggen wordt voor een toenemend aantal diensten sterke authenticatie vereist. Dat zien we overal in de digitale dienstverlening, we zien het ook terug in de Regeling betrouwbaarheidsniveaus. Voor heel veel diensten wordt met die Regeling authenticatie op het niveau eIDAS Substantieel verplicht en voor echt gevoelige gegevens zoals medische dossiers zelfs eIDAS Hoog. Dit is niet louter regelzucht, het is ook van belang om gevoelige gegevens en transacties adequaat te beschermen, zeker in een tijd van toenemende cyberdreigingen.
- Om te kunnen functioneren in een maatschappij die in toenemende mate digitaliseert, is authenticatie bovendien een frequent voorkomende actie, die in de verschillende contexten op verschillende wijze moet plaatsvinden. Het ene moment logt iemand in op de digitale omgeving van zijn werkgever, het volgende moment maakt iemand gebruik van zijn privé webmail, in de avond moet iemand inloggen bij een e-commerce aanbieder om kleding te bestellen. En daarna vervult iemand mantelzorgtaken voor een familielid en raadpleegt hij een Persoonlijke Gezondheids Omgeving (PGO) en werkt hij de contracten bij voor het Persoonsgebonden Budget (PGB).

Als we de omvang en snelheid van deze ontwikkelingen zien, dan moeten we ons zorgen maken of iedereen wel mee kan blijven doen. Begrijpelijkheid en toegankelijkheid zijn dan ook terecht thema's bij het ontwikkelen van digitale dienstverlening.

In dat licht zijn de volgende principes in het algemeen aan te bevelen:

Hanteer een omnichannel aanpak in het bedienen van uw klanten.
Het is een gezond uitgangspunt dat de klant het kanaal kiest waarlangs die bediend wil worden. En in het verlengde daarvan moet het mogelijk zijn om een aanvraag of aangifte te kunnen opslaan om die op een later moment via hetzelfde of via een ander kanaal weer op te pakken.

Lever hulp op maat bij digitale dienstverlening.
Bied ondersteuning bij het afnemen van de digitale dienst, bijvoorbeeld via chat of telefoon. Zorg dat een ondersteuner daarbij de burger ook in de specifieke zaak verder kan helpen, en niet in algemene adviezen blijft hangen. Waar het echt niet anders kan, biedt de mogelijkheid om de dienst via een ander kanaal af te nemen.

Hanteer waar mogelijk een gestandaardiseerd en (her)kenbaar interactiemodel
Veel zaken verlopen via een gestandaardiseerd interactiemodel. Bijvoorbeeld rondom een aanvraag:

- Oriëntatie
- Keuze dienst
- Inloggen
- Gegevens verzamelen of aanleveren
- Aanvraag formuleren
- Samenvatten, bevestigen en eventueel ondertekenen
- Reactie dienstaanbieder en leveren dienst

Het is wenselijk dat interacties in de dienstverlening steeds zoveel mogelijk langs dergelijke standaard interactiemodellen verlopen. En dat inloggen, bevestigen (samenvatten en 'ja' knop) en ondertekenen steeds op een vergelijkbare manier verlopen. Zorg er ook voor dat de klant op elk moment in de dienst kan zien waar in het proces hij zit.

8.2 Gebruiksgemak in relatie tot authenticatie, eenmalig inloggen machtiging

Als we inzoomen op authenticaties, machtiging en dergelijke, dan zijn de volgende aspecten relevant voor gebruiksgemak:

Zorg voor een mogelijkheid van eenmalig inloggen, zeker voor toepassingen die in combinatie met elkaar gebruikt worden.
Eenmalig inloggen, ook bekend als *single sign-on* (SSO), is de mogelijkheid voor gebruikers om via één authenticatie(voorziening) toegang te krijgen

tot verschillende diensten. De gebruiker logt dan eenmaal in bij de eerste dienst en hoeft daarna niet nogmaals zijn identiteit te bevestigen voor andere diensten. Dit is bevorderlijk voor een soepele gebruikerservaring. Wel zijn er mogelijkerwijs maatregelen aan de orde als de gebruiker van de dienst van de ene dienstverlener naar de dienst van een andere dienstverlener overstapt.

Op dit punt komt het onderscheid dat er gemaakt is tussen het BSN-domein en het domein daarbuiten als potentieel pijnpunt naar voren voor sommige soorten diensten. Soms wordt een toepassing samengesteld uit diensten van dienstaanbieders die gerechtigd zijn het BSN te verwerken en diensten van dienstaanbieders die het BSN niet mogen verwerken. In het stelsel zoals we dat momenteel hebben in Nederland zien we dat hiervoor dan ook verschillende authenticatiemiddelen worden gebruikt.
Het is echter aan gebruikers niet goed uit te leggen dat er meerdere authenticatiemiddelen nodig zijn voor iets dat als één toepassing wordt ervaren. Zie ook het kader 'Voorbeeld: pijnpunt in netwerkzorg' met het voorbeeld van netwerkzorg in paragraaf 8.4 'Wat betekent dit voor toepassing van het classificatiemodel?'. Dit probleem komt hier nu naar voren, maar naar verwachting zal het ongemak van dit onderscheid in de komende jaren verder opspelen.

Zorg voor een mogelijkheid voor een gebruiker om alle actieve sessies met één handeling te beëindigen

In het algemeen zal het overstappen op een andere dienst niet zomaar leiden tot het beëindigen van de eerdere sessie. Door het open hebben staan van meerdere sessies ontstaan er wel extra beveiligingsrisico's. Denk bijvoorbeeld aan een situatie dat een gebruiker van uw diensten gebruik heeft gemaakt op een openbare locatie zoals een bibliotheek. Om dit risico goed te beheersen is het van belang dat gebruikers een mogelijkheid wordt geboden alle actieve sessies met één handeling te beëindigen. Bovendien dienen gebruikers gewezen te worden op de risico's die verbonden zijn aan het niet beëindigen van de sessie.

Zorg voor een mogelijkheid voor machtigen die goed aansluit bij de specifieke dienstverlening

Het is goed om te onderkennen dat het vaak sterk afhangt van de soort dienst of een bepaalde oplossing voor machtiging past op de situatie of niet. Wat daarbij van belang is:

- Of een dienst vele contactmomenten kent of juist incidenteel contact;
- Of de diensten uitsluitend digitaal zijn of hybride. Denk bijvoorbeeld aan het verlenen van zorg waarbij de digitale dienstverlening in het algemeen in het verlengde zal liggen van de fysieke dienstverlening;

- Wat de doelgroep is van personen die een machtiging afgeeft. Gaat het bijvoorbeeld om digibeten of personen die minder bij machte zijn hun eigen zaken te behartigen?
- Wat de motivatie is om een machtiging af te geven? Gaat het om specialistische ondersteuning (bijvoorbeeld bij fiscale intermediairs) of gaat het om zorg in situaties van minder handelingskrachtige personen.

Bovenstaande kan maken dat u vanuit het perspectief van gebruiksgemak een rol te spelen heeft in het voorzien in mogelijkheden voor het registeren en beheren van machtigingen, naast generieke voorzieningen zoals DigiD Machtigen en het gebruik van Machtigingsregisters in eHerkenning. Zie ook het hoofdstuk 5 'Machtigen' in deze handreiking.

Zorg voor een uniforme wijze waarop een gebruiker aangeeft voor zichzelf of voor een ander zaken te doen

Het is vanuit gebruiksgemak wenselijk dat de gebruiker steeds op eenzelfde wijze kan aangeven of hij voor zichzelf een dienst afneemt, of ten behoeve van iemand anders waarvoor hij gemachtigd is of wiens wettelijk vertegenwoordiger hij is.

8.3 Overige aandachtspunten voor de dienstaanbieder

Als dienstaanbieder kunt u stilstaan bij de aspecten die het gebruiksgemak verhogen, zoals benoemd in de voorgaande paragrafen. Verder is het goed om als dienstverlener in ogenschouw te nemen, die de gebruiker niet direct betreffen maar die wel samenhangen met de bovenstaande aanbevelingen. Het gaat hier om de volgende zaken:

Logische clustering van diensten.

Het is zaak om een, vanuit de gebruiker beziene, logische clustering van diensten aan te brengen, die min of meer als een samenhangende dienst kan worden afgenomen.

Hierbij ligt het voor hand om voor het cluster eenmalig inloggen mogelijk te maken. Ook valt te overwegen om machtigingen te registreren en te gebruiken die voor het gehele cluster van toepassing zijn.

Zoveel mogelijk één betrouwbaarheidsniveau per cluster, mogelijke uitzondering voor bevestiging van transacties

Ook is het logisch dat voor een dergelijk cluster één betrouwbaarheidsniveau van toepassing is. Eventueel kan ervoor gekozen worden om, als onderdeel van de gehele klantinteractie, het bevestigen van een wijziging

of een transactie apart te behandelen. Het doorvoeren van die wijziging of uitvoeren van een transactie kan dan worden voorbereid op het niveau van het cluster en via een herauthenticatie / ondertekening kan de gebruiker deze transactie bevestigen, eventueel zelfs op een hoger betrouwbaarheidsniveau.

Aansluiting bij een bestaand cluster van diensten

Een overweging die in de praktijk vaak zal spelen, is of u als dienstaanbieder zelfstandig de clustering van diensten gaat organiseren, of dat u aansluit bij een groter samenwerkingsverband met meerdere dienstverleners. Zo'n samenwerkingsverband (soms ook een federatie genoemd) kan variëren van één individuele organisatie met verschillende digitale diensten tot bijvoorbeeld een overheidsbreed portaal waar diensten van een groot aantal dienstaanbieders in zijn ondergebracht.

Overwegingen zijn dan:

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

8.4 Wat betekent dit voor toepassing van het classificatiemodel?

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

Wel speelt dat eenmalig inloggen de vorming van clusters van diensten met zich mee kan brengen of leidt tot aansluiting bij bestaande federaties. Dit kan consequenties voor u als dienstaanbieder hebben, ook waar het gaat om de keuze van een betrouwbaarheidsniveau.

Lage drempel van de Sociale Verzekeringsbank

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

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

Voorbeeld van eenmalig inloggen

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

Voorbeeld: pijnpunt in netwerkzorg

In het kader van netwerkzorg zien we in toenemende mate dat gegevens van meerdere zorgaanbieders worden gecombineerd. Ook zien we ontwikkelingen dat daarbij de gegevens met die van de patiënt worden gecombineerd en samen met de gegevens van de verschillende zorgaanbieders in één omgeving worden beheerd.

Eenmalig inloggen over verschillende zorgaanbieders heen is dan een belangrijke mogelijkheid om de oplossing gebruikersvriendelijk te houden. Ook is het dan van belang dat eenzelfde inlogmiddel zowel gebruikt kan worden voor zowel het inloggen bij de zorgaanbieders als bij een persoonlijke omgeving van de patiënt.

We zien dat een dergelijke toepassing nog tegen de grenzen aanloopt van hetgeen thans wordt geboden met generieke voorzieningen zoals DigiD en beleidsmatige afbakeningen tussen inloggen in het BSN-domein en buiten het BSN-domein. Het is zaak om bestaande beperkingen te bezien in het kader van een wenselijke gebruikerservaring.

9 Ondertekening

Heeft u een elektronische handtekening nodig voor uw dienst en zo ja, hoe geef ik dat vorm?

9.1 Inleiding

In de fysieke wereld zijn we gewend om met een grote regelmaat documenten te ondertekenen. De vraag is of dit ook een vereiste is bij digitale dienstverlening.

Dit hoofdstuk geeft antwoord op de volgende vragen:

1. Waar hebben we het over bij ondertekenen en de elektronische handtekening? (Zie paragraaf 9.2.)
2. Wat heeft u als dienstaanbieder met elektronische handtekeningen te maken? Wat moet u regelen en wat voor inrichtingskeuzes moet u maken? Hoe passen ondertekendiensten daar eventueel in? (Zie paragraaf 9.3.)
3. Overige vragen, waaronder:
   - Moet u een elektronische handtekening ondersteunen? Zo ja, welke? (zie paragraaf 9.3.1.)
   - In hoeverre kunt u het ondertekenen en het valideren van handtekeningen uitbesteden aan ondertekendiensten? (Zie paragraaf 9.3.2.)
   - Wat zijn de internationale aspecten van ondertekening? (Zie paragraaf 9.4.)

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

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

- De ondertekenaar krijgt de te ondertekenen gegevens op een eenduidige, dat wil zeggen niet voor meerdere interpretaties vatbaar, *gepresenteerd*.
- De ondertekenaar *begrijpt* de betreffende inhoud en de consequenties van ondertekening.
- Hij *bevestigt* de betreffende inhoud.
- De ondertekening levert *bewijs* op van het bovenstaande voor een derde.

Deze juridische binding vereist een zeker *ceremonieel* dat het moment van ondertekening duidelijk markeert. Het reduceert de kans op overhaast ondertekenen. In wet- en regelgeving staat vaak de eis van schriftelijkheid bij ondertekening. Schriftelijk betekent ‘met schrifttekens samengesteld’, en niet per se een fysiek document en/of een ‘natte’ handtekening.

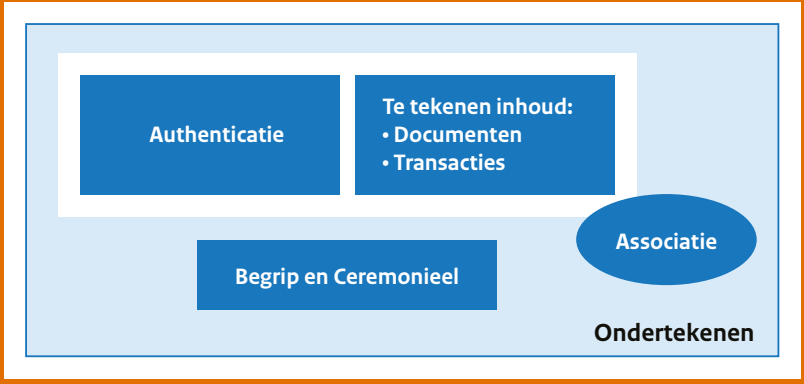
We zien dat de eisen die meer betrekking hebben op de procesmatige elementen in de wetgeving nogal onderbelicht zijn gebleven. Niettemin zullen ze vaak een overweging van de rechter zijn indien er een rechtszaak ontstaat over een elektronische handtekening.

Wat 'doet' een handtekening eigenlijk?

Het begrijpen en bevestigen van een transactie of document moet leiden tot een zogenoemde associatie. Een associatie wil zeggen dat op een betrouwbare wijze een verbinding is gekomen tussen: het ondertekende document, de identificatie en authenticatie van de ondertekenaar en de dienst of het proces waarin het document tot stand is gekomen en is ondertekend. Een elektronische handtekening is een set gegevens die logisch geassocieerd zijn met het te ondertekenen document (of andere gegevens). Met een elektronische handtekening is de bovengenoemde associatie bewijsbaar. De bewijskracht is afhankelijk van de soort elektronische handtekening die wordt gebruikt en – een slag dieper - de sterkte van de onderliggende authenticatie- en associatiemechanismen.

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

Figuur 3 *Relatie tussen identificatie, authenticatie en associatie bij een elektronische handtekening*



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

Elektronische handtekeningen in eIDAS

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

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

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

Elektronische handtekeningen die niet gekwalificeerd of geavanceerd zijn worden ook wel aangeduid als 'gewone' elektronische handtekeningen.

1. 'Gewone' elektronische handtekening

Een 'gewone' elektronische handtekening hoeft slechts te voldoen aan de eisen die impliciet zijn in de definitie. Het moet dus gaan om elektronische gegevens die door de ondertekenaar aan andere elektronische gegevens worden verbonden met als doel de wil van de ondertekenaar te bevestigen en vast te leggen. Verder worden er geen eisen aan gesteld aan de wijze waarop deze elektronische handtekening tot stand is gekomen of aan de bewijskracht die deze biedt.

2. Geavanceerde elektronische handtekening

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

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

3. Gekwalificeerde elektronische handtekening
De gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening. Maar bovendien is een gekwalificeerde elektronische handtekening

- gebaseerd op een gekwalificeerd certificaat en
- gebruikt een daarvoor gekwalificeerd middel voor het aanmaken van elektronische handtekeningen.

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

Deze drie klassen van elektronische handtekening hebben van 'gewone' tot gekwalificeerde een toenemende bewijskracht. Het is lastiger om dergelijke ondertekening te vervalsen. Het is dientengevolge ook moeilijker om een ondertekening op een later moment te ontkennen of te weerleggen; met andere woorden de *onloochenbaarheid* van een gekwalificeerde elektronische handtekening is zeer sterk terwijl die voor een 'gewone' elektronische handtekening beperkt is (en vooral door de omstandigheden in de omgeving wordt bepaald).

Een *gekwalificeerd certificaat* is een bevestiging van de identiteit van de ondertekenaar, gekoppeld aan gegevens waarmee de elektronische handtekening kan worden geverifieerd. Dat gekwalificeerde certificaat wordt door een gekwalificeerde verlener van vertrouwensdiensten uitgegeven, na een zorgvuldige identiteitsverificatie. De gekwalificeerde verlener van vertrouwensdiensten is vooraf gecertificeerd tegen Europese normen.
De identiteitsverificatie van de ondertekenaar omvat een *face-to-face* controle, steunt op een veilige wijze op een eerdere *face-to-face* controle, of omvat een *online identy proofing* procedure die vergelijkbare zekerheden oplevert als een *face-to-face* controle. De eisen aan het gekwalificeerd certificaat zijn in (een bijlage van) de eIDAS-verordening opgenomen. Het voert te ver om die hier integraal te behandelen. Uitgevers van gekwalificeerde certificaten dienen, net als andere leveranciers van gekwalificeerde vertrouwensdiensten, zelf ook gekwalificeerd te zijn. Dat betekent dat zij als organisatie ook onder toezicht van de Rijksinspectie Digitale Infrastructuur (RDI) staan.

De gegevens om de elektronische handtekening aan te maken worden door het gebruik van een *gekwalificeerd middel* beschermd tegen uitlekken, kopiëren of misbruik door derden. Het betreft hier concreet een geheim te houden cryptografische sleutel, die alleen door de legitieme ondertekenaar mag worden gebruikt. Een gekwalificeerd middel geeft een hoge mate van bescherming tegen het lekken of het misbruiken van die cryptografische sleutel, situaties die ertoe zouden kunnen leiden dat een onbevoegde derde een elektronische handtekening zou kunnen vervalsen. Een gekwalificeerd middel kan een smartcard of USB-cryptotoken zijn, maar er zijn ook andere vormfactoren mogelijk. Zo maken online ondertekendiensten veelal gebruik van (gecertificeerde) Hardware Security Modules (HSM), die de cryptografische sleutels waarmee een elektronische handtekening gezet kan worden.
De eIDAS verordening biedt bovendien ruimte voor het inrichten van de opslag, het beheer en het gebruik van die cryptografische sleutels. Waar onder de eerdere Richtlijn elektronische handtekeningen controle over het sleutelmateriaal ook het *fysiek bezit van de gegevens waarmee wordt ondertekend* impliceerde, is dit het met de introductie van de eIDAS Verordening zo dat *logische beheersing* volstaat. Zodoende is het ook mogelijk geworden om cryptografische sleutels elders op te slaan, te beheren en te gebruiken, wat de weg heeft geopend voor online ondertekendiensten (zie ook paragraaf 9.3.2 ‘Praktische ondersteuning van elektronische handtekeningen’). Deze zijn in breed beschikbaar op het niveau geavanceerd en in beperkte mate op het niveau gekwalificeerd.

Rechtsgeldigheid van elektronische handtekeningen

- Qua rechtsgevolg is de gekwalificeerde elektronische handtekening gelijk aan de handgeschreven handtekening.
- Ook andere elektronische handtekeningen kunnen een rechtsgevolg hebben en dienen als bewijsmiddel. Het kale feit dat ze elektronisch zijn of niet voldoen aan de eisen voor gekwalificeerde elektronische handtekeningen doet daar niets aan af.

In Nederland is in het Burgerlijk Wetboek (BW) een iets bredere gelijkstelling van de elektronische handtekening met de handgeschreven handtekening opgenomen. Dit geeft een concretere invulling aan het tweede hiervoor genoemde punt. Het BW refereert aan elektronische handtekeningen zoals bedoeld in de eIDAS-verordening, en stelt dat naast de gekwalificeerde handtekening andere elektronische handtekeningen dezelfde rechtsgevolgen hebben als de handgeschreven handtekening, mits ze voldoende betrouwbaar zijn voor de dienst waar ze voor worden gebruikt.

Bij processen en transacties met minder grote rechtsgevolgen of minder grote andere consequenties kan derhalve worden volstaan met een eenvoudige elektronische handtekening (een elektronische handtekening, niet zijnde een geavanceerde elektronische handtekening), terwijl voor transacties waarvan de rechtsgevolgen of consequenties groter zijn een geavanceerde of gekwalificeerde elektronische handtekening nodig is.

Belang van het ondertekenproces en de omgeving

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

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

- Hoe waarschijnlijk is het dat de elektronische handtekening daadwerkelijk is gezet door de ondertekenaar aan wie die handtekening wordt toegeschreven? (Was het de ondertekenaar wel echt zelf?)
- Is het ondertekenproces zo ingericht dat de ondertekenaar zich bewust is van de inhoud en de gevolgen van wat hij ondertekend heeft?

- Is er een betrouwbare tijdsaanduiding gebruikt bij het moment van ondertekenen, zoals bijvoorbeeld een tijdstempel, of was de tijdsindicatie zuiver bepaald door de ondertekenaar?
- Wat is de sterkte van het associatiemechanisme, dat wil zeggen hoe zeker is het dat de elektronische handtekening ook daadwerkelijk bij de ondertekende gegevens of het ondertekende document hoort?

9.3 Elektronische handtekeningen voor u als dienstaanbieder

9.3.1 Moet ik een elektronische handtekening ondersteunen en zo ja, welke?

Het is om te beginnen de vraag of u überhaupt elektronische handtekeningen nodig heeft voor uw dienstverlening. In het algemeen gaat het om situaties, waarin u als dienstaanbieder moet bepalen of u personen wellicht om een handtekening moet vragen. Daarbij zijn de volgende zaken relevant:

Wat is de formeelrechtelijke situatie?

- Dwingt wet- en regelgeving u om digitale stukken te accepteren die ondertekend moeten zijn?
  Met de Wet modernisering elektronisch bestuurlijk verkeer, worden bestuursorganen verplicht om digitale berichten vanuit de maatschappij te ontvangen en te behandelen, behoudens enkele uitzonderingen. Waar het openstellen van de elektronische weg voor inkomende berichten tot voorheen nog vrijblijvend was, moeten bestuursorganen hier nu actief mee aan de gang.
- Dwingt wet- en regelgeving u om gebruik te maken van ondertekening, zonder dit nader te specificeren?

Een verplichting tot toepassing van elektronische handtekeningen kan door u als dienstverlener of door de wetgever (casu quo regelgever) worden voorgeschreven. Zie de Algemene wet bestuursrecht (AWB, art. 2:16 en verder). Indien een elektronische handtekening wordt voorgeschreven, dan kunt u te maken hebben met extra eisen rond de veiligheid en betrouwbaarheid van de ondertekening. Denk bijvoorbeeld aan het niveau van authenticatie dat nodig is om de elektronische handtekening aan te maken of aan de onafhankelijkheid en veiligheid van de ondertekening. Ook kunnen er aanvullende eisen gelden met betrekking tot de eenvoudige elektronische handtekening die bijvoorbeeld met een tablet of touch screen wordt gezet.

Begrijpen en bevestigen en de rol van ceremonieel. Goed proces en 'ja'-knop als alternatief.

Zoals gezegd is bij ondertekening niet altijd de bewijskracht waar het om draait, maar het ceremonieel waarin de ondertekenaar begrijpt waar hij zich aan verbindt en dit in vol bewustzijn bevestigt.

Is hiervoor altijd een elektronische handtekening nodig in de klassieke zin? Of volstaat hiervoor ook een samenvatting van de relevante gegevens en is een bevestiging via een ja knop op een website voldoende? En kan de bescherming tegen een onverhoopte latere ontkenning ook eenvoudig worden geregeld door een bevestiging van de transactie te sturen aan de ondertekenaar?

In heel veel processen zal het antwoord hierop positief zijn, bijvoorbeeld als de rechtgevolgen vooral vallen in de relatie tussen ondertekenaar en het bestuursorgaan in kwestie en indien rechtsgevolgen ook omkeerbaar zijn als blijkt dat er bijvoorbeeld sprake is van een onjuiste of valse aangifte.

Maar bij bijvoorbeeld het tekenen van een contract ligt het anders. Dan hebben beide partijen behoefte aan een getekend document dat ze op verschillende plekken kunnen overleggen. Dan gaan bewijskracht en de analogie met de papieren wereld de bovenhand voeren en is een expliciete elektronische handtekening op een elektronisch document noodzakelijk.

Om een 'ja'-knop zoveel mogelijk als een elektronische handtekening te kunnen beschouwen, is aan te bevelen de volgende zaken in de systemen vast te leggen:

- Wat zijn de te ondertekenen gegevens precies?
- Wat is het ondertekenmoment?
- Op welke wijze heeft de ondertekenaar zijn identiteit kenbaar gemaakt en op welke wijze is die identiteit verifieerd?
- Eventueel bewijs van de identiteitsverificatie of authenticatie.

Analogie met de papieren situatie

Vraagt u een handtekening in uw traditionele 'papieren' dienstverlening? Dan hoeft dat niet automatisch te betekenen dat u dan ook moet doen in uw elektronische dienstverlening. Op papier kan een handtekening namelijk een andere functie hebben. Bijvoorbeeld ceremonieel, om de ondertekenaar ervan te doordringen dat hij zich aan iets verbindt. Of ter bevestiging van de opgegeven identiteit, zoals met authenticatie bij elektronische dienstverlening. Ga daarom niet zomaar van de papieren situatie uit. Vraag u eerst af wat het doel en nut zijn van de handtekening op papier voordat u die ondertekening één op één vertaalt naar een elektronische handtekening.

Ja, ik heb echt een elektronische handtekening nodig. Maar welke kies ik dan?

Goed, u heeft vastgesteld dat u echt een elektronische handtekening nodig heeft. Bijvoorbeeld omdat er een kans is op disputen of omdat u de ondertekenaar een valse aangifte wilt kunnen tegenwerpen.

We constateren dat in die situaties een simpele elektronische handtekening niet zal volstaan omdat de onloochenbaarheid van de ondertekening belangrijk is. Ook speelt dan dat het ten overstaan van een derde eenvoudig moet zijn om de ondertekening vast te kunnen stellen. Of die derde nu een rechter is of een andere persoon.

Eigenlijk wordt de keuze tussen het niveau van geavanceerde of gekwalificeerde elektronische handtekening vooral bepaald door:

- De zwaarte van de gevolgen. In de zin van economisch belang of wijziging van gegevens in basisregistraties.
- De omkeerbaarheid van de gevolgen.
- De sanctioneerbaarheid van het doen van een valse opgave.

Zijn de gevolgen zwaarwegend, en is de omkeerbaarheid beperkt, dan is het aan te bevelen te kiezen voor een gekwalificeerde elektronische handtekening. In de andere gevallen is meestal te volstaan met een geavanceerde elektronische handtekening.

Dit gezegd hebbende: een gekwalificeerde elektronische handtekening is ook bruikbaar in die situaties dat een geavanceerde elektronische handtekening zou volstaan.

Het bovenstaande lezende, zou men denken dan altijd een keuze te maken voor een gekwalificeerde elektronische handtekening? De praktijk is echter dat de ondertekenaar hiervoor in de huidige situatie kosten zal moeten maken, waarmee zeker incidenteel gebruik voor hoogwaardige transacties snel buiten beeld geraakt. De adoptie van de EU Digital Identity (EUDI) Wallet zou hier verandering in moeten brengen. Die EUDI Wallet gaat de mogelijkheid bieden om, zonder kosten voor de (burger als) ondertekenaar, een gekwalificeerde handtekening te zetten. Dit zal de afweging tussen een geavanceerde en een gekwalificeerde handtekening in de loop van de tijd (vanaf 2027 naar verwachting) doen verschuiven.

Voorbeeldcasus: subsidieverstrekker

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

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

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

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

Voorbeeldcasus: uitzendbranche en payrolling

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

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

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

9.3.2 Praktische ondersteuning van elektronische handtekeningen

Variëteit aan kanalen

Zoals ook onder paragraaf 7.2 'Wat betekent dit voor een individuele dienst?' is aangegeven zijn er meerdere mogelijkheden om inkomend berichtenverkeer mogelijk te maken:

- Voor burgers is een webportaal of een app het meest voor de hand liggend;
- Daarnaast is, zeker in interactie met bedrijven, applicatie-applicatieverkeer zeer goed mogelijk;
- Ten slotte is het ook denkbaar dat men als bestuursorgaan te maken krijgt met stukken die per elektronische post worden ingezonden.

Volgens de Awb dienen officiële inkomende berichten in het algemeen schriftelijk en ondertekend te zijn, of deze nu via applicatie-applicatieverkeer binnenkomen of via email.

Allereerst is het goed om te beseffen dat het u als dienstverlener met de Wet modernisering elektronisch bestuurlijk verkeer vrij staat om aan te geven langs welke kanalen berichten dienen te worden verstuurd en hoe aan de eisen van vertrouwelijkheid en betrouwbaarheid kan worden voldaan. U hoeft dus niet alle mogelijk kanalen en vormen van berichten te ondersteunen in uw dienstverlening. Maar soms is dat in het kader van het bieden van goede dienstverlening wel nodig.

Gebruik van ondertekendiensten

Traditioneel zorgde de ondertekenaar zelf voor zijn elektronische handtekening. De ondertekenaar had bij een trust service provider een certificaat gekocht en hij had tevens gezorgd voor software om een handtekening te zetten. Voor de feitelijke ondertekening doorliep hij een passend proces, dat onjuiste of overhaaste ondertekening vermijdt, iets dat of door de ondertekenapplicatie of door de procedure daaromheen werd geregeld.

Het bovenstaand traditionele implementatiemodel functioneert technisch goed, maar de implementatielast vormt een grote drempel voor breed gebruik, zeker voor burgers of kleine bedrijven. De verschillende voortgangsrapportages over de adoptie van de elektronische handtekening hebben dit duidelijk gemaakt. En intussen maakte een strikte interpretatie van de regels onder de eerdere Richtlijn elektronische handtekeningen (door de toezichthouders) het niet mogelijk om elektronische handtekeningen op betrouwbare niveaus op een andere manier te implementeren.

Sinds de eIDAS Verordening is dit wezenlijk veranderd. Een groot aantal aanbieders van online ondertekendiensten heeft zich op de markt begeven. Soms betreft dat generieke ondertekendiensten, soms ook specifieke ondertekendiensten in bepaalde sectoren. Daarmee zijn deze diensten inmiddels de praktijkstandaard geworden voor het incidenteel ondertekenen van documenten.

De ondertekendienst verzorgt het proces van het presenteren van het te tekenen bericht, het ceremonieel en het technisch aanmaken van de elektronische handtekening (de associatie). De ondertekenaar hoeft dus uitsluitend te beschikken over een authenticatiemiddel van voldoende betrouwbaarheid. Voor het hoogste niveau, de gekwalificeerde elektronische handtekening, bevat de ondertekendienst veelal ook het gekwalificeerde certificaat. Vaak worden die gekwalificeerde certificaten aangemaakt na een biometrische identiteitsverificatie op afstand, een andere wezenlijke vernieuwing die inmiddels breed is geadopteerd.

Gebruik maken van een ondertekendienst kan de ondertekenaar en diens organisatie dus ontzorgen. Voor u als dienstaanbieder geldt dat eveneens: een ondertekendienst kan zorgen dat elektronische handtekeningen die u ontvangt van de juiste betrouwbaarheid en in het juiste formaat zijn en dat het ondertekenproces zorgvuldig is geweest.

Als het gaat om elektronische handtekeningen die u als dienstverlener ontvangt, dan heeft u wat betreft ondertekendiensten de volgende mogelijkheden:

- Niets doen. U geeft slechts aan wat voor soort handtekening u wenst te ontvangen. De partij die iets moet ondertekenen moet er dan voor zorgen dat deze over de handtekening beschikt die uw organisatie vraagt.
- Verwijzen. U verwijst naar onafhankelijke ondertekendiensten. De partij die iets moet ondertekenen kan, als deze zelf niet over een elektronische handtekening beschikt, dan terecht bij de ondertekendienst om iets te ondertekenen.
- Zelf doen. U implementeert zelf een ondertekendienst voor uw elektronische dienstverlening. De partij die iets moet ondertekenen kan dit dan in uw digitale omgeving doen waarbij uw organisatie verantwoordelijk is voor de ondertekening.
- Integreren. U contracteert een ondertekendienst voor uw elektronische dienstverlening. De partij die iets moet ondertekenen kan vanuit uw digitale omgeving gebruik maken van een ondertekendienst die door een externe partij wordt verzorgd.

Alles overziend vormen ondertekendiensten een interessante vorm van dienstverlening die de implementatielast van de elektronische handtekening vermindert. Niet alleen voor de ondertekenaar, maar ook voor u als dienstaanbieder.

Webportalen. 'Ja'-box of ondertekendienst?

Bij webportalen is de voornaamste vraag of volstaan kan worden met een 'ja'-box of dat een geavanceerde of gekwalificeerde handtekening gezet moet worden. Zie voor deze keuze de verhandeling in paragraaf 9.3.1. 'Moet ik een elektronische handtekening ondersteunen en zo ja, welke?'.

En, mocht het nodig zijn gebruik te maken van een geavanceerde of elektronische handtekening, dan is het zinvol om de hiervoor opgenomen tekst aangaande het gebruik van ondertekendiensten te lezen.

Applicatie-applicatieverkeer.

Het kan zo zijn dat u om juridische redenen onloochenbaarheid wenst van berichten die u als dienstaanbieder via applicatie-applicatieverkeer ontvangt. De vraag is echter of u dit wenst te regelen middels een elektronische handtekening of een elektronisch zegel.

In de praktijk is er altijd sprake van een situatie van een aansluiting van een applicatie voor formeel elektronisch berichtenverkeer. In die situatie kent u de aansluitende partij en kunt u voorwaarden overeenkomen, die erop neerkomen dat berichten die via de aangesloten applicatie worden aangeleverd als authentiek worden beschouwd. In essentie zijn daarmee 'open' juridische kaders zoals voor de elektronische handtekening (zoals ook in de eIDAS Verordening opgenomen) minder relevant. Uiteraard ontslaat u dit niet van technische maatregelen om vervalsing van berichten tegen te gaan, maar latere ontkenning van berichten speelt in veel mindere mate.

Email verkeer

Zoals aangegeven bij paragraaf 7.2. 'Wat betekent dit voor een individuele dienst?' is email als vrij formaat inkomend bericht minder geschikt om als dienstverlener te ondersteunen. Derhalve gaan we hier niet in detail in op het handelingsperspectief.

9.4 Internationale aspecten

eIDAS regelt een aantal grensoverschrijdende zaken:

- De gekwalificeerde elektronische handtekening is in alle lidstaten uniform gedefinieerd. De essentiële eisen voor die gekwalificeerde elektronische handtekening zijn EU-breed vastgesteld. De juridische

status van deze handtekening is bovendien in alle lidstaten gelijk.
- Voor grensoverschrijdend verkeer is het niet toegestaan een hoger niveau te vereisen dan de gekwalificeerde elektronische handtekening, of anderszins aanvullende eisen te stellen. Er bestaat overigens ook geen gestandaardiseerd niveau boven het niveau 'gekwalificeerd'.
- Vereist u als dienstaanbieder minimaal een geavanceerde elektronische handtekening? Dan moet u elektronische handtekeningen en zegels op dit en op hogere betrouwbaarheidsniveaus accepteren (zie de eIDAS-verordening, artikel 27).
- U bent als ontvanger van elektronische handtekening bovendien verplicht een aantal formaten van elektronische handtekeningen te ondersteunen, in casu de XAdES-, PAdES- en CAdES- en de ASiC standaarden (zie het EU-uitvoeringsbesluit 2015/1506). In dit verband is het ook goed om te wijzen op de Ades Baseline Profiles voor deze standaarden, verplicht zijn aan de overheid ('Pas toe of leg uit'-verplichting) via de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. Deze regelen het correcte gebruik van deze zogenaamde AdES ondertekeningsformaten.

Handtekening binnen de Dienstenrichtlijn

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

Internationale handtekeningen

Heeft u te maken met een geavanceerde elektronische handtekening op basis van een gekwalificeerd certificaat? Of met een gekwalificeerde elektronische handtekening? Dan zijn die in de hele EU geldig. U moet deze accepteren, in ieder geval als deze voldoen aan de gestandaardiseerde Ades formaten voor elektronische handtekeningen.

Overigens kunt u ook andere elektronische handtekeningen niet zonder meer weigeren, gelet op het feit dat elektronische handtekeningen geen rechtsgevolg kunnen worden ontzegd, louter omdat ze elektronisch zijn of niet voldoen aan bepaalde betrouwbaarheidseisen. De handtekening moet dus worden geaccepteerd tenzij er goede redenen zijn om dat niet te doen. Wel mag u als dienstverlener een bepaald betrouwbaarheidsniveau van de elektronische handtekening vereisen voor uw elektronische dienst.

Bijlage 1 Juridisch kader: relevante wet- en regelgeving

1. Juridisch kader vereiste betrouwbaarheidsniveaus inlogmiddelen digitale diensten krachtens de (U)AVG

Recht op bescherming van persoonsgegevens: (U)AVG

De verwerking van persoonsgegevens is een beperking van het recht op de bescherming van de *persoonlijke levenssfeer* in de zin van artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM), artikel 17 van het Internationaal verdrag inzake burgerlijke en politieke vrijheden, artikel 7 van het EU-Handvest en artikel 10 van de Grondwet.

Daarnaast is het recht op bescherming van *persoonsgegevens* opgenomen in artikel 8 van het EU-Handvest en artikel 16 van het verdrag betreffende de werking van de EU (VWEU). De verwerking van persoonsgegevens moet voldoen aan de eisen die uit deze artikelen voortvloeien. Voor artikel 7 van het EU-Handvest geldt dat het in principe dezelfde reikwijdte en inhoud heeft als artikel 8 van het EVRM. Zoals beschreven in overweging 1 en 12 van de AVG zijn artikel 8 van het EU-Handvest en artikel 16 van het VWEU (op basis van artikel 16, tweede lid VWEU) uitgewerkt in de AVG en overige regelgeving.

Passende technische en organisatorische maatregelen

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) - in het Engels ook wel de *General Data Protection Regulation* (GDPR) genoemd - rechtstreeks van toepassing in alle lidstaten van de EU en de Europese Economische Ruimte (EER). Het doel van de AVG is om twee belangen te waarborgen: de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens en het vrije verkeer van persoonsgegevens binnen de EER. De UAVG geeft in Nederland uitvoering aan de AVG (artikel 1 AVG).

De AVG vereist dat persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze worden verwerkt (artikel 5, eerste lid, sub a AVG). Persoonsgegevens moeten door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5, eerste lid, sub f, AVG). Zie tevens artikel 32 AVG dat de verwerkingsverantwoordelijke en verwerker verplicht de persoonsgegevens die worden verwerkt te beveiligen door passende technische en organisatorische maatregelen

te treffen. Hierbij dient rekening te worden gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen (zie ook artikel 25, eerste lid, AVG en overweging 83 van de AVG). Wat passende maatregelen zijn hangt dus af van de specifieke verwerking en de risico's die daarmee gepaard gaan, zoals ook wordt toegelicht in de 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming' par. 5.8 .

Juistheid en actualiteit

Verder moeten maatregelen worden getroffen waarmee wordt geborgd dat de persoonsgegevens die verwerkt worden juist en actueel zijn. Dit volgt uit artikel 5, eerste lid, aanhef en onder d, AVG. Zie ook overweging 39 AVG: "Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist.".

Bijzondere categorieën van persoonsgegevens

Voor de verwerking van de zogeheten bijzondere categorieën van persoonsgegevens gelden specifieke eisen. Het gaat om persoonsgegevens die naar hun aard gevoelig zijn. Het zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid. Het verwerken van bijzondere categorieën van persoonsgegevens is verboden, tenzij een van de uitzonderingen genoemd in artikel 9, tweede lid, van de AVG van toepassing is (artikel 9 AVG in samenhang bezien met de artikelen 22 tot en met 30 UAVG). Deze uitzonderingen zijn op nationaal niveau nader uitgewerkt in paragraaf 3.1 van de UAVG.

2. *Wet digitale overheid (kaderwet)*

De Wet digitale overheid (Wdo) regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een substantiële of hoge mate van betrouwbaarheid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit (zie ook het onderwerp 'Wet digitale overheid' op de website DigitaleOverheid.nl). De Wdo maakt het mogelijk om via publieke én private inlogmiddelen digitaal zaken te doen met bijvoorbeeld gemeenten (voor

zover deze middelen onder de reikwijdte van de Wdo vallen). Alleen middelen die door de overheid op veiligheid en betrouwbaarheid zijn gecontroleerd worden toegelaten, zoals is te lezen via DigitaleOverheid.nl. Die zijn dan in het publieke domein toegestaan. Hoewel inloggen bij diensten van commerciële/private partijen zoals webwinkels niet in de Wdo wordt geregeld, wordt aangegeven dat het de bedoeling is dat burgers met de gecontroleerde private middelen ook daar kunnen inloggen.

Na (volledige) inwerkingtreding geldt voor de organisaties die onder de reikwijdte van de Wdo vallen onder andere dat:

- zij hun digitale diensten moeten indelen naar betrouwbaarheidsniveaus;
- zij een acceptatieplicht hebben voor toegelaten inlogmiddelen; en
- zij hun informatiebeveiliging op orde moeten hebben.

De Wdo sluit aan bij Europese ontwikkelingen in digitale overheidsdienstverlening en inloggen bij de overheid. De toe te laten publieke en private inlogmiddelen moeten voldoen aan de Europese eisen (i.c. de eIDAS-verordening).

De Minister van BZK is verantwoordelijk voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur (artikel 5 Wdo) (Stelsel Toegang). De techniek (ICT) en de organisatie achter het Stelsel Toegang zijn momenteel in ontwikkeling. Zodra dit gereed is, is het stelsel toegankelijk voor dienstverleners en kunnen inlogmiddelen erkend worden.

De Wdo is een kaderwet, uitwerking vindt plaats in de lagere regelgeving, zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen. Hiervoor is gekozen om ruimte te laten voor innovatie, verdere keuzes en nieuwe voorzieningen en functionaliteiten.

2.1 Gefaseerde invoering Wdo

De eerste deel van de Wdo is op 1 juli 2023 in werking getreden. Onderstaand worden de voor het vraagstuk van deze handreiking meest relevante onderdelen beschreven. In paragraaf 2.2 van deze bijlage zal nader worden ingegaan op het tweede deel Wdo: acceptatieplicht en toegelaten middelen.

Betrouwbaarheidsniveaus: artikel 6 Wdo

Artikel 6 Wdo ziet op de betrouwbaarheidsniveaus als het gaat om toegang tot elektronische dienstverlening. De Wdo volgt de betrouwbaarheidsniveaus van de eIDAS-verordening: laag, substantieel en hoog.

In het eerste lid is geregeld dat bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, bestuursorganen en aangewezen organisaties uitsluitend toegang tot de dienstverlening verlenen indien gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben.

In artikel 6, tweede lid, Wdo is opgenomen dat bestuursorganen en aangewezen organisaties volgens bij ministeriële regeling te stellen regels bepalen voor welke door hen te verlenen elektronische diensten authenticatie op een bepaald betrouwbaarheidsniveau vereist is. Dit is nader uitgewerkt in de Regeling Betrouwbaarheidsniveaus authenticatie elektronische dienstverlening (Regeling betrouwbaarheidsniveaus).

Regeling betrouwbaarheidsniveaus

(Semi-) overheidsdiensten moeten de diensten die zij verlenen en waarbij elektronische toegang mogelijk is indelen in betrouwbaarheidsniveau laag, substantieel of hoog. In de Regeling betrouwbaarheidsniveaus worden nadere regels gesteld over de criteria die door publieke dienstverleners moeten worden gehanteerd (zie Toelichting bij het Conceptbesluit identificatiemiddelen, par. 2.2). Deze regeling is 1 juli 2023 in werking getreden.

Op grond van artikel 2, tweede lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau hoog vereist is als het gaat om gegevens die onder het medisch beroepsgeheim vallen.

Op grond van artikel 2, derde lid, Regeling betrouwbaarheidsniveaus juncto bijlage 2 bij de Regeling betrouwbaarheidsniveaus wordt geconcludeerd dat (in het geval niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is) betrouwbaarheidsniveau substantieel vereist is als het om bijzondere categorieën van persoonsgegevens (zoals gegevens over gezondheid; artikel 1 Regeling betrouwbaarheidsniveaus juncto artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming en artikel 9, eerste lid, AVG) gaat.

In bijlage 2 bij de Regeling betrouwbaarheidsniveaus is daarnaast opgenomen als criterium voor betrouwbaarheidsniveau hoog dat het BSN wordt verwerkt in combinatie met andere persoonsgegevens.

Vaststellen betrouwbaarheidsniveau dienst één niveau lager

Risicoverlagende factoren
In artikel 3, eerste lid, Regeling betrouwbaarheidsniveaus is geregeld dat een bestuursorgaan of aangewezen organisatie voor een elektronische dienst authenticatie op één betrouwbaarheidsniveau lager kan vaststellen, indien:

a. het proces van toegangsverlening voorziet in een adequate aanvullende technische of fysieke controle op de authenticiteit van de gebruiker van het identificatiemiddel na het moment waarop daarmee voor de eerste keer voor de desbetreffende dienst een authenticatie is uitgevoerd;
b. het bestuursorgaan of de aangewezen organisatie in het proces herstelmaatregelen neemt of kan nemen.

Als artikel 3, eerste lid, Regeling betrouwbaarheidsniveaus wordt toegepast sluit dit gelijktijdige toepassing van artikel 6 Regeling betrouwbaarheidsniveaus uit (artikel 3, tweede lid, Regeling betrouwbaarheidsniveaus; zie ook artikel 6, tweede lid, Regeling betrouwbaarheidsniveaus).

Risicoverhogende factoren
In artikel 4 Regeling betrouwbaarheidsniveaus is geregeld dat indien naar het oordeel van het bestuursorgaan of de aangewezen organisatie, gelet op de aard van de dienst, sprake is van risicoverhogende factoren, waaronder identiteitsfraude of misbruik van de dienst, wordt een volledige risicoanalyse uitgevoerd teneinde het passende betrouwbaarheidsniveau voor die dienst te kunnen bepalen.

Tijdelijk één betrouwbaarheidsniveau lager
Artikel 6, vierde lid, Wdo biedt de mogelijkheid om bij ministeriële regeling regels te stellen over het gedurende een bepaalde periode toestaan van toegang tot diensten, waarvoor volgens de krachtens het tweede lid gestelde regels authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, met gebruikmaking van door de Minister van BZK aangewezen identificatiemiddelen die het betrouwbaarheidsniveau laag respectievelijk substantieel hebben.

Dit is nader uitgewerkt in artikel 6, eerste lid, Regeling betrouwbaarheidsniveaus. Hierin is opgenomen dat onverminderd de toepasselijkheid van een wettelijk voorschrift dat bepaalt dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is, een bestuursorgaan of aangewezen organisatie, indien de beschikbaarheid of het gebruik van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog of de mogelijkheid om deze te gebruiken om toegang te krijgen

tot dienstverlening onvoldoende is, voor een elektronische dienst, waarvoor authenticatie op betrouwbaarheidsniveau hoog respectievelijk substantieel benodigd is, tot twee jaar na inwerkingtreding van de Regeling betrouwbaarheidsniveaus voor toegang tot die dienst tevens het gebruik van een toegelaten of erkend middel op betrouwbaarheidsniveau substantieel respectievelijk een middel op betrouwbaarheidsniveau laag kan toestaan. Gelijktijdige toepassing met artikel 3 Regeling betrouwbaarheidsniveaus wordt uitgesloten (zie artikel 6, tweede lid, Regeling betrouwbaarheidsniveaus; zie ook artikel 3, tweede lid, Regeling betrouwbaarheidsniveaus).

Voor dit artikel lijkt het uitgangspunt te zijn geweest dat het Stelsel Toegang gereed zou zijn bij de inwerkingtreding van de Regeling betrouwbaarheidsniveaus en dat er toegelaten of erkende middelen beschikbaar zouden zijn (koppeling lager niveau aan toegelaten en erkende middelen). Dat is tot op heden nog niet het geval. Onduidelijk is daarmee hoe dit artikel in de praktijk moet worden geïnterpreteerd. Wellicht zal de overgangsperiode van twee jaar worden verlengd nadat toegelaten of erkende middelen beschikbaar zijn.

Uit gesprekken komt naar voren dat nog niet duidelijk is wanneer het stelsel gereed is. Er wordt voorzien dat het meer tijd zal kosten dan in de oorspronkelijke planning opgenomen. Het Stelsel Toegang zal naar verwachting niet eerder dan in 2025 gereed zijn. Dat betekent dat het stelsel toegankelijk voor dienstverleners zou moeten zijn en dat inlogmiddelen erkend kunnen worden. Het is de bedoeling dat alle dienstverleners in de komende 3 jaar aansluiten op het stelsel.

2.2 Tweede deel Wdo: acceptatieplicht, toegelaten middelen

Voor de volgende fase van de Wdo is van belang dat de ontwikkeling van de ICT en de organisatie achter het Stelsel Toegang afgerond zijn.
De tweede fase van de Wdo zal onder andere het volgende regelen:

- een acceptatieplicht voor toegelaten identificatiemiddelen en digitale machtigingsverklaringen; en
- de informatiebeveiliging moet op orde zijn (zie artikel 4, Wdo).

Voor de hierboven genoemde acceptatieplicht geldt dat artikel 7 Wdo nog niet in werking is getreden. Een toegelaten identificatiemiddel wordt in de Wdo omschreven als een identificatiemiddel voor een natuurlijke persoon dat is aangewezen ingevolge artikel 9 Wdo.

Artikel 7 Wdo, acceptatieplicht (nog niet in werking)

In artikel 7, tweede lid, Wdo is het volgende opgenomen: aangewezen organisaties accepteren bij hun elektronische dienstverlening aan natuurlijke personen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is uitsluitend:

a. alle toegelaten identificatiemiddelen;
b. elektronische verklaringen als bedoeld in artikel 5, eerste lid, onderdeel b; en
c. onverminderd het bepaalde in artikel 6 van de eIDAS-verordening, alle identificatiemiddelen die behoren tot een door een lidstaat van de EU ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel indien dit is bepaald bij besluit van Onze Minister in overeenstemming met Onze Minister die het mede aangaat.

Dit betekent voor alle dienstaanbieders dat nadat de acceptatieplicht van kracht is uitsluitend toegelaten en erkende identificatiemiddelen gebruikt mogen worden. Niet toegelaten en niet-erkende middelen mogen daarmee dus niet meer worden geaccepteerd.

Inwerkingtreding acceptatieplicht art. 7 Wdo

In artikel 29, derde lid, Wdo wordt bepaald dat de in de artikel 7 Wdo opgenomen acceptatieplicht voor een aangewezen organisatie niet eerder van toepassing is dan nadat die aangewezen organisatie kan worden aangesloten op de in artikel 5, eerste lid, onderdelen a tot en met e, en tweede lid Wdo bedoelde infrastructuur en voorzieningen overeenkomstig het bij regeling van Onze Minister, gehoord Onze Ministers die het mede aangaat, op te stellen aansluitschema. Het aansluitschema kan erin voorzien dat de acceptatieplichten voor verschillende diensten van een bestuursorgaan of aangewezen organisatie op verschillende momenten van toepassing worden.

Dit betekent dat ook nadat de acceptatieplicht in artikel 7 Wdo in werking treedt, deze niet eerder van toepassing is dan nadat er ook daadwerkelijk kan worden aangesloten op het Stelsel Toegang. Dit zal dan plaatsvinden op basis van een aansluitschema. De Wdo gaat dus pas volledig gelden als een instantie technisch en organisatorisch klaar is om aan te sluiten.
De departementen, de publieke dienstverleners en Logius stellen samen een aansluitschema op. Dit aansluitschema gaat een planning bevatten met data waarop de specifieke onderdelen van de wet voor elke instantie van kracht worden.

Afwijking acceptatieplicht art. 7 Wdo

In artikel 7, vierde lid, Wdo is een mogelijkheid opgenomen om af te wijken van de acceptatieplicht indien dit noodzakelijk is gelet op de aard van de dienstverlening of de aard van de doelgroep. Een aangewezen organisatie kan volgens bij ministeriële regeling te stellen regels voor een welbepaalde doelgroep afwijken van het gestelde in het eerste lid, onderdeel a, respectievelijk het tweede lid onderdeel a, indien acceptatie van niet-toegelaten identificatiemiddelen onder uitsluiting van toegelaten identificatiemiddelen noodzakelijk is gelet op de aard van de dienstverlening of de aard van de doelgroep.

Artikel 9 Wdo, toelaten identificatiemiddelen en diensten

De toelatingseisen worden opgenomen in lagere regelgeving. Het Besluit bedrijfs- en organisatiemiddel Wdo en het Besluit identificatiemiddelen voor natuurlijke personen zijn op 7 maart 2024 gepubliceerd. Met deze besluiten is uitvoering gegeven aan artikel 9 Wdo. Dat artikel regelt dat identificatiemiddelen voor burgers door de Minister van BZK kunnen worden toegelaten door middel van een erkenning of aangewezen als deze voldoen aan nader te stellen eisen. Zowel de eisen voor toetsing als de eisen waaraan een toegelaten middel moet voldoen zullen met het Conceptbesluit identificatiemiddelen worden vastgelegd. Dit besluit regelt daarmee ook de acceptatie van identificatiemiddelen in een nationale context. Dit wordt nader uitgewerkt in de Conceptregeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo (Conceptregeling identificatiemiddelen). De toelichting bij de Conceptregeling identificatiemiddelen stelt: *"In twee algemene maatregelen van bestuur zijn de kernbepalingen opgenomen ten aanzien van bescherming van gegevens, betrouwbaarheid van authenticaties en de besluitvormingsprocedure. Voor het overige bevatten deze algemene maatregelen van bestuur een basis om nadere eisen en regels te stellen bij ministeriële regeling. De onderhavige ministeriële regeling is daarop gebaseerd en bevat de aanvullende, meer gedetailleerde eisen waaraan wordt getoetst, aanvullende regels over de aanvraagprocedure voor een erkenning en nadere verplichtingen voor houders van een erkenning of aanwijzing."* Aan deze middelen worden eisen gesteld om de veiligheid en privacy te borgen. Daarop wordt gecontroleerd voordat middelen worden toegelaten en vervolgens wordt er toezicht op gehouden. De Conceptregeling identificatiemiddelen vult deze eisen meer specifiek in, zoals de eisen rond open source software, het verhandelverbod en *privacy by design*.

In dit kader is het volgende nog relevant. In artikel 2.13 van de Conceptregeling identificatiemiddelen is een verbod opgenomen voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens: *"Het authenticatiemechanisme van een identificatiemiddel op betrouwbaarheidsniveau substantieel en hoog maakt geen gebruik van een inherente authenticatiefactor, als bedoeld in de bijlage bij Uitvoeringsverordening (EU) 2015/1502."*

Hierover is in de toelichting – voor zover relevant – het volgende opgenomen: *"Het gebruik van biometrische kenmerken voor authenticatie is in de afgelopen jaren sterk toegenomen. In deze regeling is bepaald dat een erkenning niet wordt verleend voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens. De beschikbare techniek en de vele varianten die daarvoor in omloop zijn hebben nog niet een niveau bereikt dat voldoende is voor verantwoorde toepassing bij toegang tot elektronische overheidsdiensten. Wanneer de kwaliteit van deze techniek verbetert of wanneer internationale ontwikkelingen daartoe aanleiding geven kan deze regeling worden gewijzigd om authenticatie met gebruik van biometrische gegevens alsnog mogelijk te maken. Deze regeling staat in beginsel niet in de weg aan verificatie van de identiteit (dus vaststelling van de identiteit ten tijde van uitgifte van een identificatiemiddel) met gebruik van biometrie. Voor die toepassing zal in een aanvang moeten worden onderbouwd dat de gebruikte techniek voldoende betrouwbaar is om op het gewenste betrouwbaarheidsniveau te worden gebruikt."*

Ook voor het Conceptbesluit identificatiemiddelen en de bijbehorende Conceptregeling identificatiemiddelen geldt dat deze pas in werking kunnen treden als het Stelsel Toegang gereed is.

Voorstel Besluit digitale overheid, artikel 4 en 16 Wdo

Op moment van publiceren van deze Handreiking Betrouwbaarheidsniveaus is een wetsvoorstel Besluit digitale overheid (Bdo) in procedure. Het Bdo zal de onderwerpen persoonsgegevensverwerking en informatieveiligheid in het kader van de toegang tot elektronische overheidsdienstverlening reguleren. In het bijzonder zal het Bdo ter uitvoering van de artikelen 4 en 16 van de Wdo dienen.

Voorstel Besluit directe bevraging gezagsmodule

Met het conceptbesluit directe bevraging gezagsmodule zal mogelijk worden gemaakt dat overheidsinstanties kunnen opvragen welke personen gezag hebben over een minderjarige. Dit besluit wijzigt het Bdo in verband met regels over directe bevraging van de gezagsmodule.

2.3 Overzicht artikelen en leden van de Wdo die nog niet in werking zijn getreden (per juli 2024)

Artikel	Omschrijving	Opmerking
1.	Definities	
2.	Reikwijdte	
3.	Standaarden	
4.	Informatieveiligheid	Nog niet in werking getreden.
5.	Verantwoordelijkheid voor het beheer	Lid 1, onder g is nog niet in werking getreden. Ook lid 6 is nog niet in werking getreden.
6.	Betrouwbaarheidsniveaus	
7.	Acceptatie	Nog niet in werking getreden.
8.	Gebruik in publieke domein	
9.	Toelaten van identificatiemiddelen en diensten	Nog niet in werking getreden.
10.	Regels ten aanzien van gebruik	
11.	Erkenning bedrijfs- en organisatiemiddel en bijbehorende diensten	Nog niet in werking getreden.
12.	Aanwijzing van attributen	Nog niet in werking getreden.
13.	Rechten en plichten voor erkende diensten	Nog niet in werking getreden.
14.	Intrekking en overdracht van erkenning	Nog niet in werking getreden.
15.	Acceptatie bedrijfs- en organisatiemiddelen	Nog niet in werking getreden.
16.	Bescherming persoonsgegevens	Leden 2 en 3 zijn nog niet in werking getreden.
17.	Toezicht en handhaving	Leden 3, 5 en 7 zijn nog niet in werking getreden.
18.	Bijzondere bevoegdheden	
19.	Informatieverstrekking	

Artikel	Omschrijving	Opmerking
20.	Leges voor verstrekking publiek identificatiemiddel	
21.	Doorberekening kosten	Nog niet in werking getreden.
22.	Doorberekening aanvraag erkenning en toezicht op naleving erkenningseisen	Nog niet in werking getreden.
23.	Evaluatie	
24.	Overgangsrecht bedrijfs- en organisatiemiddel	Nog niet in werking getreden.
25.	Parlementair betrokkenheid bij gedelegeerde regelgeving	
26.	Innovatie	
27.	Wijziging Wegenverkeerswet 1994	Nog niet in werking getreden.
28.	Omhangen	
29.	Inwerkingtreding	
30.	Citeertitel	

3. *eIDAS-Verordening*

De eIDAS-verordening is per 1 juli 2016 van kracht geworden. Deze verordening gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. De eIDAS-verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de EU.

De eIDAS-verordening kent drie betrouwbaarheidsniveaus: laag, substantieel en hoog (artikel 6 eIDAS-verordening). Deze zijn nader uitgewerkt in een uitvoeringsverordening. Dit betreft de uitvoeringsverordening van de Commissie van 8 september tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid. De betrouwbaarheidsniveaus, zoals in de eIDAS- verordening opgenomen, worden ook in de AVG en de Wdo toegepast.

Een elektronische identificatie die in een EU-land wordt toegelaten, moet in alle andere EU-landen worden erkend. Dit vergt dat de elektronische identificatie aan de eisen van de eIDAS-verordening voldoet, is aangemeld bij de Commissie en is opgenomen in een lijst (zie ook 'EUR-Lex, 'Veiligere transacties via internet, Samenvatting van: Verordening (EU) nr. 910/2014: betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt').

Een stelsel voor elektronische identificatie moet een van de drie betrouwbaarheidsniveaus vermelden (laag, substantieel en hoog) op grond van dat stelsel uitgegeven vormen van elektronische identificatie. Wederzijdse erkenning is alleen verplicht wanneer de relevante overheidsinstantie de betrouwbaarheidsniveaus substantieel of hoog gebruikt om toegang te krijgen tot de online diensten (artikel 8 eIDAS-verordening; zie ook EUR-Lex, 'Veiligere transacties via internet, Samenvatting van: Verordening (EU) nr. 910/2014: betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt'). Nederlandse overheidsorganisaties en private organisaties met een publieke taak moeten sinds 29 september 2018 Europees erkende inlogmiddelen accepteren in hun digitale dienstverlening. Concreet betekent dit dat burgers die de beschikking hebben over een erkend inlogmiddel dezelfde zaken moeten kunnen regelen als alle andere burgers in een EU-lidstaat.

eIDAS 2.0

eIDAS 2.0 is er op gericht om de tekortkomingen van de eerdere eIDAS 1.0-verordening op te lossen. Op 28 mei 2021 publiceerde de Europese Commissie de evaluatie van de huidige eIDAS-verordening. Uit deze evaluatie bleek dat de huidige verordening op verschillende gebieden tekortschiet. Slechts iets meer dan de helft van de inwoners van de EU heeft toegang tot betrouwbare en veilige grensoverschrijdende eID-regelingen. Er blijken weinig publieke onlinediensten te zijn die naast in het eigen land toegankelijk te zijn, ook (via het eIDAS-netwerk) toegankelijk zijn vanuit andere lidstaten. De huidige eIDAS-verordening is er niet op gemaakt om op een toereikende manier in te spelen op nieuwe marktveranderingen. Er is een grote vraag naar nieuwe elektronische identificatiemiddelen, ook in het publieke domein. De eIDAS 2.0-verordening is hier op toegespitst.

De nieuwe verordening introduceert een Europese portemonnee waarmee burgers gebruik te maken van digitale diensten, welke voor verschillende doeleinden ingezet kan worden. De digitale identiteit is op vrijwillige basis en maakt het mogelijk voor individuen om controle te hebben over hun persoonsgegevens. De portemonnee kan gebruikt worden als een identificatiemiddel waarmee specifieke documenten aangeleverd

kunnen worden. De portemonnee kan bijvoorbeeld toegang geven tot een persoonlijke bankrekening of de aanvraag van een lening. Ook het indienen van een belastingaangifte kan straks geschieden met behulp van de portemonnee, evenals dat de inschrijving voor een onderwijsinstelling kan worden voltooid via de inzet van de portemonnee.

Op 20 mei 2024 is de verordening eIDAS 2.0 in werking getreden en daarmee ook de revisie van eIDAS 1.0. In 2026 moet eIDAS 2.0 in Nederland zijn ingevoerd en zijn uitgewerkt in nationale wetgeving. Het voornemen is om in diezelfde periode een nieuwe actualisatie van deze Handreiking Betrouwbaarheidsniveaus (versie 6) te publiceren die zal zijn gebaseerd op de praktische uitwerking van eIDAS 2.0 die dan beschikbaar zou moeten zijn. Met de inwerkingtreding van eIDAS 2.0. is de komst van de Europese Digitale Identiteit (EDI) een stap dichterbij. In 2026 zullen alle Europeanen een eigen EDI wallet moeten kunnen gebruiken. De EDI is van belang voor onderhavige Handreiking. Tegelijkertijd is hierover nog lang niet alles duidelijk. Er volgen nog tientallen '*implementing acts*'. Vandaar dat EDI wallets pas bij de actualisatie van de Handreiking in 2026 aan de orde zullen komen.

Impact van andere wetgeving (NIS2, BIO en Wmebv)

De goede werking van de eIDAS-verordening hangt samen met de implementatie van een aantal andere Europese digitale wetten. Zo is het voor de verordening noodzakelijk dat de regels rondom cyberveiligheid worden nageleefd. Hiervoor zal onder meer worden gekeken naar het wetsvoorstel voor de Cyberbeveiligingswet die in 2025 wordt verwacht als nationale invulling van de *Network and Information Security directive*, of NIS2-richtlijn. Deze richtlijn is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Het is de opvolger van de eerste NIS-richtlijn, ook wel bekend als de NIB die in Nederland in 2016 is opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni).

Voor overheidsorganisaties geldt specifiek dat zij momenteel al moeten voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). De BIO wordt onderdeel van de zorgplicht van NIS2 voor de overheid. Het voldoen aan de BIO en andere bestaande kaders voor informatiebeveiliging bij de overheid, is dus een belangrijk beginpunt.

Tot besluit zal naar verwachting 1 januari 2026 de Wet modernisering elektronisch bestuurlijk verkeer (Wmebv) in werking treden. Met de Wmebv wordt de Algemene wet bestuursrecht (Awb) gewijzigd. De wet elektronisch bestuurlijk verkeer regelt dat burgers en bedrijven het recht krijgen om elektronisch zaken te doen met de overheid.

Bijlage 2 Bronvermelding Verordeningen, wetten en documentatie m.b.t. wetgevingsproces (incl. conceptwetgeving)

- **AVG**, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&qid=1685451198313
- **Bdo**, te raadplegen via https://www.internetconsultatie.nl/digitaleoverheid/document/3439
- **Conceptbesluit identificatiemiddelen**, te raadplegen via https://www.internetconsultatie.nl/identificatiemiddelen/document/5663
- **Conceptregeling identificatiemiddelen** incl. toelichting, te raadplegen via https://open.overheid.nl/repository/ronl-677653689327557096 67befed8c491ddb5cba0f9/1/pdf/concept-regeling-eisen-identificatiemiddelen-wdo.pdf
- **eIDAS 2.0**, zie: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52021PC0281
- **eIDAS-verordening**, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&qid=1689941728375
- **Regeling betrouwbaarheidsniveaus**, te raadplegen via https://zoek.officielebekendmakingen.nl/stcrt-2023-13656.html
- **Uitvoeringsverordening** van de Commissie van 8 september tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, te raadplegen via https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32015R1502&from=EN
- **Wdo**, te raadplegen via https://wetten.overheid.nl/BWBR0048156

Bijlage 3 Afkortingen en begrippen

Definitie	Toelichting
AVG	Algemene Verordening Gegevensbescherming
Bdo	Besluit digitale overheid
BSN	Burgerservicenummer
BW	Burgerlijk Wetboek van Nederland
BZK	De minister en/of het ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Conceptbesluit identificatiemiddelen	Conceptbesluit identificatiemiddelen voor burgers Wdo
Conceptregeling identificatiemiddelen	Conceptregeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo
eID	Elektronische identificatiemiddelen of Elektronische identiteit
eIDAS 2.0	20 mei 2024 van kracht geworden Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit of de herziene eIDAS-verordening
eIDAS 1.0	Gereviseerde Verordening (EU) van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG
EU	Europese Unie
Regeling betrouwbaarheidsniveaus	Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening of Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 8 mei 2023, nr. 23-0000244782, houdende regels betreffende de bepaling van het vereiste betrouwbaarheidsniveau van authenticatie voor de verlening van elektronisch diensten en overgangsrecht met betrekking tot betrouwbaarheidsniveaus
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming

Definitie	Toelichting
Wallet	European Digital Identity Wallet op basis van eIDAS 2.0
Wbp	Wet bescherming persoonsgegevens. Deze wet is per 25 mei 2018 vervallen.
Wdo	Wet digitale overheid, voorheen Wet tot algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur
Wmebv	Wet modernisering elektronisch bestuurlijk verkeer

Bij hergebruik graag vermelden:
Forum Standaardisatie: handreiking betrouwbaarheidsniveaus voor digitale dienstverlening, november 2024

Deze handreiking is een uitgave van:

Forum Standaardisatie
November 2024

Forum Standaardisatie
Standaard Samenwerken