(Controleprotocol eID 2018) – versie 0.9.2

1. Inleiding

De minister van BZK is op grond van artikel X van de Wet elektronisch berichtenverkeer belastingdienst (de wet EBV) verantwoordelijk voor voorzieningen voor elektronische authenticatie. De minister heeft uit hoofde van deze verantwoordelijkheid de mogelijkheid om identificatiemiddelen en authenticatiediensten in het BSN-domein toe te laten voor toegang tot digitale dienstverlening van overheidsorganisaties. Randvoorwaardelijk voor de toelating van identificatiemiddelen op de niveaus substantieel en hoog is dat zij voldoen aan de op grond van de eIDAS uitvoeringsverordening 1502 aan deze niveaus gestelde normen. Dit Controleprotocol eID 2018 dient als leidraad voor de toetsing aan de eIDAS-eisen en de eisen zoals opgenomen in een nog af te ronden set van eisen.

1.1 Ruimte bij invulling van vereiste elementen voor eIDAS betrouwbaarheidsniveaus substantieel en hoog

Dit Controleprotocol bevat aanwijzingen hoe voor de Nederlandse situatie wordt gecontroleerd of identificatiemiddelen en authenticatiediensten (aanbieders) voldoen aan de desbetreffende normen voor de betrouwbaarheidsniveaus substantieel en hoog zoals opgenomen in de eIDAS uitvoeringsverordening 1502 en welke ruimte (tolerantie) daarbij geaccepteerd is.
Nadrukkelijk wordt opgemerkt dat de aanbieders ruimte wordt gelaten bij de wijze van naleving van de eIDAS-normen. Uitgangspunt is dat de auditor een "principle based" benadering hanteert bij de controle. Daar waar het de controle op de op te stellen Nederlandse set van eisen betreft, wordt deze ruimte niet geboden. Het betreft daar eisen, waaraan voldaan moet worden, bijvoorbeeld om redenen van interoperabiliteit met de randvoorwaardelijke voorzieningen binnen het stelsel.

1.2. Reikwijdte en wijze van toepassing van het Controleprotocol

Dit Controleprotocol eID betreft de Nederlandse leidraad voor de auditor die ten behoeve van toelating van identificatiemiddel door de minister toetst of overeenstemming bestaat met de normen uit de eIDAS-uitvoeringsverordening 1502 die betrekking hebben op de betrouwbaarheidsniveaus substantieel en hoog, alsmede overeenstemming met de nader te stellen Nederlandse eisen (set van eisen eID). Dit Controleprotocol eID haakt daarom met de indeling aan bij de indeling van de eIDAS-uitvoeringsverordening 1502.
De begrippen die in dit Controleprotocol worden gehanteerd waar het de Nederlandse invulling betreft betreffen de begrippen zoals deze worden gedefinieerd in de set van eisen eID.
Deze voorgenomen begrippen zijn voor nu en voor zover relevant als bijlage bij dit Controleprotocol gevoegd.

1.3. Status van het Controleprotocol

Dit controleprotocol wordt vastgesteld als beleidsregel op basis van de huidige regelgeving. Na totstandkoming van de Wet digitale overheid die volgens plan per 1 januari 2019 in werking zal treden, zal dit protocol van toepassing zijn ten behoeve van de erkenning en toelating ingevolge die wet.

1.4 Goedkeurende verklaring

Een goedkeurende verklaring ten aanzien van de normen uit de eIDAS-verordening kan leiden tot de vaststelling dat een identificatiemiddel of authenticatiedienst valt te kwalificeren op betrouwbaarheidsniveaus substantieel dan wel hoog en de conformiteit met de Nederlandse (aanvullende) eisen kan leiden tot toelating tot gebruik in het BSN-domein (incl. de bijbehorende koppeling aan het BSNk en de routeringsdienst voor het BSN-domein).

1.5. Leeswijzer/Indeling van het Controleprotocol

1.5.1 Inhoudelijk

Aan de hand van de in de bijlage van de eIDAS uitvoeringsverordening 1502 beschreven elementen van de technische specificaties en procedures wordt bepaald op welke wijze de vereisten en criteria van artikel 8 van Verordening (EU) nr. 910/2014 worden toegepast op elektronische identificatiemiddelen die zijn uitgegeven op grond van een stelsel voor elektronische identificatie. Dit protocol haakt daarbij aan.
Achtereenvolgens wordt in dit controleprotocol aangegeven waarop wordt gecontroleerd of wordt voldaan aan de beoogde eIDAS waarborgen voor de betrouwbaarheidsniveaus substantieel en hoog ten aanzien de eIDAS elementen. Het betreft in de eerste plaats de inschrijving van een identificatiemiddel (waaronder de aanvraag, de registratie en het bewijs en verificatie van identiteit). Vervolgens komt het beheer van elektronische identificatiemiddelen aan de orde,

waaronder het ontwerp en de lifecycle (uitgifte, beheer, verlenging en beëindiging) van identificatiemiddelen. Hierna volgen de waarborgen voor authenticatie(mechanisme). Voort komen de elementen die zien op het beheer van organisatie aan bod, waaronder algemene eisen aan organisaties, de informatievoorziening aan gebruikers van identificatiemiddelen, informatiebeveiliging, administratie, faciliteiten en personeel en technische controles. Na toelichting op de invulling van controle op de naleving (compliance en audit), wordt beschreven hoe de controle op de op te stellen set van eisen eID dient plaats te vinden.

1.5.2. Vorm

In dit Controleprotocol worden de genoemde elementen langsgelopen. Daarbij is per element gekozen voor de volgende opbouw.
Eerst wordt steeds het element uit de bijlage van de eIDAS-uitvoeringsverordening 1502 integraal opgenomen in de tekst.
Vervolgens wordt – indien beschikbaar - de duiding (guidance) opgenomen die de stellers van de eIDAS uitvoeringsverordening 1502 bij het betreffende element hebben aangegeven. Deze is afkomstig c.q. vertaald uit het document "*Guidance for the application of the levels of assurance which support the eIDAS Regulation*". Hoewel dit document in EU-verband geen formele status kent – het is nooit formeel vastgesteld – kan het dienstig zijn bij de vaststelling c.q. invulling van de betreffende elementen.
Ten slotte wordt per element aangegeven waarop gecontroleerd dient te worden om het element in te vullen naar de Nederlandse situatie.

2.1. *Inschrijving*

Voor de inschrijving van een identificatiemiddel wordt aangegeven welke controles dienen plaats te vinden voor de registratie en welke gegevens moeten worden geregistreerd, waaronder gegevens om met gebruikers in contact te kunnen treden in geval van misbruik. Tevens wordt bepaald welk bewijs van identiteit dient te worden overlegd en welke controles moeten worden uitgevoerd teneinde een voldoende mate van zekerheid te krijgen dat de identiteit van de persoon overeenkomt met de opgegeven gegevens.

2.1.1. Aanvraag en registratie

Vereisten elementen

Voor de aanvraag en registratie van identificatiemiddelen vereist de eIDAS-uitvoeringsverordening 1502 dat aan de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 2. De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoorzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden. 3. De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld.
Substantieel	Hetzelfde als niveau laag.
Hoog	Hetzelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.1.1 Aanvraag en Registratie

LAAG

1. De aanvrager moet bekend zijn met de voorwaarden die aan het gebruik van het elektronische identificatiemiddel zijn verbonden.

RICHTLIJN VOOR BEOORDELING:

Dit hangt af van een meerdere factoren, waaronder het de mate van betrouwbaarheid in het eID stelsel en het belang van de voorwaarden voor het functioneren en beveiliging van het stelsel..

Voorbeelden :

- *De informatie maakt onderdeel uit van nationale wetgeving en kan daarom worden verondersteld bij de aanvrager bekend te zijn.*
- *De aanvrager krijgt de vereiste informatie in schriftelijke vorm.*
- *De aanvrager accepteert de voorwaarden expliciet.*

***2. De aanvrager moet bekend zijn met de aanbevolen veiligheidsvoo*rzorgen die aan het gebruik van het elektronische identificatiemiddel zijn verbonden.** 3

RICHTLIJN VOOR BEOORDELING:

Zie ook hierboven onder 1.

Voorbeelden van veiligheidsvoorzorgsmaatregelen zijn:

- *Het kiezen van een veilig wachtwoord/PIN in overeenstemming met het beleid*
- *Het Veilig bewaren van op bezit gebaseerde elektronische identificatiemiddelen.*
- *Het niet aan anderen afgeven van het elektronische identificatiemiddel.*

Zie hiervoor ook paragraaf 2.4.6 ten aanzien van het continu monitoren van de meest actuele beveiligingsvoorzorgsmaatregelen het communiceren van de noodzakelijke voorzorgsmaatregelen aan de aanvragers.

3. De relevante identiteitsgegevens die voor het bewijs en de verificatie van de identiteit vereist zijn, moeten zijn verzameld.

RICHTLIJN VOOR BEOORDELING:

Ten minste die informatie moet worden gevraagd om de Minimale gegevensset voor eID beschikbaar te hebben. Informatie die bekend is of gegenereerd wordt binnen het stelsel moet verzameld worden, bijvoorbeeld bij de aanvragen of andere bronnen.

Zie hierover ook de volgende paragrafen met verwijziging naar artikel 7 (d) van de eIDAS-Verordering 1502, and refer to Article 7 (d) of the Regulation.

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van Aanvraag en registratie van natuurlijke personen wordt het volgende uitgangspunt gehanteerd:

1. Als invulling van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.1.1 Aanvraag en registratie (natuurlijk persoon) bij betrouwbaarheidsniveau Laag punt 1 geldt voor de niveaus Substantieel en Hoog dat voorafgaand aan de dienstverlening de voorwaarden voor het gebruik van het elektronische identificatiemiddel bekend worden gemaakt aan de gebruiker. De voorwaarden betreffen in elk geval:
   a. de geldigheidsduur van het identificatiemiddel, indien van toepassing;
   b. de kosten van het identificatiemiddel;
   c. procedures voor het uitgeven, schorsen, heractiveren, intrekken en vernieuwen van het identificatiemiddel.
2. Als invulling op de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.1.1 bij betrouwbaarheidsniveau Laag punt 2 geldt voor de niveaus Substantieel en Hoog dat de veiligheidsvoorschriften voor het gebruik van het elektronische identificatiemiddel bekend worden gemaakt aan de gebruiker. De veiligheidsvoorschriften betreffen in elk geval:
   a. de verplichting voor gebruikers om vermoedens van misbruik of inbreuken op de veiligheid van het identificatiemiddel te melden aan de aanbieder opdat identificatiemiddelen tijdig geschorst of ingetrokken kunnen worden;
   b. de verplichting voor gebruikers om hun identificatiemiddel niet door anderen te laten gebruiken en daarmee het geheimhouden van wachtwoorden, activeringscodes, pincodes en dergelijke.
   c. rechten en plichten van gebruikers in het geval dat het middel vanwege rechtswege wordt opgeschort, dan wel ingetrokken.
3. Er moeten zodanige contactgegevens van de gebruiker beschikbaar zijn, dat met de gebruiker in contact kan worden getreden via een ander kanaal dan het identificatiemiddel van de gebruiker.

2.1.2. Bewijs en verificatie van identiteit (natuurlijke persoon)

Vereisten elementen

Voor bewijs en verificatie van identiteit (natuurlijke persoon) vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt. 2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn. 3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 4 vermelde alternatieven.

	1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt; en het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is. of 2. Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 3. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad (1) of een daaraan gelijkwaardige instantie. of 4. Indien elektronische identificatiemiddelen worden

	uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.
Hoog	Er moet zijn voldaan aan de vereisten van punt 1 of punt 2. 1. Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven. a) Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron; 6 en de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron. of b) Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie; en er zijn maatregelen getroffen om aan te tonen dat de resultaten van de eerdere procedures nog steeds geldig zijn.

	of c) Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. en er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn. OF 2. Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

Richtlijnen voor de toepassing van betrouwbaarheidsniveaus die de eIDAS-verordening ondersteunen

2.1.2 Bewijs en verificatie van identiteit (natuurlijke persoon)

LAAG

De persoon kan in redelijkheid worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt.

.

RICHTLIJN VOOR BEOORDELING:

Er kan *in redelijkheid* worden verondersteld dat de betrokkene in het bezit is van bewijs, indien er geen aanwijzingen zijn dat dit niet het geval is en uit de ervaring is gebleken dat het bewijs dat deze veronderstelling staaft in de praktijk voldoende is.

Voorbeelden:

- *Bezit kan worden gewaarborgd door het bewijs in fysieke of elektronische vorm te overleggen.*

- *Bezit kan worden gewaarborgd door niet-openbare informatie te geven die is vervat in documenten die aan een bekend adres aan de betrokkene zijn verzonden*

2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn

RICHTLIJN VOOR BEOORDELING:

De term "echt" verwijst naar de authenticiteit van het bewijs op het moment van uitgifte. Het kan worden verondersteld nog altijd echt te zijn als het niet vervalst of gemanipuleerd is en door de bevoegde instantie is uitgegeven.

De term "geldigheid" verwijst naar de juistheid van het bewijs op het moment van overlegging. Dit kan onder andere de juistheid omvatten van de in het bewijs vervatte informatie en de intrekkings-/schorsingsstatus ervan.

Tenzij dit in de nationale wetgeving of de bestuurlijke praktijk is vastgelegd, is het gangbaar de echtheid van fysieke bewijzen door middel van fysieke inspectie vast te stellen. Voor elektronisch bewijs is het verifiëren van de digitale handtekeningen van de instantie die het bewijs uitgeeft een beste praktijk.

Op het betrouwbaarheidsniveau Laag zijn uitvoerige controles niet nodig om te waarborgen of bewijs echt en geldig lijkt

3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is

RICHTLIJN VOOR BEOORDELING:

In veel lidstaten is een bevolkingsregister een gezaghebbende bron voor het bestaan van de persoon. Ook officieel bewijs zoals uittreksels uit registers, identiteitsdocumenten of ander langs officiële weg verstrekt bewijs fungeert als gezaghebbende bron van het bestaan van de persoon.

Bestaan betekent onder andere dat de persoon die door de opgegeven identiteit wordt vertegenwoordigd niet is overleden.

Om te controleren of de aanvrager de persoon is zoals wordt verklaard door de gezaghebbende bron, kan er een fysieke vergelijking zoals een foto-identificatie worden toegepast, of kan het bewijs worden gekoppeld aan een elektronische authenticatie waarbij attributen die verband houden met de authenticatie overeenkomen met de attributen waarover de gezaghebbende bron beschikt (identificatiecodes, naam, geboortegegevens etc.)

SUBSTANTIEEL

Niveau laag plus een van de onder de punten 1 tot en met 4 vermelde alternatieven:

1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt

RICHTLIJN VOOR BEOORDELING:

Het is gangbaar het bezit van fysiek bewijs door overlegging van het bewijs tijdens, of voorafgaand aan, het aanvragen te verifiëren, en hier op het moment van aanvragen op betrouwbare wijze naar te verwijzen. Afhankelijk van het soort bewijs kan fysieke overlegging op het verificatiepunt vereist zijn of kan overlegging op afstand mogelijk zijn.

Verificatie van niet-fysiek bewijs kan bijvoorbeeld bestaan uit het verifiëren van toegang tot een bankrekening of iets vergelijkbaars, door de aanvrager te vragen een transactie uit te voeren die daadwerkelijk toegang tot de bankrekening vereist

en

het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon

RICHTLIJN VOOR BEOORDELING:

NB: de controles van betrouwbaarheidsniveau Laag zijn ook van toepassing, hetgeen impliceert dat het bewijs geldig moet lijken.

Het is gangbaar fysiek bewijs op echtheid te controleren door middel van een fysieke inspectie van de veiligheidskenmerken van het bewijs. Voorbeelden van veiligheidskenmerken zijn watermerken, inktsoorten, hologrammen, microprint etc.

Elektronisch bewijs kan bijvoorbeeld worden geverifieerd door middel van digitale handtekeningen of door online verificatie van het bewijs aan de hand van een gezaghebbende bron. Voorbeelden van dergelijk elektronisch bewijs zijn uittreksels uit bevolkingsregisters of uittreksels uit overheidsregisters waarvoor identiteitsinformatie is geverifieerd tijdens de inschrijving

en

er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is;

RICHTLIJN VOOR BEOORDELING:

De praktijken van de lidstaat kunnen afhankelijk van de nationale infrastructuur verschillen. Het is mogelijk dat sommige lidstaten op slechts één instantie en de beveiligingsmaatregelen daarvan vertrouwen, zoals één instantie voor identiteitsdocumenten die de identiteit verifieert. Andere lidstaten kunnen verder gaan door het bewijs van iemands identiteit aan te vullen met beveiligingsmaatregelen op meer niveaus waarbij de gegevens van verschillende instanties met elkaar worden vergeleken (bijv. wanneer een belastingapplicatie die een verklaring indient over de betrokkene de gegevens van de betrokkene met de eigen belastinggegevens vergelijkt, hetgeen vervolgens weer wordt vergeleken met het bevolkingsregister dat activeringscodes naar het officiële woonadres van de betrokkene stuurt etc.).

Het risico van verloren, gestolen, ingetrokken, verlopen of geschorste documenten is afhankelijk van de robuustheid van en het aantal betrokken onafhankelijke bronnen, maar ook van hoe

waarschijnlijk het is dat er snel melding wordt gemaakt van verlies of diefstal van een legitimatiebewijs. Factoren die van invloed zijn op hoe waarschijnlijk dit is, zijn onder andere de gebruiksfrequentie, waarde voor de houder etc. De bewijswaarde van verlopen documenten zou ook afhankelijk van de omstandigheden kunnen verschillen, bijv. welke kenmerken van een verlopen document wel nog bewijswaarde hebben (bijv. sommige lidstaten zouden kunnen toestaan dat een rijbewijs als bewijs gebruikt wordt, zelfs indien het rijbewijs van de houder om een auto/specifiek soort voertuig te besturen verlopen is)

Voorbeelden van mogelijke stappen om de risico's te minimaliseren zijn:

- *de geldigheid aan de hand van registers controleren.*
- *intrekkingscontroles voor bewijsmateriaal op basis van PKI/smartcard.*
- *vergelijking van fysieke kenmerken van de aanvrager met het bewijsmateriaal.*
- *gevestigde sectorpraktijken toepassen, zoals "ken-de-cliënt" in de financiële sector (zie ook de anti-witwasrichtlijn).*
- *maatregelen om bedrieglijk gebruik van dergelijke documenten, te ontmoedigen bijv. actuele biometrische informatie (foto, vingerafdruk etc.) van de aanvrager vastleggen*

of

Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd

10

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven.

en

er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn;

RICHTLIJN VOOR BEOORDELING:

Zie voor richtlijnen hierover de bovenstaande punten

of

3. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad (1) of een daaraan gelijkwaardige instantie

RICHTLIJN VOOR BEOORDELING:

Voorbeelden van een dergelijke eerder gebruikte procedure kunnen zijn inschrijving bij een instantie die unieke identificatie vraagt (bijv. de belastingdienst), of het openen van een bankrekening waarvoor identificatie- en ken-de-cliënt-eisen gelden krachtens wetgeving op het bankwezen.

Deze mogelijkheid weerspiegelt de procedures waarnaar wordt verwezen in art. 24, lid 1, onder d), van de eIDAS-verordening en waardoor ook duidelijk rekening wordt gehouden met de eis in overweging 16 van de verordening met betrekking tot "… consequente toepassing van deze verordening, met name wat betreft betrouwbaarheidsniveau hoog voor het bewijzen van de identiteit voor het afgeven van gekwalificeerde certificaten."

Bevestiging van de gelijkwaardigheid en betrouwbaarheid betekent dat aan de uitkomsten van het betrouwbaarheidsniveau wordt voldaan door de eerder gebruikte procedures met betrekking tot de eisen voor elk niveau.

Voorbeelden van instanties die gelijkwaardig zijn aan conformiteitsbeoordelingsinstanties volgens 765/2008 zijn nationale toezichthoudende organen.

of

4. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.

RICHTLIJN VOOR BEOORDELING:

Aan de vereisten voor het bewijs en de verificatie van de identiteit kan worden voldaan met behulp van een al uitgegeven elektronisch identificatiemiddel. NB: het bewijs en de verificatie van de identiteit is slechts een onderdeel van het inschrijvings- en uitgifteproces. Vereisten die verder gaan dan het bewijs en de verificatie van de identiteit moeten afzonderlijk in overweging worden genomen.

Verlenging en vervanging worden in hoofdstuk 2.2.4 behandeld. Voor de niveaus laag en substantieel is verlenging en vervanging mogelijk met dezelfde procedure die in dit punt wordt beschreven

HOOG

Er moet zijn voldaan aan de vereisten van punt 1 of punt 2:

1. Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven:

a. Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron;

RICHTLIJN VOOR BEOORDELING:

Zie de richtlijnen over de definitie van gezaghebbende bron

en

de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron;

RICHTLIJN VOOR BEOORDELING:

De vergelijking van de fysieke kenmerken moet met voldoende betrouwbaarheid worden uitgevoerd om duidelijke verificatie van de identiteit van de persoon te waarborgen.

Of procedures voldoen, kan bijv. blijken uit een laag aantal foutresultaten bij vergelijkingen. Factoren hiervoor kunnen onder andere een voldoende hoge kwaliteit van de vergelijkingsgegevens zijn.

- Indien personeelsleden betrokken zijn bij de vergelijking, is het belangrijk dat rekening wordt gehouden met de eisen uit hoofdstuk 2.4.5 dat de personeelsleden over voldoende vaardigheden moeten beschikken om de vergelijking uit te voeren.

- Naar analogie daarmee moet bij gebruikmaking van geautomatiseerde vergelijking rekening worden gehouden met beschikbare beste praktijken

of

b. Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie

en

er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere procedure nog steeds geldig zijn;

RICHTLIJN VOOR BEOORDELING:

In het algemeen is het mogelijk dat identificatiegegevens die in het verleden geverifieerd zijn niet meer actueel zijn, bijv. een verandering van naam, verandering van adres etc. Het doel van deze eis is waarborgen dat de identificatiegegevens op geldigheid gecontroleerd en, zo nodig, bijgewerkt worden. Zie ook artikel 7, lid d, van de verordening.

In het geval van de voorbeelden "belastingdienst" en "banken" bij punt 3 van het niveau Substantieel, kunnen dergelijke maatregelen die worden getroffen om aan te tonen dat de resultaten van de eerdere verificatie van de identiteit nog steeds geldig zijn, bestaan uit het bij andere bronnen, zoals een bevolkingsregister, controleren van attributen van eerdere verificatie van de identiteit die kunnen veranderen (bijv. naam, adres)

c. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie

en

er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn.

RICHTLIJN VOOR BEOORDELING:

Zie punt 4 van het niveau Substantieel

OF

Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken.

RICHTLIJN VOOR BEOORDELING: 13

Dit punt geeft aan dat nationale procedures voor de verkrijging van erkende bewijsstukken met foto of biometrische kenmerken geldige procedures zijn als gevolg van het verkrijgen van dergelijke bewijsstukken.

Voorbeelden van erkende bewijsstukken met foto of biometrische kenmerken zijn paspoorten en identiteitskaarten

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van bewijs en verificatie identiteit natuurlijke persoon wordt het volgende uitgangspunt gehanteerd:
Nadere duiding voor de Nederlandse situatie
Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.1.2 Bewijs en verificatie identiteit (natuurlijk persoon) bij betrouwbaarheidsniveau Substantieel punt 1 en 2 geldt voor de niveaus Substantieel en Hoog dat de identiteit van de persoon die het identificatiemiddel aanvraagt wordt geverifieerd aan zijn WID of aan een inlog met een identificatiemiddel dat door de Minister is toegelaten. Daarbij moet in ieder geval het volgende worden vastgesteld:

a. het bezit van het WID door de persoon die de aanvraag doet;
b. de echtheid en zo mogelijk de geldigheid van het WID;
c. de persoon die het middel aanvraagt en de identiteit die het WID vertegenwoordigt komen overeen.

2.1.3. Bewijs en verificatie van identiteit (rechtspersoon)

Deze paragraaf is voor het BSN-domein buiten scope

2.1.4. Koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen

Deze paragraaf is voor het BSN-domein buiten scope

2.2. *Beheer van elektronische identificatiemiddelen*

De eIDAS verordening 1502 stelt regels omtrent de uitgifte, het beëindigen van middelen op de niveaus substantieel en hoog. Het betreft regels die worden gesteld teneinde de identificatiemiddelen op veilige en betrouwbare wijze in bezit te stellen van de gebruiker.
Om de betrouwbaarheid gedurende de levensduur van het middel te garanderen zijn tevens regels gesteld aan de wijze waarop identificatiemiddelen moeten worden ontworpen, om te zorgen dat deze middelen dan wel de systemen waarvan gebruik wordt gemaakt niet tussentijds kunnen worden gecompromitteerd. Er zijn regels gesteld ten aanzien van het zogeheten aanvalspotentieel waartegen systemen bestand moeten zijn en de frequenties waarmee de controle op die bestendigheid moet worden herhaald.

Gedurende de levensduur van een middel en door het gebruik ervan kunnen er situaties optreden waarbij het nodig is om identificatiemiddelen te schorsen, in te trekken, te verlengen of te vervangen. Om de betrouwbaarheid te kunnen worden tevens regels gesteld waarop deze activiteiten moeten plaatsvinden, dat we procedures moeten worden gevolgd, controles nodig zijn en hoe het contact met de gebruiker moet plaatsvinden.

RICHTLIJN VOOR BEOORDELING:

In dit hele hoofdstuk geldt dat goede praktijken en de redelijke verwachtingen van een instantie die de verificatie uitvoert gepaard behoren te gaan met het bewustzijn dat het waarschijnlijk is dat betrokkenen vanuit een niet-vertrouwde omgeving actief zijn.

2.2.1. Kenmerken en ontwerp van elektronische identificatiemiddelen

<u>Vereisten elementen</u>

Ten aanzien van kenmerken en ontwerp van elektronische identificatiemiddelen vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het elektronische identificatiemiddel maakt gebruik van ten minste één authenticatiefactor. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle van de persoon aan wie het toebehoort.
Substantieel	1. Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.
Hoog	Niveau substantieel, plus: 1. Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en

	vervalsing en tegen aanvallers met een hoog aanvalspotentieel. 2. Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.2.1 Kenmerken en ontwerp van elektronische identificatiemiddelen

LAAG

1. Het elektronische identificatiemiddel maakt gebruik van ten minste één authenticatiefactor

RICHTLIJN VOOR BEOORDELING:
Authenticatiefactoren kunnen direct als onderdeel van een authenticatie worden gebruikt (bijv. het verzenden van een wachtwoord) of ze kunnen indirect worden gebruikt om een token te ontsluiten dat vervolgens in de authenticatie voorziet (bijv. het bewijs van een sleutel)

2. Het elektronische identificatiemiddel is zodanig ontworpen dat de uitgever ervan redelijke stappen onderneemt om te verifiëren dat het slechts wordt gebruikt door of onder controle van de persoon aan wie het toebehoort.

RICHTLIJN VOOR BEOORDELING:

NB: waar er verwijzingen zijn naar het treffen van maatregelen met betrekking tot of het elektronische identificatiemiddel onder controle is van de betrokkene, kan dit alleen betrekking hebben op stappen waarvan men in redelijkheid kan verwachten dat de uitgever die onderneemt. Hoe dit wordt gedaan, houdt verband met de eisen van [2.2.2]

SUBSTANTIEEL

Het elektronische identificatiemiddel maakt gebruik van ten minste twee authenticatiefactoren die tot verschillende categorieën behoren.

RICHTLIJN VOOR BEOORDELING:

Het gebruik van meer authenticatiefactoren die tot verschillende categorieën behoren en elkaar aanvullen, kan de algehele beveiliging van het identificatiemiddel verhogen. Een gangbaar voorbeeld is het combineren van een op bezit gebaseerd token met een wachtwoord of pincode om het token te kunnen ontsluiten. Zelf als het token verloren raakt of gestolen wordt, kan het zonder de pincode niet voor authenticatie worden gebruikt.

Let op: dit betreft altijd één elektronisch identificatiemiddel – om alle twijfel te voorkomen behoort het duidelijk te zijn dat de verschillende factoren hetzelfde elektronische identificatiemiddel zullen betreffen. In het kader van de authenticatie worden er meerdere factoren gezamenlijk gebruikt

2. Het elektronische identificatiemiddel is zodanig ontworpen dat het kan worden verondersteld slechts te worden gebruikt door of onder controle van de persoon aan wie het toebehoort.

RICHTLIJN VOOR BEOORDELING:

Het elektronische identificatiemiddel aan de betrokkene koppelen is een eerste vereiste om het voor authenticatie te gebruiken. Een token zonder persoonlijke gebruikerspincode of wachtwoord zal bijvoorbeeld niet volstaan, aangezien iedereen een verloren of gestolen token kan gebruiken. Daarom behoort uit ten minste één van de factoren kennis of een inherent kenmerk van de betrokkene te blijken.

HOOG

Niveau substantieel, plus:

Het elektronische identificatiemiddel biedt bescherming tegen kopiëring en vervalsing en tegen aanvallers met een hoog aanvalspotentieel.

RICHTLIJN VOOR BEOORDELING:
Bescherming tegen kopiëring en vervalsing verwijst naar het totale elektronische identificatiemiddel en niet naar elke individuele authenticatiefactor. Het gebruik van verschillende authenticatiefactoren is bedoeld om risico te beperken, aangezien verschillende categorieën authenticatiefactoren voor verschillende bedreigingen vatbaar zijn. Personen of systemen (keyloggers) zouden wachtwoorden kunnen waarnemen tijdens het gebruik ervan of als ze opgeschreven zijn, op bezit gebaseerde authenticatiefactoren zouden gestolen kunnen worden of verloren kunnen raken, op inherente authenticatiefactoren gebaseerde systemen zouden kwetsbaar kunnen zijn voor gefingeerd bewijs (look-alikes/wijzigingen van echte biometrische gegevens, kunstmatig bewijsmateriaal, latex-vingerafdrukken etc.).

Factorspecifieke voorbeelden van bescherming tegen kopiëring en vervalsing zijn onder andere:

- *Op bezit gebaseerde authenticatiefactoren: bedden materiaal voor cryptografische sleutels in in hardware die bestendig is tegen ongeoorloofde manipulatie waardoor wordt voorkomen dat de sleutel aan het apparaat wordt onttrokken of in het apparaat wordt gemanipuleerd via fysieke of elektronische middelen, hardwarebeveiligingsmodule*

- *Inherente authenticatiefactoren: controle op 'in leven zijn', vertrouwde omgeving, weinig foutresultaten bij vergelijkingen*

Volgens goede praktijken behoort bewezen te zijn dat een elektronisch identificatiemiddel bestendig is tegen kopiëring en vervalsing. Dit kan onder worden gedaan door testen; bijvoorbeeld doordat het middel gecertificeerd is op basis van relevante technische normen (bijv. gemeenschappelijke criteria).
Zie hoofdstuk 2.3.1 voor richtlijnen over "een hoog aanvalspotentieel"

2. Het elektronische identificatiemiddel is zodanig ontworpen dat het door de persoon aan wie het toebehoort op betrouwbare wijze kan worden beschermd tegen gebruik door anderen.

RICHTLIJN VOOR BEOORDELING:

'op betrouwbare wijze kan worden beschermd' verwijst naar de inspanningen die worden verricht om te voorkomen dat het elektronische identificatiemiddel zonder het medeweten en de actieve toestemming van de betrokkene wordt gebruikt. Het behoort bijvoorbeeld niet mogelijk te zijn dat een persoonlijke sleutel in een token voor een cryptografische sleutel zonder de actieve

toestemming van de gebruiker (bijv. door middel van een pincode) door een machinaal proces wordt gebruikt.

Deze eis biedt bescherming tegen: kopiëren, gissen, herafspelen en manipuleren van communicatiebedreigingen.

Andere technieken die in aanvulling op de eerder genoemde technieken gebruikt zouden kunnen worden, zijn:

- De sterkte van statische wachtwoorden
- Biometrische verificatie van de gebruiker
- Controles van de omgeving op kwaadwillende code
- 'Out of band'-verificatie

Voor alle op geheimhouding gebaseerde authenticatiefactoren (statische wachtwoorden, eenmalig wachtwoord in hardware) is gissen een bedreiging die beperkt moet worden teneinde een zeer hoog weerbaarheidsniveau te bereiken – bijv. door het aantal pogingen/vertragingsmechanismen te beperken en voldoende entropie te waarborgen

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van kenmerken en ontwerp van elektronische identificatiemiddelen wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.1. Kenmerken en Ontwerp van elektronische identificatiemiddelen bij betrouwbaarheidsniveau Substantieel punt 1 en 2 geldt voor de niveaus Substantieel en Hoog dat wordt gewaarborgd dat een identificatiemiddel gedurende de levensduur van het middel en gedurende de voorgeschreven bewaartermijnen van gebruikersgegevens en gebruiksgegevens is gekoppeld aan maximaal één natuurlijk persoon.

Een identificatiemiddel bestaat uit een samenstel van tenminste 2 verschillende authenticatiefactoren en attributen en heeft zodanige unieke kenmerken dat het geheel bij gebruik van het identificatiemiddel de authenticiteit van de identiteit van een natuurlijke persoon waarborgt. Er moet gewaarborgd worden dat deze authenticiteit gedurende de levensduur van het identificatiemiddel en gedurende de voorgeschreven bewaartermijnen van gebruikersgegevens en gebruiksgegevens behouden blijft.

2. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.1. Kenmerken en Ontwerp van elektronische identificatiemiddelen bij betrouwbaarheidsniveau Hoog punten 1 en 2 geldt voor het betrouwbaarheidsniveau Hoog dat moet worden gewaarborgd dat het correcte functioneren van het identificatiemiddel weerstand biedt tegen fysieke en logische manipulatie door een aanvaller met een 'hoog aanvalspotentieel'. Dit betekent dat:

a. de weerstand tegen een 'hoog aanvalspotentieel' wordt beoordeeld door een ter zake deskundige en onafhankelijke instantie.

b. deze weerstand periodiek wordt herbevestigd. Herbevestiging door een ter zake deskundige en onafhankelijke instantie vindt in ieder geval plaats:

1°. bij substantiële wijzigingen aan het identificatiemiddel en;

2°. bij wijzigingen van de werking van het identificatiemiddel, of;

3°. na het verstrijken van drie jaren na de laatste beoordeling van de weerstand.

De term 'aanvalspotentieel' verwijst naar de Common Criteria (ISO/IEC 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B). De validatie van de weerstand tegen een hoog aanvalspotentieel (high attacker potential) kan worden uitbesteed aan een andere organisatie dan die toetst aan de eisen. In dat geval bepaalt de auditor of het bewijs van de validatie kan worden geaccepteerd en onderdeel kan worden van het conformiteitsrapport.

2.2.2. Uitgifte, uitreiking en activering

Vereisten elementen

Ten aanzien van de uitgifte, uitreiking en activering van identificatiemiddelen vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee het kan worden verondersteld alleen de beoogde persoon te bereiken.
Substantieel	Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.
Hoog	Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische identificatiemiddel toebehoort ervan in het bezit wordt gesteld.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.2.2 Uitgifte, uitreiking en activering

18

LAAG

Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee het kan worden verondersteld alleen de beoogde persoon te bereiken.

RICHTLIJN VOOR BEOORDELING:

In het geval van één enkele factor (d.w.z. wachtwoord) die online wordt uitgegeven, zou de activatiecode via de gewone post aan het geverifieerde adres van de betrokkene kunnen worden uitgereikt of naar de mobiele telefoon van de aanvrager kunnen worden verzonden (bijv. via SMS), nadat geverifieerd is dat het telefoonnummer inderdaad van de betrokkene is (bijv. via terugbellen).

In het geval van meerdere factoren moet ten minste één factor worden uitgereikt via een hierboven beschreven methode en is, afhankelijk van het stelsel, het gebruik van activatiecodes wellicht niet vereist.

SUBSTANTIEEL

Na de uitgifte wordt het elektronische identificatiemiddel uitgereikt via een mechanisme waarmee kan worden verondersteld dat alleen de persoon aan wie het toebehoort in het bezit ervan wordt gesteld.

RICHTLIJN VOOR BEOORDELING:

Mogelijke mechanismen zijn onder andere

- persoonlijke uitreiking
- uitreiking per aangetekende post

het gebruik van een activeringsproces waarbij in redelijkheid kan worden verondersteld dat alleen de betrokkene over de benodigde informatie beschikt om het middel te activeren (bijv. een transport-pincode die afzonderlijk van het identificatiemiddel wordt uitgereikt).

Voor Substantieel moeten meerdere authenticatiefactoren worden gebruikt. Activatiecodes zijn niet per se vereist. Er is een aantal combinaties van uitgifte, uitreiking en activering mogelijk die aan Substantieel voldoen:

- Het elektronische identificatiemiddel kan worden uitgereikt via de gewone post en worden geactiveerd door een code naar de bankrekening van de betrokkene te sturen. De aanvrager voert de code in om het elektronische identificatiemiddel te activeren. Hierbij wordt ervan uitgegaan dat bankauthenticatie ten minste van het niveau Substantieel is.
- Aparte uitreiking van het elektronische identificatiemiddel en de activatiecode via gewone post aan het geverifieerde adres van de betrokkene.
- Uitreiking van het elektronische identificatiemiddel via gewone post aan het adres van de aanvrager. Het elektronische identificatiemiddel wordt overgedragen nadat de identiteit van de aanvrager geverifieerd is

HOOG

Bij het activeringsproces wordt geverifieerd dat slechts de persoon aan wie het elektronische identificatiemiddel toebehoort ervan in het bezit wordt gesteld.

RICHTLIJN VOOR BEOORDELING:

Deze controle vereist dat er een activeringsproces wordt uitgevoerd, hetgeen wil zeggen dat veilige uitreiking op zich niet voldoende is. In het algemeen vereist een activeringsproces bepaalde gebruikersinteractie.

Het doel van een activeringsproces – naast het waarborgen dat de middelen aan de juiste betrokkene worden uitgereikt – is dat de betrokkene een expliciete stap onderneemt om eigenaar te worden van het middel. Pas daarna kan het middel voor authenticatie worden gebruikt.

Voor Hoog moet het activeringsproces waarborgen dat alleen de legitieme eigenaar het elektronische identificatiemiddel kan activeren en dat het activeringsproces beschermd wordt tegen onopzettelijk verlies en bedreigingen van binnenuit zoals collusie.

Het registreren en uitgeven van elektronische identificatiemiddelen mag nooit door slechts één persoon worden uitgevoerd.

Indien er activatiecodes worden gebruikt, moet de aanvrager deze binnen een gespecificeerde tijdsperiode gebruiken.

Bijvoorbeeld

- *De uitgifte van het elektronische identificatiemiddel bij de inschrijfbalie en de uitreiking van een activatiecode via gewone post aan het geverifieerde adres van de betrokkene.*
- *De uitreiking van een online aangevraagd elektronisch identificatiemiddel via gewone post en de uitgifte van een activatiecode aan een vertrouwde partij (bijv. een nabijgelegen postkantoor). De deelnemer moet de activatiecode persoonlijk afhalen en daarbij een identiteitsbewijs overleggen.*

Het elektronische identificatiemiddel wordt online aangevraagd en door een vertrouwde koerier overgedragen nadat de identiteit van de aanvrager geverifieerd is. Een activatiecode wordt apart via de gewone post naar het geverifieerde adres van de betrokkene verzonden.

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van Uitgifte, uitreiking en activering wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.2 Uitgifte, uitreiking en activering bij betrouwbaarheidsniveau Substantieel, geldt voor de niveaus Substantieel en Hoog dat:

a. de gebruiker in staat is gesteld om met kennis van het proces voor uitgifte, uitreiking en activering afwijkingen te ontdekken in de uitvoering van het proces. Daar wordt in ieder geval gewaarborgd dat:

1° de gebruiker over het verloop van de processen voor uitgifte, uitreiking en activering van het identificatiemiddel wordt geïnformeerd;

2°. de gebruiker via de door gebruiker zelf opgegeven en beheerde contactgegevens over het moment van verstrekking van één of meerdere authenticatiefactoren van het middel wordt geïnformeerd, en;

3°. gebruiker in staat wordt gesteld om tijdig en doeltreffend in contact te treden met de aanbieder indien de gebruiker een afwijking vermoedt in het proces van uitgifte, uitreiking en activering.

b. voor de uitgifte van authenticatiefactoren 'persoonlijke' contactgegevens van de gebruiker worden gebruikt;

c. maatregelen zijn getroffen die waarborgen dat bij de verstrekking van authenticatiefactoren door ongeautoriseerden, deze worden onderschept. Authenticatiefactoren die bij hetzelfde identificatiemiddel behoren worden afzonderlijk verstrekt:

1°. via gescheiden kanalen of;

2°. via hetzelfde kanaal maar dan gescheiden in tijd.

d. gewaarborgd wordt dat, indien van toepassing, de bruikbaarheid van activatiecodes beperkt is in tijd;

e. gewaarborgd wordt dat het gebruik van het identificatiemiddel door de gebruiker nodig is om zijn identificatiemiddel te activeren.

De kans dat alle authenticatiefactoren bij de uitgifte en activering in handen komen van een andere persoon dan de gebruiker moet op niveau substantieel zo klein mogelijk zijn. Als een derde inbreuk in het registratieproces pleegt moet het voor deze derde niet ook mogelijk zijn om bijvoorbeeld eventuele postberichten aan de gebruiker te onderscheppen. Daarom moet het gebruik van adressen waarvan verondersteld kan worden dat ook anderen dan de gebruiker daar toegang toe hebben zoveel mogelijk worden vermeden. Voorbeelden van dergelijke adressen zijn algemene bedrijfsadressen, postbussen, 'studentenhuizen'. Als het gebruik van algemene adressen niet kan worden vermeden moeten er compenserende maatregelen worden genomen zoals het persoonlijk verstrekken van activeringscodes aan de gebruiker tijdens het identificatieproces. Daarbij kan aangesloten worden op de huidige systematiek waarbij na gebleken risico in bepaalde postcodegebieden postberichten in persoon worden afgeleverd.

Voor de in het verleden reeds uitgegeven authenticatiemiddelen is ten aanzien van de controle op het proces van uitgifte een specifieke aanpak nodig, waarbij gebruik wordt gemaakt van kennis over de wijze van uitgifte in het verleden. Voor de in het verleden reeds uitgegeven authenticatiemiddelen is ten aanzien van de controle op het proces van uitgifte een specifieke aanpak nodig, om vast te stellen of deze aan de vigerende eisen voldoet. De aanbieder dient dit te onderbouwen. Hierbij wordt gebruik gemaakt van kennis over de wijze van uitgifte in het verleden en toezicht/controle dat daarop heeft plaatsgevonden. Daarbij zal - op basis van onder meer beschikbare documentatie over de eerder gehanteerde procedures en uitgevoerde controles bij de registratie en uitgifte van middelen, inclusief wijzigingen daarin – door een onafhankelijke auditor, moeten worden gecontroleerd of daarbij gelijkwaardige waarborgen zijn gehanteerd. De ambtenaren die in opdracht van de minister zijn belast met controle zullen vervolgens, mede op basis van het audit rapport en een eventuele aanvullende eigen controle, een definitief oordeel geven over de juistheid en volledigheid van het proces van uitgifte van in het verleden uitgegeven authenticatiemiddelen. Ter vaststelling van de zekerheid kan daarbij tevens – aanvullend - worden gesteund op het gebruik van het identificatiemiddel sinds de uitgifte ervan, bijvoorbeeld als door –

aantoonbare - interne controle gedurende de gebruiksperiode geen onverklaarbare afwijkingen in het gebruik zijn geconstateerd en ook gebruikers geen melding hebben gemaakt van onregelmatigheid.
Het is mogelijk dat het ontstaan van een identificatiemiddel en het activeren daarvan voor gebruik in dit kader gescheiden is. Voorbeeld daarvan is het uitgeven van het rijbewijs met daarop een nog niet geactiveerd publiek identificatiemiddel. Voor het activeren van de mogelijkheid om dit identificatiemiddel als publiek identificatiemiddel te gebruiken is een actieve handeling van de gebruiker noodzakelijk in de vorm van het gebruik zijn identificatiemiddel dat is gericht op activering. Een ander voorbeeld is een identificatiemiddel dat in een ander kader is uitgegeven en voor een ander doel en dat wordt hergebruikt in dit kader. Ook in dat geval moet de gebruiker de expliciete wens uiten om het identificatiemiddel ook in dit kader te willen gebruiken.

2. Als invulling op de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.2 Uitgifte, uitreiking en activering bij betrouwbaarheidsniveau Hoog geldt voor het niveau Hoog dat gewaarborgd wordt dat minimaal één authenticatiefactor of activeringscode persoonlijk en na identificatie wordt verstrekt aan de gebruiker.

De kans dat alle authenticatiefactoren gedurende het proces voor de uitgifte en activering van een identificatiemiddel in handen komen van een andere persoon dan de gebruiker moet op niveau Hoog in beginsel afwezig zijn.

2.2.3. Schorsing, herroeping en reactivering

Vereisten elementen

Ten aanzien van schorsing, herroeping en reactivering van identificatiemiddelen vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/of te herroepen. 2. Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen. 3. Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.2.3 Schorsing, herroeping en reactivering

LAAG

1. Het is mogelijk het elektronische identificatiemiddel snel en doeltreffend te schorsen en/of te herroepen.

RICHTLIJN VOOR BEOORDELING:
Dit behoort openbaar toegankelijk te zijn. Mogelijke voorbeelden zijn: telefonisch, via een website, een e-mailadres etc. Indien een instantie die verificaties uitvoert een verzoek hiertoe ontvangt, moet er zo snel mogelijk actie worden ondernomen

2. Er bestaan maatregelen om ongeoorloofde schorsing, herroeping en reactivering te voorkomen.

RICHTLIJN VOOR BEOORDELING:
In het algemeen impliceert dit authenticatie van de bevoegdheid van de aanvrager om zo te handelen. Het behoort te worden vastgesteld wie naast de gebruiker schorsing en/of herroeping mag toestaan, bijvoorbeeld relevante overheidsinstanties.

3. Een elektronisch identificatiemiddel mag slechts worden gereactiveerd indien nog steeds wordt voldaan aan dezelfde betrouwbaarheidsvereisten als die welke voorafgaand aan de schorsing of herroeping van kracht waren.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven.

Nadere duiding voor de Nederlandse situatie
Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van schorsing, herroeping en reactivering wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.3 Schorsing, herroeping en reactivering bij betrouwbaarheidsniveau Laag punt 1 geldt voor de niveaus Substantieel en Hoog dat bij gerede vermoedens van misbruik en bij melding van vermissing van het identificatiemiddel dat identificatiemiddel of de authenticatiefunctie ervan ingetrokken of geschorst moet kunnen worden.

Intrekking of schorsing van de authenticatiefunctie betreft hier het onmogelijk maken om met het betreffende identificatiemiddel toegang te verkrijgen tot online publieke diensten van bestuursorganen en aangewezen organisaties. Een gerede vermoeden van misbruik kan bijvoorbeeld voortkomen uit een gedetecteerd signaal of ontvangen melding. Het betreft een op redelijke gronden gebaseerd vermoeden met betrekking tot de uitgifte van identificatiemiddelen, het gebruik daarvan en waarbij het persoonlijke belang van de gebruiker of een maatschappelijk belang in het geding is. Daarbij kan het bijvoorbeeld gaan om:

a. een (dreigend) strafbaar feit;
b. een (dreigende) schending van wet- en regelgeving;
c. een (dreiging van) bewust onjuist informeren van bestuursorganen en aangewezen organisaties;
d. een (dreigende) verspilling van overheidsgeld;
e. (een dreiging van) het bewust achterhouden, vernietigen of manipuleren van informatie over deze feiten.

2. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.3 Schorsing, herroeping en reactivering bij betrouwbaarheidsniveau Laag punt 2 geldt voor de niveaus Substantieel en Hoog dat de procedure voor schorsing, intrekking en reactivering publiceert wordt gepubliceerd. De procedure bevat in elk geval:

a. wie gerechtigd is om het verzoek te doen, waaronder in elk geval:
1°. de gebruiker zelf en;
2°. de bevoegde vertegenwoordiger van de gebruiker en;
3°. de bevoegde medewerker van de aanbieder en;
4°. de bevoegde vertegenwoordiger van het ministerie van BZK;
b. de weg waarlangs het verzoek gedaan moet worden;
c. het verzoek aan de gebruiker om de reden voor het verzoek op te geven indien het gaat om vermoedens van misbruik of diefstal van het identificatiemiddel.

3. Gewaarborgd wordt dat de doorlooptijd van een verzoek tot schorsen, intrekken of reactiveren minimaal voldoet aan de vereisten voor intrekking van gekwalificeerde certificaten

zoals is aangeven in de norm ETSI EN 319411-1 voor gekwalificeerde certificaten, par 6.2.4 Identification en authentication for revocation request.
De norm ETSI EN 319411-1 betekent dit geval dat binnen 24 uur na dat een verzoek is gedaan volgens de gepubliceerde procedure, betrouwbaar wordt vastgesteld of het verzoek afkomstig is van de juiste persoon en ook dat binnen 60 minuten nadat is geconcludeerd dat het verzoek door de juiste persoon is gedaan dit verzoek tot schorsing, intrekking of reactivering is uitgevoerd..

4. Verzoeken tot- en de uitvoering van schorsingen, intrekkingen en reactiveringen worden vastgelegd met het oog op onderzoek van misbruik en geschillen. De vastlegging van de verzoeken worden doeltreffend geanalyseerd met het oog op het voorkomen van oneigenlijke verzoeken.

5. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.3 Schorsing, herroeping en reactivering bij betrouwbaarheidsniveau Laag punt 3 geldt voor de niveaus Substantieel en Hoog dat voor een heractivatie na schorsing van een identificatiemiddel wordt gekozen voor één van de volgende mogelijkheden:

1°. inzet van een tweede geldig identificatiemiddel met een gelijk betrouwbaarheidsniveau van de gebruiker of;

2°. volgen van het identificatieproces dat is gebruikt voor de uitgifte van het identificatiemiddel of;

3°. vaststelling dat de gebruiker nog in bezit is van het identificatiemiddel en;

4°. gebruik van een back-up authenticatiefactor die wordt ingevoerd door de gebruiker zelf. De back-up authenticatiefactor moet in dat geval met dezelfde betrouwbaarheid als de primaire authenticatiefactor zijn uitgereikt.

5. Een identificatiemiddel dat na onderzoek ten onrechte op initiatief van de aanbieder blijkt te zijn geschorst door de bevoegde medewerker (zie lid 2 sub onder 3) mag door de aanbieder zelf mag worden gereactiveerd.

2.2.4. Verlenging en vervanging

Vereisten elementen

23

Ten aanzien van schorsing, herroeping en reactivering van identificatiemiddelen vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.
Substantieel	Zelfde als niveau laag.
Hoog	Niveau laag, plus: Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.2.4 Verlenging en vervanging

LAAG

Rekening houdend met het risico dat de persoonsidentificatiegegevens zijn gewijzigd, moet voor verlenging of vervanging aan dezelfde betrouwbaarheidsvereisten zijn voldaan als voor het initiële proces van bewijs en verificatie van de identiteit, of moet worden uitgegaan van een geldig elektronisch identificatiemiddel met hetzelfde of een hoger betrouwbaarheidsniveau.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven.

HOOG

Niveau laag, plus:

Als voor verlenging of vervanging wordt uitgegaan van een geldig elektronisch identificatiemiddel, worden de identiteitsgegevens geverifieerd aan de hand van een gezaghebbende bron.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven.

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van verlenging en vervanging wordt het volgende uitgangspunt gehanteerd:

1. bij vervanging of vernieuwing van één enkele authenticatiefactor van het identificatiemiddel, wordt gewaarborgd dat de uitgifte daarvan het betrouwbaarheidsniveau van het identificatiemiddel doeltreffend handhaaft. 24

Als het niet noodzakelijk is om het gehele identificatiemiddel te vervangen maar slechts een enkele authenticatiefactor wordt vervangen zoals een smartcard, een PIN, wachtwoord of een herinstallatie van een authenticatie-app op een smartphone etc. dan mag de wijze waarop deze enkele authenticatiefactor wordt uitgegeven het betrouwbaarheidsniveau van het identificatiemiddel als zodanig niet aantasten.

2. In aanvulling op de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.2.4 Verlenging en vervanging bij betrouwbaarheidsniveau Hoog geldt voor het niveau Hoog dat in dit controleprotocol met verlengen en vervangen van een identificatiemiddel wordt bedoeld dat alle authenticatiefactoren worden vervangen. Verlengen en vervangen wordt derhalve gelijk gesteld met het uitgeven van een nieuw identificatiemiddel. Indien een middel niet in zijn geheel, dus slechts een enkele authenticatiefactor wordt vervangen is hetgeen lid 1 aangeeft passend om te voldoen aan de hierboven genoemde eIDAS vereisten.

2.3. *Authenticatie*

Dit onderdeel is met name gericht op dreigingen die gepaard gaan met het gebruik van het authenticatiemechanisme. Het vermeldt de vereisten voor elk van de betrouwbaarheidsniveaus. In dit onderdeel wordt ervan uitgegaan dat de controles in overeenstemming zijn met de risico's op het desbetreffende niveau.

In de eIDAS verordening 1502 zijn de regels en waarborgen neergelegd waaraan authenticatiemechanisme moeten voldoen om authenticaties te kunnen uitvoeren op de betrouwbaarheidsniveaus substantieel en hoog. Er wordt geregeld hoe de communicatie richting de gebruiker moet plaatsvinden op het moment dat een gebruiker zich authenticeert. Van belang is dat de gebruiker op de hoogte wordt gesteld c.q. bevestigd krijgt dat bij een bepaalde

dienstverlener wordt ingelogd. De gebruiker moet daarbij de mogelijkheid krijgen het proces af te breken en indien nodig contact op te nemen, bijvoorbeeld indien de gebruiker afwijkend gebruik vermoedt. In het artikel worden tevens regels gesteld over de wijze waarop hergebruik van authenticaties kan plaatsvinden (single sign on, ook wel eenmalig inloggen genoemd).

2.3.1. Authenticatiemechanisme

Vereisten elementen

Ten aanzien van het authenticatiemechanisme vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld. In de onderstaande tabel worden voor elk betrouwbaarheidsniveau de vereisten weergegeven voor het authenticatiemechanisme, door middel waarvan de natuurlijke persoon of rechtspersoon het elektronische identificatiemiddel gebruikt om zijn identiteit te bevestigen tegenover een vertrouwende partij.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd. 2. Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse. 3. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.
Substantieel	Niveau laag, plus: 1. Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie. 2. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.

Hoog	Niveau substantieel, plus: Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.3.1 Authenticatiemechanisme

RICHTLIJN VOOR BEOORDELING:

De in de authenticatiefase gebruikte authenticatiemechanismen kunnen niet alle aanvallen volledig voorkomen; ze kunnen slechts op een bepaald beveiligings-/betrouwbaarheidsniveau weerstand bieden tegen aanvallen. Een standaardmanier om de weerstand van verschillende mechanismen te kwantificeren is ze te rangschikken op basis van hun weerstand tegen aanvallen met een bepaald aanvalspotentieel (d.w.z. de kracht van een aanvaller).

Voor het betrouwbaarheidsniveau wordt gebruikgemaakt van de termen "laag", "gematigd" en "hoog" om de verschillen in aanvalspotentieel aan te geven. Deze terminologie is ontleend aan ISO/IEC 15408 "Information technology – Security techniques – Evaluation criteria for IT security" en ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". De tekst van de normen is ook vrij beschikbaar op www.commoncriteriaportal.org/cc (CCPART1-3 is gelijkwaardig aan ISO/IEC 15408 en CEM is gelijkwaardig aan ISO/IEC 18045).

ISO/IEC 15408-1 bevat de volgende definitie "aanvalspotentieel – maatstaf van de inspanning die moet worden gestoken in het aanvallen van een [mechanisme], uitgedrukt aan de hand van de expertise, middelen en motivatie van een aanvaller".

Bijlage B.4 bij ISO/IEC 18045 / CEM bevat richtlijnen voor het berekenen van het aanvalspotentieel dat nodig is om een bepaalde zwakte van een authenticatiemechanisme te benutten.

Om te voldoen aan de in het uitvoeringsbesluit vervatte eisen, behoort er een beoordeling van de weerstand tegen mogelijke aanvallen te worden uitgevoerd.
De beoordeling behoort rekening te houden met relevante dreigingen. Zo noemt ISO 29115 bijvoorbeeld: online gissen, offline gissen, kopiëren van legitimatiebewijzen, phishing, afluisteren, aanvallen door herafspelen, sessie hijacking, man-in-the-middle, diefstal van legitimatiebewijzen, spoofing en masquerading.
Tijdens het beoordelen van de weerstand tegen aanvallen behoort rekening te worden gehouden met het hele authenticatiemechanisme, met inbegrip van de risico's die het gevolg zijn van het verifiëren van het bezit van het elektronische identificatiemiddel.

Bijvoorbeeld

- *Voor betrouwbaarheidsniveau Hoog is het niet voldoende dat een smartcard een cryptografische sleutel tegen manipulatie met een hoog aanvalspotentieel beschermt, maar moet ook het cryptografische protocol de verificatie van het bezit van de sleutel tegen manipulatie/herafspelen tegen een hoog aanvalspotentieel beschermen.*
- *Voor een eenmalig wachtwoord-token, waarbij het gegenereerde eenmalige wachtwoord via een beveiligd kanaal wordt verzonden (bijv. TLS), wordt de sterkte van de op bezit*

gebaseerde factor niet alleen beperkt door de sterkte van het token, maar ook door de sterkte van het beveiligde kanaal.

- *Het mechanisme voor het aantonen van bezit van een op tijd gebaseerde generator van eenmalige wachtwoorden is het overleggen van een gegenereerd eenmalig wachtwoord aan de instantie die de verificatie uitvoert. De kracht van dit mechanisme wordt onder andere beperkt door de lengte van het eenmalige wachtwoord, het tijdskader voor de geldigheid van het wachtwoord en de vertrouwelijkheid van de overdracht.*

Met redelijke aannames over het beveiligingsniveau van componenten die worden gebruikt door, maar geen deel uitmaken van het authenticatiestelsel (bijv. de omgeving van de gebruiker, browser, smartphone etc.) behoort rekening te worden gehouden tijdens de risicobeoordeling.

Componenten kunnen in verschillende configuraties met verschillende beveiligingsinstellingen worden toegepast.

Zo zou er bij de beoordeling bijvoorbeeld vanuit kunnen worden gegaan dat de gebruiker een persoonlijke firewall en antivirusbescherming op zijn/haar computer heeft draaien.

Als tegenvoorbeeld zou het momenteel niet redelijk zijn aan te nemen dat de browser van de gebruiker dusdanig is geconfigureerd dat deze alleen gebruikmaakt van beveiligde coderingssuites voor transportlaagbeveiliging (Transport Layer Security - TLS); dit kan door de service echter wel worden afgedwongen.

Bij de beoordeling zou kunnen worden uitgegaan van redelijke instellingen voor de componenten die geen deel uitmaken van het authenticatiestelsel.

LAAG

Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd.

RICHTLIJN VOOR BEOORDELING:

Het vrijgeven van persoonsidentificatie-informatie betreft het overdragen van de minimale dataset (MDS) aan de vertrouwende partij

2. Indien als onderdeel van het authenticatiemechanisme persoonsidentificatiegegevens worden opgeslagen, wordt die informatie beveiligd ter bescherming tegen verlies en schending, met inbegrip van offlineanalyse.

RICHTLIJN VOOR BEOORDELING:

Voor opgeslagen persoonsgegevens moeten strenge toegangscontroles gelden. Er behoren maatregelen te worden toegepast om persoonsidentificatiegegevens te beschermen*, bijvoorbeeld versleutelen en hashing conform goede praktijken zoals het Algorithms, Key Sizes and Parameters Report van ENISA* of nationale cryptografische richtlijnen.

Alle toegang behoort gecontroleerd te worden

3. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een laag aanvalspotentieel.

RICHTLIJN VOOR BEOORDELING:

Alle vereiste verificatiestappen moeten duidelijk worden beschreven, geïmplementeerd en getest

SUBSTANTIEEL

Niveau laag, plus:

1.Alvorens persoonsidentificatiegegevens worden vrijgegeven, worden het elektronische identificatiemiddel en de geldigheid ervan op betrouwbare wijze geverifieerd door middel van dynamische authenticatie**.**

RICHTLIJN VOOR BEOORDELING:

In de praktijk betekent dit dat het authenticatiemiddel een eenmalige code of een eenmalige reactietest ('challenge-response') moet omvatten om te waarborgen dat het echt dynamisch is. De eenmalige code of test moet dusdanig gegenereerd worden dat er niet mee geknoeid kan worden.

Bij het gebruik van willekeurige getallen in een reactietestprotocol dient men ervoor te zorgen dat de "kwaliteit" van deze getallen wordt gewaarborgd, *bijvoorbeeld door goede praktijken te volgen voor cryptografisch beveiligde generatoren van pseudo-willekeurige getallen*

2. Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een gematigd aanvalspotentieel.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven

HOOG

Niveau substantieel, plus:

Het authenticatiemechanisme voorziet in beveiligingscontroles ter verificatie van het elektronische identificatiemiddel, die het zeer onwaarschijnlijk maken dat de authenticatiemechanismen kunnen worden omzeild door methoden als gissen, afluisteren, herafspelen of manipuleren van communicatie door een aanvaller met een hoog aanvalspotentieel.

RICHTLIJN VOOR BEOORDELING:

Indien cryptografie wordt gebruikt om een authenticatiemechanisme te beveiligen, behoren krachtige cryptografische protocollen en sleutels met een passende lengte te worden geselecteerd.

Een belangrijke methode voor het waarborgen van de sterkte van cryptografische protocollen is het uitvoeren van cryptografische analyses zoals cryptografische beveiligingsbewijzen.

Als bekend is dat een protocol niet beveiligd is (bijv. SSLv3), behoort daarmee rekening te worden gehouden; dat geldt ook voor bekende aanvallen in de praktijk op bepaalde cryptografische protocollen en maatregelen die zijn ingesteld om aanvallen af te slaan waar dergelijke protocollen gebruikt worden.

Indien het authenticatiemechanisme gebruikmaakt van een cryptografische oplossing, behoort niet alleen rekening te worden gehouden met de cryptografische primitieven, maar ook met de protocollen en de omgeving, met name sleutelbeheer.

Voorbeeld: Een typisch mechanisme voor sleutelbeheer is gebruikmaken van een publieke sleutelinfrastructuur. De operationele beveiliging van de CA (certificatie-autoriteit - Certification Authority) is rechtstreeks van invloed op de beveiliging van het authenticatiemechanisme. Naast de zuiver technische beveiliging van de CA, ook de organisatorische aspecten.

Indien op meer CA's wordt vertrouwd voor uitgifte van certificaten voor een bepaald deel van een stelsel voor elektronische identificatie, moet rekening worden gehouden met de algehele beveiliging van alle vertrouwde CA's.

Een voorbeeld voor dit laatste: indien de identificatie van communicatie-eindpunten wordt uitgevoerd met behulp van certificaten afkomstig van een "Internet PKI" (d.w.z. dat deze worden uitgegeven door CA's waarvan het root-certificaat zich in de trust-store van de browser van de gebruiker bevindt), moet de beveiliging van alle CA's die zich in de trust-stores bevinden in aanmerking worden genomen. In het algemeen behoort de gebruiker volgens goede praktijken, indien de infrastructuur van het stelsel voor elektronische identificatie gebruikmaakt van een Internet PKI, te worden geadviseerd om voor betrouwbaarheidsniveau Hoog gebruik te maken van afdoende beveiligingsmechanismen.

De authenticatie behoort bescherming te bieden tegen het manipuleren van authenticatiegegevens waarmee men de betrokkene wil doen geloven dat er authenticatie naar een andere vertrouwende partij plaatsvindt

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van authenticatiemechanisme wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.3.1 Authenticatiemechanisme bij betrouwbaarheidsniveau Laag punt 2 geldt voor niveaus Substantieel en Hoog dat wordt gewaarborgd dat persoonsidentificatiegegevens worden beschermd conform het bepaalde in hoofdstuk 3 Bescherming van persoonsgegevens van de set van eisen eID.
[In dit artikel zal worden geregeld dat tbv het BSN-domein gegevens in overeenstemming met de doelstellingen zoals vastgelegd in artikel X van de wet elektronisch bestuurlijk verkeer Belastingdienst en het Besluit verwerking persoonsgegevens generieke digitale infrastructuur dienen te worden, dat verwerking plaatsvindt op grond van een af te sluiten verwerkersovereenkomst met de minister van BZK en dat de AVG dient te worden nageleefd]

2. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.3.1 Authenticatiemechanisme bij betrouwbaarheidsniveau Substantieel punt 1 geldt voor de betrouwbaarheidsniveaus Substantieel en Hoog dat gewaarborgd is dat de afhandeling van een authenticatieverzoek in elk geval voldoet aan de eisen voor het betrouwbaarheidsniveau van het betreffende authenticatieverzoek.

3. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.3.1 Authenticatiemechanisme bij betrouwbaarheidsniveau Substantieel punt 2 geldt voor de niveaus Substantieel en Hoog dat:

a. de gebruiker bij het gebruik van zijn identificatiemiddel bericht ontvangt dat hij op het punt staat in te loggen bij een specifieke dienstaanbieder en, indien van toepassing, bij een specifieke door de betreffende dienstaanbieder geregistreerde dienst. Daarbij geldt dat:

1°. de gebruiker in staat wordt gesteld om op basis van deze informatie het inloggen af te breken;

2°. de betrouwbaarheid van het bericht gewaarborgd wordt, ook als de toepassing waarvoor de authenticatie bestemd is of het platform waarop deze toepassing actief is, gecorrumpeerd is.

b. de gebruiker in staat wordt gesteld om met informatie over uitgevoerde authenticatie pogingen bij een dienstverlener zoals is opgenomen in paragraaf 3 Informatie voor gebruikers in

contact te treden met die dienstverlener over afwijkende transacties of mogelijke geschillen ten aanzien van transacties;

c. in contact wordt getreden met de gebruiker zodra gerede vermoedens bestaan van misbruik van het identificatiemiddel van de gebruiker. Het contact met de gebruiker over (vermoed) misbruik vindt plaats langs een ander communicatiekanaal dan het identificatiemiddel van de gebruiker;

d. Voor niveau substantieel geldt dat de gebruikerservaring mag geoptimaliseerd worden maar dat elke authenticatie moet blijven voldoen aan weerstand tegen in lid 4 genoemde aanvalspotentieel. Dit betekent dat een eenmaal uitgevoerde authenticatie mag worden hergebruikt onder de voorwaarde dat:

1°. Het contact (technisch: sessie) tussen de gebruiker en de Authenticatiedienst mag niet ouder zij dan 2 uur om te mogen worden hergebruikt voor als authenticatiefactor. Deze tijdspanne wordt redelijk geacht met het oog op het uitvoeren van een activiteit door een gebruiker;

2°. bij doorgeleiden van een gebruiker naar een andere dienst of dienstverlener wordt de gebruiker daarover geïnformeerd en om instemming gevraag conform het bepaalde in lid 3 sub a.

3°. bij doorgeleiden van een gebruiker naar een andere dienst of dienstverlener de gebruiker is vereist dat de gebruiker minimaal één authenticatiefactor van zijn middel moet gebruiken, bijvoorbeeld een PIN of een biometrisch kenmerk.

4°. maatregelen zijn genomen die de integriteit van het contact (technisch: sessie waarborgen tegen o.a. sessie hijacking) tussen de gebruiker en de authenticatiedienst waarborgen.

De authenticatie moet ook bij optimalisatie van de gebruikerservaring blijven voldoen aan de vereiste weerstand tegen een gematigd aanvalspotentieel.

e. Voor niveau hoog geldt dat de gebruikerservaring geoptimaliseerd mag worden maar dat elke authenticatie moet blijven voldoen aan de vereiste weerstand tegen het in lid 5 genoemde hoge aanvalspotentieel.

Dit betekent dat een eenmaal uitgevoerde authenticatie mag worden hergebruikt onder de voorwaarde dat:

1°. Het contact (technisch: sessie) tussen de gebruiker en de Authenticatiedienst mag niet ouder zij dan 2 uur om te mogen worden hergebruikt voor als authenticatiefactor. Deze tijdspanne wordt redelijk geacht met het oog op het uitvoeren van een activiteit door een gebruiker;

2°. bij doorgeleiden van een gebruiker naar een andere dienst of dienstverlener wordt de gebruiker daarover geïnformeerd en om instemming gevraag conform het bepaalde in lid 3 sub a.

3°. bij doorgeleiden van een gebruiker naar een andere dienst of dienstverlener de gebruiker is vereist dat de gebruiker minimaal twee authenticatiefactoren van zijn middel moet gebruiken, bijvoorbeeld een PIN of een biometrisch kenmerk.

4°. maatregelen zijn getroffen die de integriteit van het contact (technisch: sessie waarborgen tegen o.a. sessie hijacking) tussen de gebruiker en de authenticatiedienst waarborgen.

De authenticatie moet ook bij optimalisatie van de gebruikerservaring blijven voldoen aan de vereiste weerstand tegen een hoog aanvalspotentieel.

In paragraaf 3 Informatie voor gebruikers zijn de verplichtingen opgenomen voor de aanbieder van de authenticatiedienst om de gebruiker inzage te bieden in transacties die hij heeft uitgevoerd met zijn identificatiemiddel, onder meer om daarmee afwijkend gebruik van zijn identificatiemiddel te ontdekken. Deze invulling van het inzagerecht dient daarmee tevens als 'beveiligingscontrole'. De eis om zowel de geregistreerde dienst als de dienstaanbieder aan de gebruiker te tonen heeft tot doel om de gebruiker adequaat te informeren over authenticaties die al dan niet mogelijke rechtsgevolgen kunnen hebben. Daarnaast beoogt deze eis een dienstverlener te ontzorgen in geval de gebruiker zich laat vertegenwoordigen voor specifieke handelingen bij de dienstverlener. Het tweede deel van de eis betreft eisen aan de betrouwbaarheid van het bericht aan de gebruiker. Onder strikte voorwaarden wordt op de niveaus substantieel en hoog een vorm zogenaamde 'single sign on' toegestaan om de gebruikerservaring te kunnen optimaliseren. Daarbij moet men zich rekenschap geven van het feit dat bij toepassing van deze vorm van gebruiksoptimalisatie de gehele authenticatie weerstand blijft bieden tegen het in dit artikel bepaalde met betrekking tot het genoemde een aanvalspotentieel en het aantonen daarvan.

4. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.3.1 Authenticatiemechanisme bij betrouwbaarheidsniveau Substantieel punt 2 geldt voor het niveau Substantieel dat gewaarborgd wordt dat het correct functioneren van het authenticatiemechanisme weerstand biedt tegen fysieke en logische manipulatie door een aanvaller met een 'gematigd

aanvalspotentieel' (moderate attacker potential) in de zin van de norm ISO/IEC 15408-3 (Common Criteria) en de bijbehorende evaluatienorm ISO/IEC 18045 Annex B. Daarbij geldt dat:

a. de weerstand tegen een 'gematigd aanvalspotentieel' wordt beoordeeld en bevestigd door een ter zake deskundige en onafhankelijke instantie. De eisen aan deze beoordelende instantie zijn opgenomen in het Hoofdstuk Naleving en Toezicht.

b. deze weerstand periodiek wordt herbevestigd. Herbevestiging door een ter zake deskundige en onafhankelijke instantie vindt in ieder geval plaats:

1°. bij substantiële wijzigingen aan het authenticatiemechanisme en;

2°. bij wijzigingen van de werking van het identificatie, of;

3°. na het verstrijken van drie jaren na de laatste beoordeling van de weerstand.

5. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.3.1 Authenticatiemechanisme bij betrouwbaarheidsniveau Hoog geldt voor het niveau Hoog dat het correct functioneren van het authenticatiemechanisme weerstand moet bieden tegen fysieke en logische manipulatie door een aanvaller met een 'hoog aanvalspotentieel' (high attacker potential) in de zin van de Common Criteria (ISO 15408-3) en de bijbehorende evaluatienorm (ISO/IEC 18045 Annex B). Daarbij geldt dat:

a. het authenticatiemechanisme een betrouwbaar kanaal moet bevatten voor notificatie van de inlogpoging van de gebruiker en de bevestiging van het authenticatieverzoek door de gebruiker, waarbij de aanbieder de gebruiker bij het gebruik van zijn identificatiemiddel bericht dat hij op het punt staat in te loggen op een specifieke dienstaanbieder en, indien van toepassing, een specifieke door de betreffende dienstverlener geregistreerde dienst. Daarbij geldt dat:

1°. de gebruiker in staat wordt gesteld om op basis van deze informatie het inloggen af te breken.

2°. de betrouwbaarheid van het authenticatiebericht gewaarborgd wordt, ook als de toepassing waarvoor de authenticatie bestemd is of het platform waarop deze toepassing actief is, gecorrumpeerd is.

b. de weerstand tegen een 'hoog aanvalspotentieel' en gepubliceerde relevante technische kwetsbaarheden worden beoordeeld en bevestigd door een ter zake deskundige en onafhankelijke instantie. De eisen aan deze beoordelende instantie zijn opgenomen in het Hoofdstuk Naleving en Toezicht.

c. deze weerstand periodiek wordt herbevestigd. Herbevestiging door een ter zake deskundige en onafhankelijke instantie vindt in ieder geval plaats:

1°. bij substantiële wijzigingen aan het authenticatiemechanisme en;

2°. bij wijzigingen van de werking van het identificatie, of;

3°. na het verstrijken van drie jaren na de laatste beoordeling van de weerstand.

Het onderscheid tussen identificatiemiddel en authenticatiemechanisme is niet altijd scherp te maken en is een deel van het authenticatiemechanisme onderdeel van het identificatiemiddel. In dat geval moeten de aanbieders die de rollen van aanbieder van authenticatiediensten en aanbieder van een elektronisch identificatiemiddel vervullen gezamenlijk aantonen dat het authenticatiemechanisme de bedoelde weerstand biedt.

2.4. *Beheer en organisatie*

Waarborgen aan aanbieders van toegelaten middelen en authenticatiediensten

De eIDAS verordening stelt regels om te zorgen dat organisaties die diensten verlenen op de niveaus substantieel en hoog aan een aantal waarborgen voldoen. Er worden regels gesteld ten aanzien van de bedrijfsvoering, (financiële) draagkracht en het kunnen dragen van aansprakelijkheid voor hun activiteiten. Doel is om te zorgen dat de diensten worden aangeboden door organisaties waarvan de continuïteit geborgd is, en daarmee te continuïteit van de aangeboden identificatiemiddelen en authenticatiediensten. Om te zorgen dat de dienstverlening adequaat wordt geadministreerd en de integriteit van de dienstverlening controleerbaar is zijn hierover regels opgenomen.

Teneinde veilige en betrouwbare dienstverlening te bevorderen worden regels gesteld aan de veiligheidseisen voor het personeel en kwaliteitseisen die betrekking hebben op de dienstverlening (zoals opleiding om deskundigheid te borgen).

Er worden tevens regels gesteld voor situaties waarin, indien aan de orde, op een ordentelijke wijze gegevens (van gebruikers) kunnen worden veiliggesteld. Onder meer voor situaties waarbij de dienstverlening beëindigd wordt of aanbieders dienstverlening willen overdragen.

Alle aanbieders die een dienst verlenen op het gebied van elektronische identificatie in een grensoverschrijdende context beschikken over gedocumenteerde methoden en beleid voor het beheer van informatiebeveiliging, benaderingen voor risicobeheersing en andere erkende controlemethoden, zodat zij de bevoegde bestuursorganen van de lidstaten op het gebied van stelsels voor elektronische identificatie garanties kunnen bieden dat in doeltreffende praktijken is voorzien. In onderdeel 2.4 wordt ervan uitgegaan dat alle vereisten/elementen in overeenstemming zijn met de risico's op het desbetreffende niveau.

2.4.1. Algemene bepalingen

Vereisten elementen

Ten aanzien van algemene aspecten aan organisaties vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn. 2. De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard. 3. De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen beschikken om hun activiteiten en de dienstverlening voort te zetten. 4. De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere

	entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden. 5. Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of ~~assurance~~ which support the eIDAS Regulation

2.4. Beheer en organisatie.

RICHTLIJN VOOR BEOORDELING:

Alle deelnemers omvat de partijen bij het proces van grensoverschrijdende authenticatie, met inbegrip van de identiteitsaanbieder en validatiediensten die door de lidstaat (eventueel) worden uitgevoerd, maar niet de gezaghebbende bronnen die worden gebruikt.

Als algemeen beginsel van risicomanagement geldt dat het aan de organisatie is te kiezen welk niveau van risico voor haar acceptabel is. Dit algemene beginsel wordt bijgesteld door de eis in 2.4, aangezien de organisatie controlemethoden behoort te hebben ingericht die in verhouding staan tot de risico's op het niveau in kwestie.

Aan veel / de meeste eisen van dit hoofdstuk wordt voldaan indien er hetzij

- een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 is ingericht en aan audits wordt onderworpen

- de aanbieders die operationele diensten aanbieden gekwalificeerde verleners van vertrouwensdiensten volgens de eIDAS-verordening zijn

Dit sluit het gebruik van andere normen, bijv. geschikte nationale stelsels die aan de eisen in dit hoofdstuk voldoen, niet uit.

In het kader van de richtlijnen voor de eisen [ntb] worden de eisen op basis van ISO/IEC 27001:2013 en de eisen voor gekwalificeerde verleners van vertrouwensdiensten in kaart gebracht. In het geval van een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 worden alle eisen uit de hoofdstukken 2.4.4 tot en met 2.4.6 afgedekt door relevante beheersmaatregelen uit die norm

2.4.1 Algemene bepalingen

LAAG

1. Aanbieders die een operationele dienst aanbieden die onder deze verordening valt, zijn een overheidsinstantie of een rechtspersoon die door het nationale recht van een lidstaat als zodanig wordt erkend, over een gevestigde organisatie beschikt en volledig operationeel is op alle gebieden die voor de verlening van de diensten relevant zijn.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven

2. De aanbieders voldoen aan al hun wettelijke verplichtingen in verband met het verrichten en leveren van de dienst, onder meer wat betreft de soorten informatie die mogen worden gevraagd, de wijze waarop het bewijs van de identiteit wordt geleverd, welke informatie mag worden bewaard en hoe lang deze mag worden bewaard.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven

3. De aanbieders kunnen aantonen dat zij in staat zijn het risico van de aansprakelijkheid voor schade op zich te nemen en over voldoende financiële middelen te beschikken om hun activiteiten en de dienstverlening voort te zetten.

RICHTLIJN VOOR BEOORDELING:

Men mag ervan uitgaan dat een overheidsinstantie over voldoende financiële middelen beschikt om aan aansprakelijkheden krachtens de verordening te voldoen. Andere manieren waarop kan worden aangetoond dat aan deze eis wordt voldaan zijn onder andere

- Passende verzekeringsdekking voor de verplichtingen.
- Een overeenkomst met een overheidsinstantie die de verplichtingen afdekt.
- Een wettelijke verplichting dat een overheidsinstantie de aansprakelijkheid/activiteiten indien nodig overneemt.

4. De aanbieders zijn verantwoordelijk voor het naleven van alle verplichtingen die zij aan andere entiteiten hebben uitbesteed en voor het voldoen aan het beleid inzake het stelsel, op dezelfde wijze als wanneer zij deze taken zelf vervulden.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven

5. Stelsels voor elektronische identificatie die niet volgens nationaal recht zijn opgezet, moeten over een doeltreffend beëindigingsplan beschikken. Dat plan omvat voorzieningen voor de ordelijke stopzetting van de dienstverlening of de voortzetting daarvan door een andere aanbieder, voor de wijze waarop de betrokken autoriteiten en

eindgebruikers worden ingelicht, alsook voor de wijze waarop de administratie wordt beschermd, bewaard en vernietigd overeenkomstig het voor het stelsel geldende beleid.

RICHTLIJN VOOR BEOORDELING:

Dit geldt zowel voor beëindiging van een dienst als het stilleggen ervan door externe instanties. Dergelijke plannen behoren alle voorzienbare omstandigheden af te dekken die tot beëindiging van de dienst / voortzetting door een andere aanbieder leiden

.

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van algemene eisen aan private organisaties wordt het volgende uitgangspunt gehanteerd:

1. bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502, paragraaf 2.4.1. Algemene bepalingen bij betrouwbaarheidsniveau Laag punt 3, geldt voor de betrouwbaarheidsniveaus Substantieel en Hoog dat bij het aanbieden van een toegelaten privaat identificatiemiddel aantoonbaar gewaarborgd is dat aansprakelijkheidsrisico's kunnen worden gedragen met het oog op de continuïteit van die dienstverlening en dat over voldoende financiële middelen wordt beschikt. Aantoonbaar gewaarborgd moet zijn, bijvoorbeeld door middel van verzekeringen dan wel zijn financiële positie, een verhaalbaarheid op basis van genoemde vormen van aansprakelijkheid in artikel 6:196b Burgerlijk Wetboek (die betrekking hebben op zowel directe als indirecte schade) af te dekken ten bedrage van tenminste EUR 10.000.000 per jaar

2. Het voldoen aan het eerste lid kan worden aangetoond door onder meer bankverklaringen, jaarrekeningen, omzetverklaringen, polissen en auditverklaringen.

Beëindiging en overgang

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van beëindiging en overgang wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.1. Algemene bepalingen bij betrouwbaarheidsniveau Laag punt 5 geldt voor de niveaus Substantieel en Hoog dat wordt vastgesteld dat aanbieders van private toegelaten identificatiemiddelen beschikken over een plan voor het beëindigen van het gebruik van het identificatiemiddel in het BSN-domein, ongeacht de intentie of oorzaak van de beëindiging, dat met het oog op navraag door gebruikers en onderzoek van misbruik in elk geval voorziet in:

1°. het onveranderd veiligstellen van de opgeslagen gegevens behorende bij de identiteit van de gebruikers en gegevens over het gebruik van het identificatiemiddel in het BSN-domein die met de identificatiemiddelen zijn uitgevoerd of;

2°. het veilig en onveranderd overdragen van de opgeslagen gegevens behorende bij de identiteit van de gebruikers en de transacties in het BSN-domein die met de identificatiemiddelen zijn uitgevoerd, waarbij de mogelijkheid moet bestaan dat alle bedoelde gegevens door de partij waaraan de gegevens zijn overgedragen betekenisvol gelezen en bewerkt kunnen worden.

2. Er wordt gecontroleerd of afspraken zijn gemaakt die regelen dat in situaties waarin een aanbieder van een privaat identificatiemiddel het voornemen heeft het gebruik in het BSN-domein te beëindigen, deze over te dragen aan een andere onderneming of op een andere onderneming over te laten gaan, onverwijld de minister van dat voornemen op de hoogte brengt, waarbij:

1°. de aanbieder bij beëindiging, overdracht aan of overgang op een andere onderneming de aanwijzingen van de minister volgt, en;

2 °. de minister bij stopzetting bepaalt of de gegevens door de aanbieder worden vernietigd of aan een ander worden overgedragen, gericht op beschikbaarheid van de gegevens voor de gebruikers gedurende de vastgestelde termijnen.

2.4.2. Gepubliceerde mededelingen en informatie voor de gebruikers

Vereisten elementen

Ten aanzien van gepubliceerde mededelingen en informatie voor de gebruikers vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring. 2. Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring. 3. Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.4.2 Gepubliceerde mededelingen en informatie voor de gebruikers

LAAG

1. Er bestaat een gepubliceerde beschrijving van de dienst met alle toepasselijke voorwaarden en vergoedingen, inclusief eventuele gebruiksbeperkingen. De beschrijving van de dienst omvat een privacyverklaring.

RICHTLIJN VOOR BEOORDELING:

Publicatie kan worden afgedekt door

- de informatie op te nemen in een wet.
- de informatie in openbaar toegankelijke documenten te verstrekken

2. Er dient te worden voorzien in passend beleid en passende procedures om de gebruikers van de dienst tijdig en op betrouwbare wijze te informeren over elke wijziging van de beschrijving van de dienst, alle toepasselijke voorwaarden en de privacyverklaring.

RICHTLIJN VOOR BEOORDELING:

Een gebruiker is een actieve deelnemer aan een stelsel, een deelnemer kan ook een aanvrager zijn voordat er een elektronisch identificatiemiddel aan wordt uitgegeven (en, indien van toepassing, geactiveerd).

In deze context betekent informeren niet alleen dat informatie altijd tot de gebruiker gericht behoort te zijn. Informeren zoals bedoeld in deze eis is ook mogelijk door de vereiste informatie te publiceren op de website van de aanbieder, afhankelijk van de inhoud ervan met betrekking tot de wijziging en het nationale recht

3. Er dient te worden voorzien in passend beleid en passende procedures om verzoeken om informatie volledig en correct te beantwoorden.

RICHTLIJN VOOR BEOORDELING:

Er worden nu geen specifieke richtlijnen gegeven

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van informatieverstrekking aan gebruikers wordt het volgende uitgangspunt gehanteerd:
Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.2 Informatie voor gebruikers bij betrouwbaarheidsniveau Laag punt 3, wordt voor de niveaus Substantieel en Hoog gewaarborgd dat:

a. De gebruiker met gebruik van zijn identificatiemiddelen geassocieerd met de authenticatiedienst, inzage wordt gegeven in:

1°. de gegevens die over hem zijn vastgelegd ten behoeve van de uitgifte van zijn identificatiemiddel;

2°. de identificatiemiddelen die op zijn persoon of identiteit zijn uitgegeven;

3°. de transacties die zijn uitgevoerd met het identificatiemiddel dat is gekoppeld aan de persoon of identiteit van de gebruiker. Het geboden inzicht bestaat in elk geval uit de datum en tijd van inloggen en de dienst of dienstverlener waarop door de gebruiker is ingelogd.

b. de gebruiker in staat wordt gesteld om op basis van het geboden inzicht met de aanbieder doeltreffend in contact te treden met vragen en het melden van fouten of vermoedens van misbruik van zijn identificatiemiddel.

Door inzicht te geven aan de gebruiker in het gebruik van zijn identificatiemiddel krijgt de gebruiker de mogelijkheid van zelfcontrole. Deze zelfcontrole draagt tevens bij aan de detectie van fouten en het bestrijden van misbruik van het identificatiemiddel door derden.

Dit uitgangspunt betreft ook dat de gebruiker met een geldig identificatiemiddel online toegang tot de betreffende gegevens moet worden gegeven en op elk gewenst moment. In het geval de gebruiker onverhoopt niet met een geldig identificatiemiddel toegang tot zijn gegevens kan worden gegeven zal deze toegang op andere wijze vormgegeven moeten worden, bijvoorbeeld door telefonisch contact op te kunnen nemen, waarbij de identiteit van de gebruiker aan de hand van de bij de aanbieder beschikbare gegevens wordt gecontroleerd. De verplichtingen genoemd in sub a betreffen de gegevens die in elk geval getoond moeten worden.

2.4.3. Beheer van informatiebeveiliging

In de eIDAS uitvoeringsverordening 1502 wordt geregeld dat aanbieders een beheersysteem voor informatiebeveiliging hebben ingericht. Daarbij wordt op een aantal onderdelen gespecificeerd waarbij wordt aangehaakt bij gangbare praktijkstandaarden (ISO/IEC 27001). Tevens wordt geregeld dat, de getroffen maatregelen moeten worden beoordeeld op de weerstand tegen een specifiek aanvalspotentieel, omdat daadwerkelijke bescherming te toetsen. Dergelijke toetsen dienen periodiek te worden herhaald.

Vereisten elementen

Ten aanzien van beheer van informatiebeveiliging vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Substantieel	Niveau laag, plus: Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.
Hoog	Zelfde als niveau substantieel.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.4.3 Beheer van informatiebeveiliging

LAAG

Er bestaat een doeltreffend beheerssysteem voor informatiebeveiliging dat zorg draagt voor het beheer en de beheersing van informatiebeveiligingsrisico's.

RICHTLIJN VOOR BEOORDELING:

Het beheer van informatiebeveiligingsrisico's is relevant voor alle delen van het stelsel voor elektronische identificatie. Om doeltreffend te zijn moet het beheerssysteem voor informatiebeveiliging de relevante risico's voor alle delen van het stelsel in aanmerking nemen.

Afhankelijk van de organisatorische structuur van een stelsel voor elektronische identificatie, kan het ook passend zijn meer beheerssystemen voor informatiebeveiliging in te zetten voor de verschillende exploitanten van componenten van het stelsel

SUBSTANTIEEL

Niveau laag, plus:

Het beheerssysteem voor informatiebeveiliging voldoet aan beproefde normen en beginselen voor het beheer en de beheersing van informatiebeveiligingsrisico's.

RICHTLIJN VOOR BEOORDELING:

ISO/IEC 27001:2013 is een bekende en bewezen norm voor het managen van informatiebeveiligingsrisico's. Zie hoofdstuk 2.4.7 voor het waarborgen van 'compliance' (het voldoen aan deze norm)

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van beheer voor informatiebeveiliging wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf bij betrouwbaarheidsniveau Laag punt 1 geldt voor de niveaus Substantieel en Hoog dat:

a. een werkend beheersysteem voor informatiebeveiliging is ingericht. Dit beheerssysteem omvat in elk geval:

1°. een managementcyclus (PDCA);
2°. de diensten die in de authenticatieketen worden geleverd inclusief de daaraan ondersteunende processen en systemen;
3°. een analyse van de beveiligingsrisico's behorende bij de diensten die worden geleverd inclusief de ondersteunende processen en systemen;
4°. een vastlegging van de beheersmaatregelen die op basis van de risicoanalyse zijn genomen inclusief vastlegging van de relatie tussen risico's en beheersmaatregelen, waarbij eventuele rest risico's in kaart zijn gebracht en expliciet moeten zijn geaccepteerd;
5°. periodieke evaluaties of (interne) audits naar de doeltreffendheid van beheersmaatregelen en een vastlegging van opvolging van verbeterpunten. Hieronder wordt ook verstaan het periodiek testen van ondersteunende systemen op kwetsbaarheden. De periodiciteit wordt bepaald aan de hand van een vastgelegde risico afweging;
6°. Een management review van het beheerssysteem.
7°. een ingericht risicomanagementproces en het bijhouden van een risico-log
De standaard ISO/IEC 27001 wordt in dit kader beschouwd als referentie voor het inrichten van het beheersysteem voor informatiebeveiliging. Voor het vaststellen van maatregelen kunnen meerdere bronnen worden gebruikt zoals de standaarden Cobit, ISO 2700x en Baseline Informatiebeveiliging Rijk.

Op basis van de risico-afweging dient een set maatregelen getroffen te zijn. Daarvan maakt in ieder geval deel uit dat de toegang tot gegevensverzamelingen met betrekking tot de dienstverlening in het kader van identificatiemiddelen en authenticatie en daaraan ondersteunende systemen is beveiligd tegen toegang door onbevoegden. Dit betreft zowel de logische toegang als de fysieke toegang.

2.4.4. Bijhouden van de administratie

Vereisten elementen

Ten aanzien van het bijhouden van de administratie vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring. 2. De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.4.4 Bijhouden van de administratie

LAAG

1. Relevante informatie wordt vastgelegd en bewaard met behulp van een doeltreffend documentenbeheersysteem, met inachtneming van de toepasselijke wetgeving en goede praktijken op het gebied van gegevensbescherming en gegevensbewaring.

RICHTLIJN VOOR BEOORDELING:

Indien er een administratie wordt bijgehouden, dient het documentenbeheersysteem te waarborgen dat de integriteit en vertrouwelijkheid gedurende de levensduur van de administratie duurzaam worden gehandhaafd.

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.12 'Operational security' (Beveiliging bedrijfsvoering) in combinatie met A.18 'Compliance' (met name A.12.4 Logging and monitoring (Logging en bewaking))

2. De gegevens moeten worden bewaard voor zover dat is toegestaan door het nationale recht of een andere nationale bestuurlijke regeling, en beschermd gedurende de termijn die noodzakelijk is met het oog op financiële controle en onderzoek van beveiligingsinbreuken; na afloop van de bewaringstermijn worden de gegevens veilig vernietigd.

RICHTLIJN VOOR BEOORDELING:

Gegevens, met name gegevens die worden gebruikt met het oog op onweerlegbaarheid, ~~m~~40eten gedurende een afdoende periode worden bewaard, zoals voorgeschreven/toegestaan volgens het nationale recht teneinde gebruikt te kunnen worden in het kader van eventuele betwistingen of gerechtelijke procedures. Indien gegevens niet meer nodig zijn, moeten ze naar behoren worden vernietigd. Dit geldt voor alle media, in elektronische vorm of op papier, waarin dergelijke gegevens worden bijgehouden.

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.18 'Compliance' (zie ook A.18.1.3)

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van de verplichting tot administratie wordt het volgende uitgangspunt gehanteerd:

Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.4 Bijhouden van Administratie bij betrouwbaarheidsniveau Laag punt 1 en 2, geldt voor de betrouwbaarheidsniveaus Substantieel en Hoog dat:

a. gegevens zijn vastgelegd over de datum en tijd van uitgifte van het identificatiemiddel, het middel zelf en de identiteit van de gebruiker, zodanig dat de integriteit van de uitgifte eenduidig kan worden vastgesteld en gecontroleerd; deze gegevens moeten worden bewaard gedurende de bewaartermijn van de meest recente loggegevens van de log-ins met het middel. (Referentie hierbij is ISO/IEC 27002:2013 paragraaf 18.1.4);

b. activiteiten van personeel en beheerders worden gelogd voor de toegang tot het beheer op systemen die zijn betrokken bij de uitgifte van identificatiemiddelen en voor toegang tot en beheer op systemen die de in dit kader bedoelde authenticaties met de identificatiemiddelen faciliteren. Deze logging wordt bewaard gedurende dezelfde termijn als hetgeen is bepaald in onderdeel a (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7);

c. de toegang tot in elk geval de in de onderdelen a en b genoemde gegevens beperkt is tot personeel dat hiertoe een specifieke benoemde bevoegdheid heeft; de logging van de toegang door

dit personeel wordt behandeld zoals in onderdeel b is aangegeven (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7);

d. de gegevens ten behoeve van technische foutopsporing en technische foutcorrectie voor de werking van de dienst worden gelogd, waarbij geldt dat (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7);

1°. gegevens ten behoeve van foutopsporing en herstel over de authenticatieketen heen 14 dagen worden bewaard;

2°. er geen voorgeschreven bewaartermijn geldt indien de bedoelde gegevens geen persoonsgegevens zijn.

e. gewaarborgd is dat zodra een geschil, administratieve fout of een vermoeden van misbruik wordt aangemeld door een gebruiker, dienstverlener of andere aanbieder de relevante gegevens zoals bedoeld in onderdelen a en b worden veiliggesteld zolang het geschil bestaat, respectievelijk zolang het onderzoek door betrokkenen naar het geschil of misbruik loopt (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7);

f. de gegevens zoals bedoeld in onderdelen a en b zodanig worden vastgelegd dat de audittrail van de informatietransactie tussen een gebruiker en dienstverlener sluitend wordt; deze audittrail moet de reconstructie van een succesvolle authenticatie mogelijk maken, zodanig dat objectief is vast te stellen dat een uniek identificatiemiddel is gebruikt; Als onderdeel van de audittrail worden in elk geval worden de volgende gegevens vastgelegd, gedurende de termijn die in onderdeel a wordt genoemd (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7):

1°. alle beschikbare informatie ten aanzien van ondertekende berichten of een betrouwbare samenvatting van de ondertekende berichten en alle door hem ontvangen ondertekende berichten of betrouwbare samenvatting van berichten;

2°. het bewijs van de uitgifte en registratie van een identificatiemiddel;

3°. Beschikbare informatie ten aanzien van een berichtenuitwisseling ten behoeve van een poging tot inloggen van een gebruiker bij een dienstverlener wordt een referentie naar het gebruikte identificatiemiddel vastgelegd;

g. de integriteit van de gegevens gedurende de bewaartermijn zijn geborgd (Referentie ISO/IEC 27002:2013 paragraaf 12.4.2,12.4.3, 12.4.4 en 16.1.7).

2.4.5. Faciliteiten en personeel

Vereisten elementen

Ten aanzien van faciliteiten en personeel vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld. Onderstaande tabel bevat de vereisten inzake faciliteiten alsmede inzake personeelsleden en eventuele subcontractanten die taken uitvoeren die onder deze verordening vallen. Aan elk van de vereisten moet worden voldaan in verhouding tot het risiconiveau waarmee het desbetreffende betrouwbaarheidsniveau gepaard gaat.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er zijn procedures om te waarborgen dat personeelsleden en subcontractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen. 2. Er zijn voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures.

	3. De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten. 4. De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.
Substantieel	Zelfde als niveau laag.
Hoog	Zelfde als niveau laag.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.4.5 Faciliteiten en personeel

LAAG

42

1. Er zijn procedures om te waarborgen dat personeelsleden en subcontractanten voldoende zijn opgeleid en gekwalificeerd en dat zij ervaren zijn in de vaardigheden die vereist zijn voor de taken die zij vervullen.

RICHTLIJN VOOR BEOORDELING:

Indien personeelsleden over bewezen vaardigheden dienen te beschikken, behoort er een opleidingsprogramma te zijn dat waarborgt dat de personeelsleden hun vaardigheden kunnen aantonen en onderhouden.

Bijvoorbeeld
Goede praktijken voor personeelsleden die fysieke documenten inspecteren (bijv. paspoorten, identiteitskaarten) kunnen onder andere zijn:
Laag

- *Zich ervan bewust zijn dat er fraude wordt gepleegd met documenten.*
- *In staat zijn documenten nauwkeurig en consequent te controleren op afwijkingen zoals spelfouten, afwijkende lettertypen, ontbrekende pagina's en onregelmatigheden in de opmaak en uitlijning van documenten.*

Substantieel

- *Opgeleid zijn voor het met behulp van het nationaal erkende hoogwaardige opleidingsmateriaal opsporen van frauduleuze documentatie.*
- *In staat zijn te herkennen of er met documenten/laminering geknoeid is.*
- *In staat zijn basisdruktechnieken te herkennen.*

Hoog

- *Een goede praktijkkennis hebben van het ontwerp van documenten en de veiligheidskenmerken ervan.*

- *Door passende opleiding over kennis beschikken van de verschillende soorten watermerken, veiligheidsvezels en druktechnieken.*
- *In staat zijn vervalste en nagemaakt documenten door onderzoek te herkennen.*
- *In staat zijn doeltreffend gebruik te maken van referentiemateriaal.*

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van beheersmaatregelen in A.7 'Human resource security' (Beveiliging personeel) (zie met name A.7.2.2)

2. Er zijn voldoende personeelsleden en subcontractanten om de dienstverlening voldoende te waarborgen overeenkomstig het beleid en de procedures.

RICHTLIJN VOOR BEOORDELING:

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van beheersmaatregelen in A.12 'Operations security' (Beveiliging bedrijfsvoering) (zie ook A.12.1.2 'Capacity management' (Capaciteitsbeheer)) waar ook wordt ingegaan op de capaciteit van personeel

3. De voor de dienstverlening gebruikte faciliteiten staan onder permanente controle en worden permanent beschermd tegen schade door milieu-invloeden, ongeoorloofde toegang en andere factoren die de veiligheid van de dienst kunnen aantasten.

RICHTLIJN VOOR BEOORDELING:

Beveiligingskritische diensten, bijv. herroeping, behoren bestand te zijn tegen uitval en onderbrekingen. Dit behoort de dienst in voldoende mate te beschermen tegen storingen en natuurfenomenen zoals brand, overstromingen, storm en aardbevingen etc. die van invloed zijn op een enkele faciliteit.

Indien relevant behoren faciliteiten fysiek beveiligd te zijn door middel van geschikte sloten, toegangscontrolemechanismen en fysieke bewaking (bijv. CCTV). Hierin kan door de faciliteit als dienst worden voorzien; het is niet vereist dat de exploitant van de dienst deze functies uitvoert.

Er behoort een proces te zijn ingericht om te monitoren op toegang door onbevoegden en om de dienst te alarmeren indien er zich eventueel gebeurtenissen in verband met onbevoegden voordoen.

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van beheersmaatregelen in A.11 'Physical en environmental security' (Fysieke en omgevingsbeveiliging) en A.9 'Access control' (Toegangscontrole). De mechanismen voor het monitoren behoren ook in aanmerking te worden genomen in het kader van beheersmaatregel A.12 'Operations security' (Beveiliging bedrijfsvoering)

.

4. De voor de dienstverlening gebruikte faciliteiten zijn zodanig ingericht dat de toegang tot zones met persoonsgegevens, cryptografische gegevens en andere gevoelige informatie beperkt is tot bevoegde personeelsleden of subcontractanten.

RICHTLIJN VOOR BEOORDELING:

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.9 'Access control' (Toegangscontrole), waarvan het doel met name is de toegang tot informatie en informatieverwerkende faciliteiten te beperken, A.10 'Cryptography' (Cryptografie) en A.18.1.5 'Regulation of cryptographic controls' (Regeling van cryptografische beheersmaatregelen)

Nadere duiding voor de Nederlandse situatie

Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van faciliteiten en personeel wordt het volgende uitgangspunt gehanteerd:

1. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.5 Faciliteiten en Personeel bij betrouwbaarheidsniveau Laag punten 1 en 2, geldt voor het niveau Substantieel en Hoog dat is gewaarborgd dat het personeel dat identificaties uitvoert ten behoeve van de uitgifte van middelen en toegang tot gebruiksgegevens bij voortduring doeltreffend is opgeleid voor het beoordelen van de relevante identiteitsdocumenten en verifiëren van persoonskenmerken(Referentie ISO/IEC 27002 paragraaf 7.2):

a. de vaststelling van de echtheid van de identiteitsbewijzen gebeurt bij niveau Substantieel op een wijze die gelijk of gelijkwaardig is aan cliëntenonderzoek overeenkomstig hoofdstuk 2 van de Wet ter voorkoming van witwassen en financieren van terrorisme en bij niveau Hoog door personeel dat beschikt over de NVVB-opleiding voor balie-ambtenaren Burgerzaken die noodzakelijk is voor de uitgifte van paspoorten en rijbewijzen of een daarmee vergelijkbare opleiding;

Bij de vaststelling van de echtheid moet aantoonbaar kunnen worden maken dat deze vaststelling van de echtheid van de identiteitsbewijzen ook daadwerkelijk per uitgegeven middel is gebeurd. Bijvoorbeeld doordat bij de controle een bepaald formulier wordt ingevuld waarin sign-of op alle checks gebeurt

b. een controleproces is ingericht dat afwijkingen van het bepaalde met betrekking tot de deskundigheid signaleert en corrigeert.

2. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.5 Faciliteiten en Personeel bij betrouwbaarheidsniveau Laag punten 3 en 4 geldt voor de niveaus Substantieel en Hoog dat er waarborgt zijn dat het personeel handelt vanuit het bewustzijn dat persoonsgegevens worden verwerkt. Men beschikt over instructies voor de omgang met persoonsgegevens en kan aantonen dat het personeel daarmee bekend is gemaakt (Referentie ISO/IEC 27002 paragraaf 7.1, 7.2).

3. Bij de toepassing van de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.5 Faciliteiten en Personeel bij betrouwbaarheidsniveau Laag punten 3 en 4 geldt voor de niveaus Substantieel en Hoog dat maatregelen zijn getroffen om de integriteit van het betrokken personeel gedurende het dienstverband te waarborgen (Referentie ISO/IEC 27002 paragraaf 7.1, 7.2, 7.3, 6.1.2). De maatregelen betreffen in elk geval:

a. het bij indiensttreding van het personeel dat direct is betrokken bij de registratie en uitgifte van middelen of authenticatiedienstverlening toepassen van een vorm van screening op betrouwbaarheid, bijvoorbeeld een Verklaring Omtrent Gedrag (VOG). De bedoelde VOG betreft in elk geval de profielen 11, 12 en 13.

b. het mitigeren van integriteitsrisico's bij processen die essentieel zijn voor de uitgifte en het gebruik van identificatiemiddelen, waaronder in ieder geval de volgende risico's:

1°. het risico dat een middel wordt uitgegeven op identiteit van een fictieve natuurlijke persoon;

2°. het risico dat een middel wordt uitgegeven op de identiteit van een bestaande natuurlijke persoon zonder dat deze natuurlijke persoon daarom heeft verzocht;

3°. het risico dat een authenticatie wordt uitgevoerd zonder dat de gebruiker de authenticatie heeft geïnitieerd;

4°. het risico op onrechtmatige toegang en misbruik van persoonsidentificatiegegevens en bijbehorende gegevens over uitgevoerde authenticaties;

4. Het beheer van de hiervoor bedoelde maatregelen zijn opgenomen in het managementsysteem voor het beheer van informatiebeveiliging.

Bedoeld zijn hier in elk geval risico's in processen die bij optreden kunnen leiden tot uitgifte van middelen met het oog op misbruik, het uitvoeren van valse authenticaties en onrechtmatige toegang tot persoonsgegevens.

2.4.6. Technische controles

Vereisten elementen

Ten aanzien van technische controles vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd. 2. De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen. 3. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen. 4. Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken. 5. Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.
Substantieel	Zelfde als niveau laag, plus: Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.
Hoog	Zelfde als niveau substantieel.

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

2.4.6 Technische controles

LAAG

1. Er is voorzien in proportionele controles ter beheersing van de risico's voor de veiligheid van de diensten, waarbij de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkte informatie worden beschermd.

RICHTLIJN VOOR BEOORDELING:

Het is belangrijk de beoordeling van beschermingseisen van vertrouwelijkheid en integriteit te scheiden. Waar bescherming van integriteit (of authenticiteit) in principe aan de hand van het betrouwbaarheidsniveau wordt bepaald, moet er bij de vertrouwelijkheid van persoonsgerelateerde gegevens rekening worden gehouden met de soort gegevens en eventuele wettelijke eisen aan de gegevensbescherming.

De vertrouwelijkheid van persoonsgegevens moet worden beschermd, er behoren controles te zijn ingesteld op basis van een beoordeling aan de hand van een beoordeling op risicobasis volgens het geselecteerde beheerssysteem voor informatiebeveiliging. Deze moeten bepaalde gebieden afdekken, zoals bescherming bieden tegen hacken, misbruik, foutief gebruik, denial-of-service- (DoS) en distributed-denial-of-service- (DDoS) aanvallen.

De vertrouwelijkheid en authenticiteit/integriteit van persoonsgegevens tijdens grensoverschrijdende verzending wordt afgedekt door de Uitvoeringshandeling aangaande het Interoperabiliteitskader.

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.10 'Cryptography' (Cryptografie), A.12 'Operations security' (Beveiliging bedrijfsvoering), (in verband met beschikbaarheid) A.17 'Information security aspects of business continuity management ' (Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer) en A.18.1.5 'Regulation of cryptographic controls' (Regeling van cryptografische beheersmaatregelen)

2. De elektronische communicatiekanalen die voor de uitwisseling van persoonsgegevens en gevoelige gegevens worden gebruikt, worden beschermd tegen afluisteren, manipuleren en herafspelen

.

RICHTLIJN VOOR BEOORDELING:

Er behoort aandacht te worden besteed aan het feit dat er zich communicatiekanalen kunnen voordoen tussen verschillende partijen die betrokken zijn binnen een identificatiestelsel, bijv. tussen de eigenaar van het identificatiemiddel en een dienst of tussen gemeente en fabrikant.

Een mogelijkheid voor technische controles voor communicatiekanalen is het gebruik van technische richtsnoeren die zijn uitgegeven door een instantie die eisen geeft over cryptografie en de te gebruiken beveiligingsmaatregelen. Dit wordt meestal bereikt met behulp van cryptografische protocollen met beschreven verificatiestappen.

Eisen voor communicatiekanalen tussen knooppunten van het eIDAS-interoperabiliteitskader staan vermeld in de technische eIDAS-specificaties voor het kader.

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.10 'Cryptography' (Cryptografie), A.13 'Communications security' (Communicatiebeveiliging) en A.18.1.5 'Regulation of cryptographic controls' (Regeling van cryptografische beheersmaatregelen), die verwijzingen naar de bovenvermelde technische richtsnoeren kunnen bevatten

.

3. De toegang tot gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, is beperkt tot de uitoefening van taken en toepassingen waarvoor de toegang strikt noodzakelijk is. Er wordt op toegezien dat dergelijk materiaal niet permanent in onversleutelde staat wordt opgeslagen.

RICHTLIJN VOOR BEOORDELING:

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.9 'Access control' (Toegangscontrole) en A.10 'Cryptography' (Cryptografie).'

4. Er zijn procedures die waarborgen dat de veiligheid duurzaam wordt gehandhaafd en dat een respons mogelijk is op wijzigingen van het risiconiveau, incidenten en veiligheidsinbreuken.

RICHTLIJN VOOR BEOORDELING:

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.14 'Security in development and support processes' (Beveiliging binnen ontwikkel- en ondersteuningsprocessen) en A.16 'Information security incident management' (Informatiebeveiligingsincidentbeheer)

5. Alle media die persoonsgegevens, cryptografische informatie of andere gevoelige informatie bevatten, worden veilig opgeslagen, vervoerd en verwijderd.

RICHTLIJN VOOR BEOORDELING:

Voor een beheerssysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen in A.8 'Asset management' (Beheer van bedrijfsmiddelen)

SUBSTANTIEEL

Niveau laag, plus:

Gevoelig cryptografisch materiaal dat voor de uitgifte van elektronische identificatiemiddelen en voor authenticatie wordt gebruikt, wordt beschermd tegen ongeoorloofde manipulatie.

RICHTLIJN VOOR BEOORDELING:

Gevoelig cryptografisch materiaal verwijst naar sleutelmaterialen die worden gebruikt om elektronische identificatiemiddelen uit te geven, gebruikers te authenticeren en verklaringen uit te

geven (indien van toepassing). Bescherming van deze soorten cryptografische sleutels is van het hoogste belang voor de beveiliging van een stelsel voor elektronische identificatie.

Mechanismen die bescherming bieden tegen ongeoorloofde manipulatie hebben als doel pogingen tot het blootleggen, manipuleren of onjuist gebruiken van het cryptografische sleutelmateriaal tijdens de gehele levenscyclus ervan tegen te gaan. Dit wordt bereikt door zowel fysieke als logische beveiligingscontroles en -beheersmaatregelen voor de bescherming van deze sleutels te implementeren.

Het is gebruikelijk dat deze beveiligingscontroles en -beheersmaatregelen in het kader van een hardwarebeveiligingsmodule worden geïmplementeerd. Dergelijke producten die aan dit doel voldoen, behoren transparantie te bieden binnen de geïmplementeerde beveiligingsmechanismen en te voldoen aan de hoogste kwaliteits- en beveiligingsnormen. Veiligheidscertificering kan begeleidend bewijs leveren en is een goede praktijk voor het beoordelen van de kwaliteit van hardwarebeveiligingsmodules, zoals certificering volgens Criteria Recognition Arrangement (CCRA) en/of de Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA), of FIPS-140. Producten behoren bij een vertrouwde leverancier te worden betrokken en dusdanig in bedrijf te worden gesteld dat de doorlopende controle in de gehele toeleveringsketen (Chain of Custody) van de eenheden, vanaf de productie van de eenheid tot en met het punt waar de hardwarebeveiligingsmodule in productie wordt genomen, wordt gewaarborgd.

Voor een beheersysteem voor informatiebeveiliging volgens ISO/IEC 27001:2013 wordt deze eis afgedekt in het kader van de beheersmaatregelen A.10 'Cryptography'(Cryptografie) en A.11 'Physical and environmental security' (Fysieke en omgevingsbeveiliging)

Nadere duiding voor de Nederlandse situatie

2.4.7. Compliance en audit

Vereisten elementen

Ten aanzien van Compliance en audit vereist de eIDAS-uitvoeringsverordening 1502 dat de volgende elementen worden ingevuld.

Betrouwbaarheidsniveau	Vereiste elementen
Laag	Er vinden periodieke interne audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.
Substantieel	Er vinden periodieke onafhankelijke interne of externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te waarborgen.
Hoog	1. Er vinden periodieke onafhankelijke externe audits plaats van alle onderdelen die voor de verlening van de aangeboden diensten relevant zijn, teneinde de naleving van het desbetreffende beleid te

	waarborgen. 2. Indien een stelsel wordt beheerd door een overheidsinstantie, vinden audits plaats overeenkomstig het nationaal recht.

(1) Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling

Nadere duiding op basis van de Guidance for the application of the levels of assurance which support the eIDAS Regulation

Nadere duiding voor de Nederlandse situatie

Certificering en Keuring en controle

In de set van eisen eID wordt in de artikelen 7 (certificering) en 9 (Keuring en controle) opgenomen hoe de naleving op de set van eisen eID , met inbegrip van de eIDAS eisen, is vormgegeven en wordt gecontroleerd. Om te worden toegelaten dienen partijen zich hieraan te conformeren.

Beoordeling van de weerstand tegen een specifiek aanvalspotentieel

Voor het overzicht worden hieronder eerst de corresponderende vereiste elementen uit de eIDAS uitvoeringsverordening 1502 (paragraaf 2.4.7. Compliance en audit) opgenomen. 49
Bij de controle of wordt voldaan aan de eIDAS-normen ten aanzien van de beoordeling van de weerstand tegen een specifiek aanvalspotentieel wordt het volgende uitgangspunt gehanteerd:

In aanvulling op de eIDAS uitvoeringsverordening 2015/1502 paragraaf 2.4.7 Compliance en Audit bij betrouwbaarheidsniveau Substantieel en Hoog, paragraaf 2.2.1 bij Hoog punt 1, paragraaf 2.3.1 bij Substantieel punt 2 en bij Hoog geldt voor de niveaus Substantieel en Hoog dat:

a. De technische beoordeling van de weerstand tegen een 'gemiddeld' (moderate) respectievelijk hoog (high) aanvalspotentieel van een identificatiemiddel met bijbehorend authenticatiemechanisme zoals bedoeld in artikel 8 Kenmerken en ontwerp van elektronische identificatiemiddelen en artikel 12 Authenticatiemechanisme moet in elk geval de volgende aspecten adresseren:

1° ten behoeve van de technische conformiteitsbeoordeling worden alle aan het identificatiemiddel en authenticatiemechanisme aangebrachte wijzigingen geadministreerd, met daarbij een analyse van de impact op de conformiteit aan de gestelde eisen;

2°. de conformiteitsbeoordeling maakt onderscheid tussen verschillende typen onderzoek, te weten:

- een initieel onderzoek, te weten een eerste beoordeling over de volledige scope van het object van onderzoek op basis van de gestelde eisen;
- een herhalingsonderzoek, indien wijzigingen aan het object van onderzoek zijn uitgevoerd die van invloed (kunnen) zijn op de conformiteit aan de gestelde eisen. De scope is beperkt tot de wijzigingen aan het object van onderzoek;
- een heronderzoek, na elke drie jaar over de volledige scope van het object van onderzoek gemeten na afgifte van rapportage over het initiële onderzoek respectievelijk de rapportage over het heronderzoek;

b. de conformiteitsbeoordelaar die de conformiteitsbeoordeling uitvoert in elk geval voldoet aan de volgende vereisten:

1°. de conformiteitsbeoordelaar heeft aantoonbaar ruime ervaring met het uitvoeren van technische beoordelingsopdrachten van identificatiemiddelen of vergelijkbare objecten van onderzoek;

2°. de conformiteitsbeoordelaar zet voor de opdracht personeel in met ruime ervaring en dat beschikt over de voor de beoordeling benodigde competenties;

3°. de conformiteitsbeoordelaar is in zijn oordeelsvorming geheel onafhankelijk van de aanbieder;

4°. de conformiteitsbeoordelaar beschikt over een intern kwaliteitssysteem en/of vaktechnische richtlijnen en procedures voor het uitvoeren van beoordelingsopdrachten, met inbegrip van registratie van ondersteunend bewijs, rapportering aan opdrachtgever en aan derden en – waar nodig - interne (peer) review;

5°. de conformiteitsbeoordelaar beschikt over een bedrijfs- of beroepsaansprakelijkheidsverzekering;

6°. Indien de conformiteitsbeoordelaar beschikt over een testlaboratorium ingevolge ISO 17025 voor de scope "testing of information technology products" dat wordt vermoed aan sub c onder ii t/m iii.

c. in de overeenkomst met de conformiteitsbeoordelaar wordt gewaarborgd dat:

1°. de auditor zoals bedoeld in artikel 16 op zijn verzoek inzage kan krijgen in het dossier waarin het ondersteunend bewijs bij het rapport is vastgelegd;

2°. de door de minister aangewezen toezichthoudende ambtenaren op elk gewenst moment, binnen 7 jaar na het uitbrengen van het beoordelingsrapport bij de conformiteitsbeoordelaar inzage kan vorderen in het rapportage en in het bijbehorende dossier waarin het ondersteunend bewijs is vastgelegd.

d. Opdracht wordt verleend indien de conformiteitsbeoordelaar voorafgaand aan de opdrachtverstrekking aan de aanbieder een formele verklaring afgeeft waarin hij conformiteit verklaart aan sub b en sub c op het moment van opdrachtverstrekking en gedurende de conformiteitsbeoordeling en waarin de juistheid van de verklaring is onderbouwd en aannemelijk is gemaakt.

f. het onderzoek van de conformiteitsbeoordelaar zodanig wordt gepland en uitgevoerd dat een zogeheten 'redelijke mate van zekerheid' kan worden verkregen dat het object van onderzoek op het in de rapportage aangegeven moment aan de gestelde eisen voldoet.

g. de rapportage van de conformiteitsbeoordelaar minimaal de volgende onderdelen bevat:

1°. de doelstelling van de opdracht, een beschrijving van het object van onderzoek (uniek identificerend, met datum en versienummer), de eisen op basis waarvan het object van onderzoek is beoordeeld en het plan van aanpak met de gevolgde stappen en de gehanteerde onderzoeksmethoden en aanvalstechnieken;

2°. het eindoordeel over de mate waarin het object op het aangegeven moment aan de gestelde eisen voldoet, met onderbouwing;

3°. belangrijkste bevindingen en aanbevelingen;

4°. inzicht in de ontwikkelingen en maatregelen sinds de vorige toets;

5°. detailbevindingen, met vermelding van referenties naar het geregistreerde bewijs over de conformiteit aan de betreffende eis.

Het beoordelen van de weerstand tegen het bedoelde aanvalspotentieel is zeer technisch specialistisch. Doorgaans zal de bedoelde geaccrediteerde certificerende instelling die een aanbieder beoordeelt steunen op rapportages van technische tests die door gekwalificeerde specialisten in opdracht van de aanbieder zijn uitgevoerd. De geaccrediteerde certificerende instelling is daarbij wel verantwoordelijk voor de beoordeling of de rapporten van technische tests van voldoende kwaliteit zijn om geaccepteerd te kunnen worden conform de beroepsstandaarden voor IT auditors. De eisen in dit artikel zijn opgenomen ten behoeve van het creëren van een solide basis voor dat oordeel door de certificerende instelling.

Controle op de set van eisen eID

De controle op de voorgaande paragrafen is van belang voor de vaststelling of identificatiemiddelen zijn te kwalificeren zijn als eIDAS betrouwbaarheidsniveau substantieel en hoog. Voor toelating van een middel is het van belang dat, nadat is vastgesteld dat een middel als zodanig te kwalificeren valt, tevens wordt voldaan aan de Nederlandse set van eisen waarin, los van de eIDAS eisen, de Nederlandse eisen zijn vastgelegd als gevolg van Nederlandse inrichting- en beleidskeuzes. De Nederlandse set van eisen – die thans wordt voorbereid - beoogt op de voorgeschreven punten geen ruimte te laten. Controle daarop kan plaatsvinden door feitelijke vaststelling of aan de eisen is voldaan. Daar waar het eisen betreft die de juiste aansluiting op en de samenwerking met randvoorwaardelijke voorzieningen beogen te borgen, kan conformiteit worden vastgesteld aan de hand van de constatering dat dit feitelijk werkend is ingericht.

Verklaring van conformiteit
De auditor betrekt in zijn evaluatie de geconstateerde afwijkingen van de normen en eveneens eventuele andere aangetroffen afwijkingen. Materiële afwijkingen brengt de auditor tot uitdrukking in de controleverklaring. Niet-materiële tekortkomingen neemt de auditor op in een rapport van bevindingen gericht aan de opdrachtgever en aan de Minister van BZK.
In de verklaring van de auditor die met toepassing van dit protocol het getoetst aan de genoemde normen wordt verwezen naar dit controleprotocol en wordt vermeld aan de normen voor welk betrouwbaarheidsniveau is getoetst.