UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE

van 8 september 2015

tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 8, lid 3,

Overwegende hetgeen volgt:

(1) In artikel 8 van Verordening (EU) nr. 910/2014 wordt bepaald dat een stelsel voor elektronische identificatie dat is aangemeld krachtens artikel 9, lid 1, de betrouwbaarheidsniveaus laag, substantieel en hoog omschrijft voor op grond van dat stelsel uitgegeven elektronische identificatiemiddelen.

(2) De minimale technische specificaties, normen en procedures dienen te worden vastgesteld om een uniforme interpretatie te waarborgen van de details van de betrouwbaarheidsniveaus en de interoperabiliteit te verzekeren wanneer de nationale betrouwbaarheidsniveaus van aangemelde stelsels voor elektronische identificatie worden gerelateerd aan de betrouwbaarheidsniveaus volgens artikel 8, zoals bepaald in artikel 12, lid 4, onder b), van Verordening (EU) nr. 910/2014.

(3) Voor het vaststellen van de specificaties en procedures die in deze uitvoeringshandeling zijn opgenomen, is rekening gehouden met de internationale norm ISO/IEC 29115, de belangrijkste internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Verordening (EU) nr. 910/2014 verschilt echter inhoudelijk van die internationale norm, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identiteitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen. In de bijlage, die weliswaar op deze internationale norm is gestoeld, dient derhalve niet te worden verwezen naar enige specifieke inhoud van ISO/IEC 29115.

(4) Deze verordening is tot stand gekomen volgens een resultaatgestuurde aanpak, omdat die het meest geschikt is; hetzelfde geldt voor de definities van termen en begrippen. Daarbij is rekening gehouden met de doelstelling van Verordening (EU) nr. 910/2014 met betrekking tot de betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Bij het vaststellen van de specificaties en procedures in deze uitvoeringshandeling moet daarom terdege rekening worden gehouden met het grootschalige proefproject STORK, inclusief de in dat verband ontwikkelde specificaties, alsmede de definities en begrippen in ISO/IEC 29115.

(5) Afhankelijk van de context waarin verificatie van een aspect van het bewijs van de identiteit moet plaatsvinden, kunnen gezaghebbende bronnen in allerlei vormen voorkomen, zoals registers, documenten, instanties en dergelijke. In de verschillende lidstaten kunnen, zelfs in vergelijkbare contexten, verschillende gezaghebbende bronnen bestaan.

(6) De vereisten voor het bewijs en de verificatie van de identiteit dienen verschillende systemen en praktijken in aanmerking te nemen, waarbij een voldoende hoog betrouwbaarheidsniveau moet worden gewaarborgd om het noodzakelijke vertrouwen tot stand te brengen. Procedures die eerder werden gebruikt voor andere doeleinden dan de afgifte van elektronische identificatiemiddelen, mogen dan ook slechts worden aanvaard indien is bevestigd dat die procedures voldoen aan de eisen die voor het overeenkomstige betrouwbaarheidsniveau zijn vastgesteld.

([1]) PB L 257 van 28.8.2014, blz. 73.

(7) Er wordt doorgaans gebruikgemaakt van authenticatiefactoren zoals gedeelde geheime sleutels, fysieke hulpmiddelen en fysieke attributen. Om het authenticatieproces beter te beveiligen, is het echter aan te bevelen om een groter aantal authenticatiefactoren te gebruiken, en dan met name authenticatiefactoren die tot verschillende categorieën behoren.

(8) Deze verordening mag geen afbreuk doen aan de vertegenwoordigingsrechten van rechtspersonen. In de bijlage dienen echter vereisten te worden opgenomen inzake de koppeling tussen de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen.

(9) Het belang van informatiebeveiliging en servicemanagementsystemen dient te worden erkend, evenals het belang van het gebruik van erkende methoden en toepassing van de beginselen die in normen zoals ISO/IEC 27000 en de normenreeks ISO/IEC 20000 zijn vervat.

(10) Tevens moet rekening worden gehouden met goede praktijken van de lidstaten inzake betrouwbaarheidsniveaus.

(11) Certificatie van de IT-beveiliging op basis van internationale normen is een belangrijk instrument voor de controle of producten voldoen aan de beveiligingseisen van deze uitvoeringshandeling.

(12) Het in artikel 48 van Verordening (EU) nr. 910/2014 bedoelde comité heeft binnen de door zijn voorzitter vastgestelde termijn geen advies uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

1. Voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, worden de betrouwbaarheidsniveaus laag, substantieel en hoog bepaald onder verwijzing naar de specificaties en procedures in de bijlage.

2. De specificaties en procedures in de bijlage worden gebruikt voor het bepalen van het betrouwbaarheidsniveau voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, door de betrouwbaarheid en de kwaliteit te bepalen van de volgende elementen:

a) inschrijving, zoals bedoeld in punt 2.1 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder a), van Verordening (EU) nr. 910/2014;

b) beheer van elektronische identificatiemiddelen, zoals bedoeld in punt 2.2 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder b) en f), van Verordening (EU) nr. 910/2014;

c) authenticatie, zoals bedoeld in punt 2.3 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder c), van Verordening (EU) nr. 910/2014;

d) beheer en organisatie, zoals bedoeld in punt 2.4 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder d) en e), van Verordening (EU) nr. 910/2014.

3. Indien het elektronische identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, voldoet aan een vereiste dat voor een hoger betrouwbaarheidsniveau is vermeld, wordt het geacht ook te voldoen aan het overeenkomstige vereiste voor een lager betrouwbaarheidsniveau.

4. Tenzij in het desbetreffende deel van de bijlage anders is aangegeven, kan een elektronisch identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, slechts aan het opgegeven betrouwbaarheidsniveau voldoen indien is voldaan aan alle elementen die in de bijlage voor dat betrouwbaarheidsniveau zijn vermeld.

Artikel 2

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

Voor de Commissie

De voorzitter

Jean-Claude JUNCKER

BIJLAGE

Technische specificaties en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog betreffende op grond van een aangemeld stelsel voor elektronische identificatie uitgegeven elektronische identificatiemiddelen

1. Definities

Voor de toepassing van deze bijlage wordt verstaan onder:

1. „gezaghebbende bron": elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond;

2. „authenticatiefactor": een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de volgende categorieën valt:

   a) „op bezit gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is;

   b) „op kennis gebaseerde authenticatiefactor": een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;

   c) „inherente authenticatiefactor": een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;

3. „dynamische authenticatie": een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;

4. „beheerssysteem voor informatiebeveiliging": een geheel van processen en procedures die zijn ontworpen om de informatieveiligheidsrisico's tot een aanvaardbaar niveau te beperken.

2. Technische specificaties en procedures

Aan de hand van de in deze bijlage 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.

2.1. *Inschrijving*

2.1.1. Aanvraag en registratie

Betrouwbaarheids-niveau	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.

2.1.2. Bewijs en verificatie van identiteit (natuurlijke persoon)

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.

Betrouwbaarheidsniveau	Vereiste elementen
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; 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.

([1]) Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

2.1.3. Bewijs en verificatie van identiteit (rechtspersoon)

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan.

Betrouwbaarheidsniveau	Vereiste elementen
	2. Het bewijsstuk lijkt geldig en kan worden verondersteld echt te zijn dan wel volgens een gezaghebbende bron te bestaan, indien de rechtspersoon op vrijwillige basis in de gezaghebbende bron is opgenomen op basis van een regeling tussen de rechtspersoon en de gezaghebbende bron. 3. De rechtspersoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat zij als die rechtspersoon optreedt.
Substantieel	Niveau laag plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam, de rechtsvorm en (indien van toepassing) het registratienummer van de rechtspersoon; en het bewijsstuk wordt gecontroleerd om te bepalen of het echt is dan wel volgens een gezaghebbende bron bestaat, indien de rechtspersoon in de gezaghebbende bron is opgenomen omdat dat voor de rechtspersoon verplicht is om in de betrokken sector actief te mogen zijn; en er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de rechtspersoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn. of 2. Indien de 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 2.1.3 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 of een daaraan gelijkwaardige instantie. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het 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	Niveau substantieel plus een van de onder de punten 1 tot en met 3 vermelde alternatieven. 1. De opgegeven identiteit van de rechtspersoon wordt aangetoond aan de hand van een bewijsstuk dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, inclusief de naam en de rechtsvorm van de rechtspersoon en ten minste één in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt; en het bewijs is gecontroleerd om de geldigheid ervan volgens een gezaghebbende bron te bepalen. of

Betrouwbaarheidsniveau	Vereiste elementen
	2. Indien de 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 2.1.3 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. of 3. Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het 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.

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

Indien van toepassing gelden de volgende voorwaarden voor de koppeling tussen het elektronische identificatiemiddel van een natuurlijke persoon en het elektronische identificatiemiddel van een rechtspersoon:

1. Het moet mogelijk zijn een koppeling te schorsen en/of te herroepen. De verschillende koppelingsstadia (o.a. activering, schorsing, hernieuwing, herroeping) worden beheerd volgens op nationaal niveau erkende procedures.

2. De natuurlijke persoon wiens elektronische identificatiemiddel is gekoppeld aan het elektronische identificatiemiddel van de rechtspersoon kan volgens op nationaal niveau erkende procedures de uitoefening van de koppeling delegeren aan een andere natuurlijke persoon. De delegerende natuurlijke persoon blijft echter aansprakelijk.

3. De koppeling wordt op de volgende wijze uitgevoerd:

Betrouwbaarheidsniveau	Vereiste elementen
Laag	1. Er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau laag of hoger. 2. De koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures. 3. De natuurlijke persoon bevindt zich volgens een gezaghebbende bron niet in een toestand die verhindert dat hij namens die rechtspersoon optreedt.
Substantieel	Punt 3 van niveau laag, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau substantieel of hoog;

Betrouwbaarheidsniveau	Vereiste elementen
	2. de koppeling is tot stand gebracht volgens op nationaal niveau erkende procedures, wat ertoe heeft geleid dat de koppeling in een gezaghebbende bron is geregistreerd; 3. de koppeling is geverifieerd op basis van informatie uit een gezaghebbende bron.
Hoog	Punt 3 van niveau laag en punt 2 van niveau substantieel, plus: 1. er is geverifieerd dat het bewijs van de identiteit van de natuurlijke persoon die namens de rechtspersoon optreedt, heeft plaatsgevonden op het niveau hoog; 2. de koppeling is geverifieerd op basis van een in een nationale context gebruikte unieke identificatiecode die de rechtspersoon vertegenwoordigt, en op basis van uit een gezaghebbende bron afkomstige informatie die op unieke wijze een natuurlijke persoon vertegenwoordigt.

2.2. *Beheer van elektronische identificatiemiddelen*

2.2.1. Kenmerken en ontwerp van elektronische identificatiemiddelen

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.

2.2.2. Uitgifte, uitreiking en activering

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.

2.2.3. Schorsing, herroeping en reactivering

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.

2.2.4. Verlenging en vervanging

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.

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.

2.3.1. Authenticatiemechanisme

In 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.

Betrouwbaarheidsniveau	Vereiste elementen
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.

2.4. *Beheer en organisatie*

Alle deelnemers die een dienst verlenen op het gebied van elektronische identificatie in een grensoverschrijdende context (hierna „aanbieders" genoemd) 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

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.

2.4.2. Gepubliceerde mededelingen en informatie voor de gebruikers

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.

2.4.3. Beheer van informatiebeveiliging

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.

2.4.4. Bijhouden van de administratie

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.

2.4.5. Faciliteiten en personeel

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.

2.4.6. Technische controles

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.

2.4.7. Compliance en audit

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.

Betrouwbaarheids-niveau	Vereiste elementen
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.