Publicatieblad
van de Europese Unie

NL
L-serie

2024/2981

4.12.2024

UITVOERINGSVERORDENING (EU) 2024/2981 VAN DE COMMISSIE

van 28 november 2024

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de certificering van Europese portemonnees voor digitale identiteit

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 5 quater, lid 6,

Overwegende hetgeen volgt:

(1) Overeenkomstig artikel 5 quater van Verordening (EU) nr. 910/2014 moet de certificering van Europese portemonnees voor digitale identiteit ("portemonnees") gebeuren in overeenstemming met de vereisten op het gebied van functionaliteit, cyberbeveiliging en gegevensbescherming, om een hoog niveau van beveiliging en vertrouwen in de portemonnees te waarborgen. Die certificeringsvereisten moeten in alle lidstaten worden geharmoniseerd om versnippering van de markt te voorkomen en een robuust kader tot stand te brengen.

(2) Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([2]) en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([3]) zijn van toepassing op alle activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van deze verordening.

(3) De Commissie voert regelmatig beoordelingen uit van nieuwe technologieën, praktijken, normen of technische specificaties. Om het hoogste niveau van harmonisatie tussen de lidstaten te waarborgen voor de ontwikkeling en de certificering van de portemonnees, berusten de in deze verordening vastgestelde technische specificaties op de werkzaamheden die zijn verricht op basis van Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit ([4]), en met name de architectuur en het referentiekader die er deel van uitmaken. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([5]) moet de Commissie deze uitvoeringsverordening in voorkomend geval evalueren en actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen, de architectuur en het referentiekader en om de beste praktijken op de interne markt te volgen.

(4) Om de conformiteit met de cyberbeveiligingsvereisten in het certificeringskader te bevestigen, moet de certificering van portemonnee-oplossingen verwijzen naar, voor zover beschikbaar en relevant, Europese regelingen voor cyberbeveiligingscertificering die zijn vastgesteld op grond van Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([6]). Bij gebrek aan dergelijke regelingen, of wanneer zij gedeeltelijk betrekking hebben op cyberbeveiligingsvereisten, worden in deze verordening de algemene vereisten vastgesteld die van toepassing zijn op nationale certificeringsregelingen, die betrekking hebben op de vereisten op het gebied van functionaliteit, cyberbeveiliging en gegevensbescherming.

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) PB L 210 van 14.6.2021, blz. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([5]) Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (PB L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([6]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Overeenkomstig artikel 5 bis, lid 11, van Verordening (EU) nr. 910/2014 moeten de portemonnees worden gecertificeerd met het betrouwbaarheidsniveau "hoog" in de zin van Verordening (EU) nr. 910/2014 en Uitvoeringsverordening (EU) 2015/1502 van de Commissie ([7]). Dit betrouwbaarheidsniveau moet door de portemonnee-oplossing als geheel worden bereikt. Op grond van deze verordening kunnen sommige componenten van de portemonnee-oplossing op een lager betrouwbaarheidsniveau worden gecertificeerd, mits dit naar behoren wordt gemotiveerd en onverminderd het betrouwbaarheidsniveau "hoog" dat door de oplossing als geheel wordt bereikt.

(6) In alle nationale certificeringsregelingen moet een regelinghouder worden aangewezen die verantwoordelijk is voor de ontwikkeling en het onderhoud van de certificeringsregeling. De regelinghouder kan een conformiteitsbeoordelingsinstantie, een overheidsinstantie of -autoriteit, een beroepsvereniging, een groep conformiteitsbeoordelingsinstanties of een andere passende instantie zijn, en kan een andere instantie zijn dan de instantie die de nationale certificeringsregeling uitvoert.

(7) Het voorwerp van de certificering moet de softwarecomponenten van de portemonnee-oplossing, zoals de portemonnee-instantie, omvatten. Hoewel ze onderdeel van de operationele omgeving vormen, mogen het beveiligd cryptografisch middel voor portemonnees, het cryptografische beveiligingsapparaat voor portemonnees en de platforms waarop deze softwarecomponenten worden uitgevoerd, alleen in het voorwerp van de certificering worden opgenomen als ze door de portemonnee-oplossing worden geleverd. In andere gevallen, en met name wanneer deze apparaten en platforms door eindgebruikers worden geleverd, moeten aanbieders veronderstellingen maken over de operationele omgeving van de portemonnee-oplossing, met inbegrip van deze apparaten en platforms, en maatregelen nemen om te bevestigen dat deze veronderstellingen in de praktijk worden geverifieerd. Om de bescherming van de kritieke activa te waarborgen door middel van hardware en systeemsoftware die wordt gebruikt voor het beheer en de bescherming van cryptografische sleutels die door het cryptografische beveiligingsapparaat voor portemonnees zijn gecreëerd, opgeslagen of verwerkt, moet het cryptografische beveiligingsapparaat voor portemonnees voldoen aan hoge certificeringsnormen zoals weergegeven in internationale normen zoals de in Uitvoeringsverordening (EU) 2024/482 van de Commissie ([8]) bepaalde gemeenschappelijke criteria voor de evaluatie van de beveiliging van informatietechnologie ("EUCC", de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling), door de evaluatie en geavanceerde methodische kwetsbaarheidsanalyses van EAL4, vergelijkbaar met AVA_VAN.5. Deze certificeringsnormen moeten uiterlijk worden gebruikt op het moment dat de conformiteit van portemonnees wordt gecertificeerd op grond van een Europese regeling voor cyberbeveiligingscertificering die is vastgesteld op grond van Verordening (EU) 2019/881.

(8) Volledig mobiele, veilige en gebruiksvriendelijke portemonnees worden ondersteund door de beschikbaarheid van gestandaardiseerde en gecertificeerde manipulatiebestendige oplossingen, zoals ingebedde beveiligde elementen, externe apparaten zoals smartcards, of ingebouwde SIM-platforms in mobiele apparaten. De tijdige toegang tot ingebedde beveiligde elementen voor nationale eID-middelen portemonnees moet worden gewaarborgd, om de inspanningen van de lidstaten op dit gebied te coördineren. De bij artikel 46 sexies, lid 1, van Verordening (EU) nr. 910/2014 opgerichte Europese samenwerkingsgroep voor digitale identiteit (de "samenwerkingsgroep") moet derhalve een specifieke subgroep voor dat doel oprichten. In overleg met belanghebbende partijen moet die subgroep overeenstemming bereiken over een gemeenschappelijke routekaart voor toegang tot de ingebedde beveiligde elementen die de Commissie voor het herbeoordelingsrapport van Verordening (EU) nr. 910/2014 in overweging moet nemen. Met het oog op de opname van de portemonnee op nationaal niveau moet de Commissie, samen met de lidstaten, bovendien een handboek voor use cases ontwikkelen en bijgewerkt houden, als onderdeel van de architectuur en het referentiekader.

(9) Het voorwerp van de certificering van nationale certificeringsregelingen moet ook de processen omvatten die worden gebruikt om de portemonnee-oplossing aan te bieden en te laten functioneren, zelfs als de definitie of uitvoering van die processen aan derden wordt uitbesteed. Om aan te tonen dat de processen aan de vereisten van de regelingen voldoen, mag de zekerheidsinformatie als bewijs worden gebruikt, mits een afhankelijkheidsanalyse wordt gebruikt om te bepalen of de zekerheidsinformatie toereikend is. Zekerheidsinformatie bestaat in veel verschillende vormen, waaronder verslagen en certificaten van overeenstemming, die privé, nationaal, Europees of internationaal kunnen zijn, op basis van normen of technische specificaties. Het doel van de afhankelijkheidsanalyse is de kwaliteit van de beschikbare zekerheidsinformatie over de componenten van een portemonnee te beoordelen.

([7]) 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 (PB L 235 van 9.9.2015, blz. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) (PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Volgens de daartoe vastgestelde procedures moet de samenwerkingsgroep adviezen en aanbevelingen kunnen uitbrengen over de bij haar ingediende ontwerpen van nationale certificeringsregelingen. Deze nationale certificeringsregelingen moeten specifiek zijn voor de architectuur van de portemonnee en er moeten specifieke profielen zijn voor elke afzonderlijke ondersteunde architectuur.

(11) Om te zorgen voor een gemeenschappelijke interpretatie en een geharmoniseerde aanpak van de beoordeling van de meest kritieke risico's die van invloed kunnen zijn op de levering en werking van portemonnees, moet een register van risico's en bedreigingen worden bijgehouden waarmee rekening moet worden gehouden bij het ontwerpen van portemonnee-oplossingen, ongeacht de specifieke architectuur ervan. Bij het vaststellen van de risico's die in het register moeten worden opgenomen, moet rekening worden gehouden met de in Verordening (EU) nr. 910/2014 beschreven cyberbeveiligingsdoelstellingen, zoals vertrouwelijkheid, integriteit en beschikbaarheid van de portemonnee-oplossing, alsook met de privacy van gebruikers en gegevens. In de vereisten van nationale certificeringsregelingen moet terdege rekening worden gehouden met de risico's en bedreigingen die in dit risicoregister zijn opgenomen. Om gelijke tred te houden met het voortdurend veranderende dreigingslandschap, moet het risicoregister samen met de samenwerkingsgroep worden bijgehouden en regelmatig worden bijgewerkt.

(12) Bij het vaststellen van hun certificeringsregelingen moeten de regelinghouders een risicobeoordeling uitvoeren om de in het register opgenomen risico's en bedreigingen te verfijnen en aan te vullen met risico's en bedreigingen die specifiek zijn voor de architectuur of de uitvoering van de portemonnee-oplossing. Bij de risicobeoordeling moet worden nagegaan hoe de toepasselijke risico's en bedreigingen op passende wijze kunnen worden afgehandeld. Portemonneeaanbieders moeten de risicobeoordeling van de regeling aanvullen om eventuele risico's en bedreigingen in kaart te brengen die specifiek zijn voor de uitvoering ervan en passende maatregelen voorstellen voor evaluatie door de certificerende instantie.

(13) Om aan te tonen dat een architectuur van een portemonnee-oplossing voldoet aan de toepasselijke beveiligingsvereisten, moet elke architectuurspecifieke regeling of elk architectuurspecifiek profiel ten minste een beschrijving van de architectuur van de portemonnee-oplossing, een lijst van beveiligingsvereisten die van toepassing zijn op de architectuur van de portemonnee-oplossing, een evaluatieplan om te bevestigen dat een op deze architectuur gebaseerde portemonnee-oplossing aan die vereisten voldoet, en een risicobeoordeling bevatten. De nationale certificeringsregelingen moeten portemonneeaanbieders verplichten om aan te tonen hoe het ontwerp van de portemonnee-oplossing die zij aanbieden, overeenkomt met de referentiearchitectuur en de beveiligingscontroles en valideringsplannen voor de specifieke portemonnee-oplossing specificeert. In de nationale certificeringsregelingen moet ook een conformiteitsbeoordelingsactiviteit worden gedefinieerd om te verifiëren of het portemonneeontwerp de referentiearchitectuur van het geselecteerde profiel naar behoren weerspiegelt. De nationale certificeringsregelingen moeten voldoen aan de vereisten van artikel 51 van Verordening (EU) 2019/881, met uitzondering van de punten e) en f), met betrekking tot de registratie.

(14) Wat de certificering van producten betreft, moet gebruik kunnen worden gemaakt van certificaten van overeenstemming die zijn afgegeven in het kader van de EUCC en certificaten van overeenstemming die zijn afgegeven in het kader van nationale certificeringsregelingen in het kader van de overeenkomst inzake wederzijdse erkenning van de SOG-IS. Voorts moeten andere nationale certificeringsregelingen kunnen worden gebruikt voor minder gevoelige productcomponenten, zoals die welke zijn vastgesteld volgens CEN EN 17640 voor een methodologie voor de evaluatie van de cyberbeveiliging op vaste tijden.

(15) Het EU-betrouwbaarheidskeurmerk van de portemonnee voor digitale identiteit ("betrouwbaarheidskeurmerk") moet worden gebruikt om op duidelijke, eenvoudige en herkenbare wijze aan te geven dat een portemonnee is geleverd overeenkomstig Verordening (EU) nr. 910/2014. Daarom moet dit worden beschouwd als een conformiteitsmerk voor een portemonnee-oplossing die is gecertificeerd in het kader van nationale certificeringsregelingen. De nationale certificeringsregelingen mogen geen andere conformiteitsmerken definiëren.

(16) Om fraude te ontmoedigen, moeten in de nationale certificeringsregelingen maatregelen worden vastgesteld die moeten worden genomen wanneer certificering in het kader van de regeling frauduleus wordt aangevraagd.

(17) Met het oog op een efficiënt beheer van kwetsbaarheidsmeldingen moeten aanbieders van portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij worden verstrekt, processen vaststellen en toepassen om de ernst en de potentiële impact van kwetsbaarheden te beoordelen. In de nationale certificeringsregelingen moet een drempel worden vastgesteld waarboven de certificerende instantie moet worden ingelicht. Een dergelijke kennisgevingsverplichting mag geen afbreuk doen aan de criteria die zijn vastgesteld in de wetgeving inzake gegevensbescherming en door de gegevensbeschermingsautoriteiten van de lidstaten voor kennisgeving van inbreuken in verband met persoonsgegevens. Er kan mogelijke synergie tot stand worden gebracht tussen de verplichte kennisgeving van inbreuken op of schendingen van de portemonnee-oplossingen en de kennisgeving van inbreuken in verband met persoonsgegevens overeenkomstig Verordening (EU) 2016/679. De beoordeling door de certificerende instantie van een verslag over de kwetsbaarheidseffectbeoordeling mag geen afbreuk doen aan de beoordeling door een gegevensbeschermingsautoriteit van een gegevensbeschermingseffectbeoordeling overeenkomstig de artikelen 35 en 36 van Verordening (EU) 2016/679.

(18) De aanbieders van portemonneeoplossingen en het stelsel voor elektronische identificatie op grond waarvan die worden aangeboden, moeten de eigenaar van het stelsel in kennis stellen van rechtvaardigingen voor uitzonderingen op de kwetsbaarheidsbeoordeling die vereist is voor de evaluatie van het beveiligd cryptografisch middel voor portemonnees en de beveiligde cryptografische toepassing voor portemonnees, zoals uiteengezet in bijlage IV.

(19) De annulering van een certificaat van overeenstemming kan ernstige gevolgen hebben, zoals de intrekking van alle ingezette portemonnee-eenheden. Daarom mogen certificerende instanties alleen overwegen te annuleren indien een niet-herstelde kwetsbaarheid waarschijnlijk aanzienlijke gevolgen zal hebben voor de betrouwbaarheid van de portemonnee-oplossing of de betrouwbaarheid van een andere portemonnee-oplossing.

(20) Er moet een specifiek proces voor de actualisering van de nationale certificeringsregelingen worden ingevoerd om de overgang tussen opeenvolgende releases van regelingen te beheren, met name met betrekking tot de maatregelen die de certificaathouder moet nemen met betrekking tot komende evaluaties, onderhoud, hercertificering en bijzondere evaluaties.

(21) Ter bevordering van de transparantie moeten portemonneeaanbieders beveiligingsinformatie over hun portemonnee-oplossing openbaar delen.

(22) Wanneer de nationale certificeringsregelingen steunen op zekerheidsinformatie uit andere certificeringsregelingen of bronnen, moet een afhankelijkheidsanalyse worden uitgevoerd om na te gaan of de zekerheidsdocumentatie, bijvoorbeeld zekerheidsverslagen en certificaten van overeenstemming, beschikbaar en adequaat is voor de portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt. Deze afhankelijkheidsanalyse moet gebaseerd zijn op de risicobeoordeling van de portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt. Bij de evaluatie moet worden vastgesteld of de zekerheidsdocumentatie die beschikbaar is voor een bepaalde portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, toereikend is om zekerheid te bieden die overeenstemt met het beoogde evaluatieniveau. De evaluatie moet ook de afhankelijkheidsanalyse actualiseren of, indien nodig, volledig herevalueren.

(23) Certificerende instanties moeten certificaten van overeenstemming afgeven in het kader van de nationale certificeringsregelingen, samen met een openbaar toegankelijk certificeringsrapport, als bedoeld in artikel 5 quinquies, lid 2, punt a), van Verordening (EU) nr. 910/2014. Het bijbehorende certificeringsbeoordelingsverslag moet ter beschikking van de samenwerkingsgroep worden gesteld.

(24) De nationale certificeringsregelingen moeten een jaarlijkse evaluatie van het toezicht vaststellen om ervoor te zorgen dat de processen rond het beheer en onderhoud van de portemonnees doeltreffend functioneren, wat betekent dat zij functioneren zoals gedefinieerd in het beleid waarin de processen zijn bepaald. De tweejaarlijkse kwetsbaarheidsbeoordeling is een vereiste dat voortvloeit uit Verordening (EU) nr. 910/2014, om ervoor te zorgen dat de portemonnee-oplossing de in het risicoregister vastgestelde cyberbeveiligingsrisico's en -bedreigingen, met inbegrip van ontwikkelingen van het dreigingslandschap, op passende wijze blijft afdekken. De begrippen "evaluatie van het toezicht", "evaluatie voor hercertificering" en "bijzondere evaluaties" moeten in overeenstemming zijn met ISO/IEC EN 17021-1:2015.

(25) Een certificeringscyclus eindigt met het verstrijken van het certificaat van overeenstemming of met de afgifte van een nieuw certificaat van overeenstemming na een succesvolle hercertificeringsbeoordeling. De evaluatie voor hercertificering moet een evaluatie van alle componenten van het voorwerp van de certificering omvatten, met inbegrip van een evaluatie van de doeltreffendheid en, indien van toepassing, een kwetsbaarheidsbeoordeling. Tijdens de hercertificering moet het mogelijk zijn de resultaten van eerdere evaluaties van componenten die niet zijn gewijzigd, te hergebruiken.

(26) Wanneer een Europese regeling voor cyberbeveiligingscertificering wordt vastgesteld, moeten de nationale certificeringsregelingen met hetzelfde toepassingsgebied na een vastgestelde overgangsperiode als bedoeld in artikel 57, lid 1, van Verordening (EU) 2019/881 geen certificeringen meer afgeven.

(27) De nationale certificeringsregelingen moeten in voorkomend geval gebaseerd zijn op bestaande kaders en bewijs hergebruiken om harmonisatie en interoperabiliteit te waarborgen. De lidstaten kunnen overeenkomsten sluiten voor het grensoverschrijdende hergebruik van certificeringsregelingen of delen ervan. De Europese Commissie en Enisa moeten, in samenwerking met de samenwerkingsgroep, de lidstaten ondersteunen bij de ontwikkeling en handhaving van hun nationale certificeringsregelingen om te zorgen voor kennisdeling en beste praktijken.

(28) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([9]) geraadpleegd en heeft op 30 september 2024 een advies uitgebracht.

(29) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het in artikel 48, lid 1, van Verordening (EU) nr. 910/2014 bedoelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Onderwerp en toepassingsgebied

Bij deze verordening worden referentienormen, specificaties en procedures vastgesteld om een robuust kader voor de certificering van portemonnees tot stand te brengen dat regelmatig moet worden bijgewerkt om in overeenstemming te blijven met de ontwikkelingen op het gebied van technologie en normen en met de werkzaamheden die worden verricht op basis van Aanbeveling (EU) 2021/946 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit, en met name de architectuur en het referentiekader.

Artikel 2

Definities

Voor de doelstellingen van deze verordening zijn de volgende definities van toepassing:

1) "portemonnee-oplossing": een combinatie van software, hardware, diensten, instellingen en configuraties, met inbegrip van portemonnee-instanties, een of meer beveiligde cryptografische toepassingen voor portemonnees en een of meer beveiligde cryptografische middelen voor portemonnees;

2) "regelinghouder": een organisatie die verantwoordelijk is voor de ontwikkeling en de handhaving van een certificeringsregeling;

3) "voorwerp van de certificering": producten, processen en diensten, of een combinatie daarvan, waarop specifieke vereisten van toepassing zijn;

4) "beveiligde cryptografische toepassing voor portemonnees": een toepassing die kritieke activa beheert door middel van koppeling aan en gebruikmaking van de cryptografische en niet-cryptografische functies van het beveiligd cryptografisch middel voor portemonnees;

5) "portemonnee-instantie": de toepassing die is geïnstalleerd en geconfigureerd op het apparaat of in de omgeving van een portemonneegebruiker, die deel uitmaakt van een portemonnee-eenheid, en die de portemonneegebruiker gebruikt voor de interactie met de portemonnee-eenheid;

([9]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

6) “beveiligd cryptografisch middel voor portemonnees”: een manipulatiebestendig apparaat dat een omgeving biedt die gekoppeld is aan en wordt gebruikt door de beveiligde cryptografische toepassing voor portemonnees om kritieke activa te beschermen en cryptografische functies te bieden voor de veilige uitvoering van kritieke activiteiten;

7) “risicoregister”: een register met informatie die relevant is voor het certificeringsproces met betrekking tot vastgestelde risico’s;

8) “aanbieder van portemonnees”: een natuurlijke of rechtspersoon die portemonnee-oplossingen aanbiedt;

9) “certificerende instantie”: een externe conformiteitsbeoordelingsinstantie die certificeringsregelingen toepast;

10) “portemonnee”: een unieke configuratie van een portemonnee-oplossing die bestaat uit portemonnee-instanties, beveiligde cryptografische toepassingen voor portemonnees en beveiligde cryptografische middelen voor portemonnees die door een aanbieder van portemonnees aan een individuele portemonneegebruiker worden verstrekt;

11) “kritieke activa”: activa in of met betrekking tot een portemonnee-eenheid die van dermate groot belang zijn dat, als de beschikbaarheid, de authenticiteit of de integriteit ervan in gevaar zou komen, dat een zeer ernstig, verzwakkend effect zou hebben op het vermogen om de portemonnee-eenheid te kunnen gebruiken;

12) “gebruiker van de portemonnee”: een gebruiker die de controle heeft over de portemonnee-eenheid;

13) “incident”: een incident zoals gedefinieerd in artikel 6, punt 6, van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([10]);

14) “ingebed openbaarmakingsbeleid”: regels die zijn opgenomen in een elektronische attestering van attributen door de aanbieder ervan, die de voorwaarden aangeeft waaraan een vertrouwende partij moet voldoen om toegang te krijgen tot de elektronische attestering van attributen.

HOOFDSTUK II

NATIONALE CERTIFICERINGSREGELINGEN

Artikel 3

Vaststelling van nationale certificeringsregelingen

1. De lidstaten duiden per nationale certificeringsregeling een regelinghouder aan.

2. Het in de nationale certificeringsregelingen gedefinieerde voorwerp van de certificering is het aanbieden en laten functioneren van portemonnee-oplossingen en van de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt.

3. Overeenkomstig Uitvoeringsverordening (EU) 2015/1502 omvat het voorwerp van de certificering in het kader van de nationale certificeringsregelingen de volgende elementen:

a) de softwarecomponenten, met inbegrip van de instellingen en configuraties van een portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan de portemonnee-oplossingen worden verstrekt;

b) de hardwarecomponenten en platforms waarop de in punt 33) bedoelde softwarecomponenten werken of waarop zij voor kritieke activiteiten afhankelijk zijn, in gevallen waarin zij direct of indirect worden geleverd door de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, en wanneer zij nodig zijn om aan het gewenste betrouwbaarheidsniveau voor die softwarecomponenten te voldoen. Als de hardwarecomponenten en platforms niet door de aanbieder van portemonnees worden geleverd, worden in de nationale certificeringsregelingen veronderstellingen voor de evaluatie van de hardwarecomponenten en platforms geformuleerd, op grond waarvan weerstand kan worden geboden tegen aanvallers met een hoog aanvalspotentieel overeenkomstig Uitvoeringsverordening (EU) 2015/1502, en worden de evaluatieactiviteiten gespecificeerd om deze in bijlage IV genoemde veronderstellingen te bevestigen;

([10]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) de processen die de levering en de werking van een portemonnee-oplossing ondersteunen, waaronder het instapproces voor gebruikers zoals bedoeld in artikel 5 bis van Verordening (EU) nr. 910/2014, die ten minste betrekking hebben op de inschrijving, het elektronisch middelenbeheer en de organisatie overeenkomstig de punten 2.1, 2.2 en 2.4 van bijlage I bij Uitvoeringsverordening (EU) 2015/1502.

4. De nationale certificeringsregelingen omvatten een beschrijving van de specifieke architectuur van portemonnee-oplossingen en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt. Wanneer de nationale certificeringsregelingen betrekking hebben op meer dan één specifieke architectuur, moeten zij een profiel per afzonderlijke architectuur bevatten.

5. Per profiel bevat de nationale certificeringsregelingen ten minste het volgende:

a) de specifieke architectuur van een portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt;

b) de beveiligingscontroles in verband met betrouwbaarheidsniveaus als bedoeld in artikel 8 van Verordening (EU) nr. 910/2014;

c) een evaluatieplan dat is opgesteld overeenkomstig punt 7.4.1 van EN ISO/IEC 17065;2012;

d) de beveiligingsvereisten die nodig zijn om de cyberbeveiligingsrisico's en -bedreigingen aan te pakken die zijn opgenomen in het in bijlage I bij deze verordening vastgestelde risicoregister, tot het vereiste betrouwbaarheidsniveau, en om, in voorkomend geval, te voldoen aan de in artikel 51 van Verordening (EU) 2019/881 vastgestelde doelstellingen;

e) een inventarisatie van de in punt b) bedoelde controles aan de hand van de componenten van de architectuur

f) een beschrijving van de wijze waarop de beveiligingscontroles, de inventarisatie, de beveiligingsvereisten en het in de punten b) tot en met c) bedoelde evaluatieplan de aanbieders van portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij worden verstrekt, in staat stellen de cyberbeveiligingsrisico's en -bedreigingen in het in punt d) bedoelde risicoregister adequaat aan te pakken, tot het vereiste betrouwbaarheidsniveau.

6. Het in lid 5, punt c), genoemde evaluatieplan vermeldt de evaluatieactiviteiten die moeten worden opgenomen in de evaluatie van portemonnee-oplossingen en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt.

7. Krachtens de in lid 6 bedoelde evaluatiewerkzaamheden moeten aanbieders van portemonnee-oplossingen en de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt, informatie verstrekken die voldoet aan de vereisten van bijlage II.

Artikel 4

Algemene vereisten

1. De nationale certificeringsregelingen hebben betrekking op de vereisten inzake functionaliteit, cyberbeveiliging en gegevensbescherming, door, indien beschikbaar en van toepassing, gebruik te maken van de volgende certificeringsregelingen:

a) de Europese regelingen voor cyberbeveiligingscertificering die zijn vastgesteld op grond van Verordening (EU) 2019/881, met inbegrip van de EUCC;

b) de nationale regelingen voor cyberbeveiligingscertificering die onder de EUCC vallen, overeenkomstig artikel 49 van Uitvoeringsverordening (EU) 2024/482.

2. De nationale certificeringsregelingen kunnen daarnaast, indien beschikbaar en van toepassing, verwijzen naar:

a) andere relevante nationale certificeringsregelingen;

b) internationale, Europese en nationale normen;

c) technische specificaties die voldoen aan de eisen van bijlage II bij Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([11]).

3. De nationale certificeringsregelingen:

a) specificeren de in punt 6.5 van ISO/IEC EN 17067:2013 vermelde elementen;

b) worden uitgevoerd als een regeling van type 6, overeenkomstig punt 5.3.8 van ISO/IEC EN 17067:2013.

4. De nationale certificeringsregelingen voldoen aan de volgende vereisten:

a) alleen aan aanbieders als bedoeld in artikel 5 bis, lid 2, van Verordening (EU) nr. 910/2014 worden certificaten in het kader van de nationale certificeringsregelingen verstrekt;

b) alleen het betrouwbaarheidskeurmerk wordt als conformiteitsmerk gebruikt;

c) aanbieders van portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij worden verstrekt, verwijzen naar Verordening (EU) nr. 910/2014 en deze verordening als zij naar de regeling verwijzen;

d) aanbieders van portemonneeoplossingen en het stelsel voor elektronische identificatie in het kader waarvan deze worden aangeboden, vormen een aanvulling op de risicobeoordeling van het stelsel als bedoeld in artikel 3, lid 5, punt f), om risico's en bedreigingen die specifiek zijn voor de uitvoering ervan in kaart te brengen en passende behandelingsmaatregelen voor alle relevante risico's en bedreigingen voor te stellen;

e) er worden verantwoordelijkheden en gerechtelijke stappen vastgesteld en er wordt verwezen naar de toepasselijke nationale wetgeving, waarin de verantwoordelijkheden en mogelijke gerechtelijke stappen worden omschreven als certificering in het kader van de regeling frauduleus wordt gebruikt.

5. De in lid 4, punt d), bedoelde beoordeling wordt ter evaluatie gedeeld met de certificerende instantie.

Artikel 5

Incidenten- en kwetsbaarheidsbeheer

1. De nationale certificeringsregelingen bevatten voorschriften voor het beheer van incidenten en kwetsbaarheden overeenkomstig de leden 2 tot en met 9.

2. De houder van een certificaat van overeenstemming van een portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, stelt de certificerende instantie onverwijld in kennis van elke inbreuk op of schending van de portemonnee-oplossing, of van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, die waarschijnlijk van invloed zal zijn op de conformiteit ervan met de vereisten van de nationale certificeringsregelingen.

3. De houder van een certificaat van overeenstemming zal een beleid en procedures voor kwetsbaarheidsbeheer opstellen, onderhouden en toepassen, rekening houdend met de procedures die zijn vastgelegd in bestaande Europese en internationale normen, waaronder ISO/IEC EN 30111:2019.

4. De houder van het certificaat van overeenstemming stelt de afgevende certificerende instantie in kennis van de kwetsbaarheden en wijzigingen die van invloed zijn op de portemonnee-oplossing op basis van vastgestelde criteria voor de gevolgen van deze kwetsbaarheden en wijzigingen.

5. De houder van het certificaat van overeenstemming stelt een verslag van de kwetsbaarheidseffectbeoordeling op voor elke kwetsbaarheid die van invloed is op de softwarecomponenten van de portemonnee-oplossing. Dat verslag bevat de volgende informatie:

a) de gevolgen van de kwetsbaarheid voor de gecertificeerde portemonnee-oplossing;

b) de mogelijke risico's die verband houden met de nabijheid of de waarschijnlijkheid van een aanval;

([11]) Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) de vraag of de kwetsbaarheid met de beschikbare middelen kan worden verholpen;

d) en indien de kwetsbaarheid met de beschikbare middelen kan worden verholpen, mogelijke manieren om die kwetsbaarheid te verhelpen.

6. Indien een kennisgeving op grond van lid 4is vereist, stuurt de houder van het certificaat van overeenstemming het in lid 5 bedoelde verslag van de kwetsbaarheidseffectbeoordeling onverwijld aan de certificerende instantie toe.

7. De houder van een certificaat van overeenstemming zal een beleid inzake kwetsbaarheidsbeheer vaststellen, onderhouden en uitvoeren [dat voldoet aan de vereisten van bijlage I bij de verordening cyberweerbaarheid ([12]).

8. In de nationale certificeringsregelingen worden vereisten inzake de openbaarmaking van kwetsbaarheden vastgesteld die op certificerende instanties van toepassing zijn.

9. De houder van een certificaat van overeenstemming zal alle algemeen bekende en herstelde kwetsbaarheden in de portemonnee-oplossing of in een van de in bijlage V bedoelde onlineregisters bekendmaken en registreren.

Artikel 6

Onderhoud van de nationale certificeringsregelingen

1. De nationale certificeringsregelingen moeten een procedure bevatten om de werking ervan periodiek te evalueren. Dat proces heeft tot doel de toereikendheid ervan te bevestigen en na te gaan welke aspecten moeten worden verbeterd, rekening houdend met de feedback van belanghebbenden.

2. De nationale certificeringsregelingen bevatten bepalingen betreffende het onderhoud ervan. Dit proces omvat ten minste de volgende vereisten:

a) regels voor de governance van de definitie en vereisten van de nationale certificeringsregelingen;

b) de vaststelling van tijdschema's voor de afgifte van certificaten na de vaststelling van geactualiseerde versies van de nationale certificeringsregelingen, zowel voor nieuwe certificaten van overeenstemming als voor eerder afgegeven certificaten;

c) een periodieke evaluatie van de nationale certificeringsregelingen om ervoor te zorgen dat de vereisten van de nationale certificeringsregelingen op consistente wijze worden toegepast, waarbij ten minste rekening wordt gehouden met de volgende aspecten:

— verzoeken om verduidelijking aan de regelinghouder met betrekking tot de vereisten van de nationale certificeringsregeling;

— feedback van belanghebbenden en andere betrokken partijen;

— de mate waarin de houder van de nationale certificeringsregeling reageert op verzoeken om informatie;

d) regels voor het bewaken van referentiedocumenten en -procedures voor de ontwikkeling van de referentieversies van de nationale certificeringsregelingen, met inbegrip van ten minste overgangsperioden;

e) een proces om ervoor te zorgen dat de recentste cyberbeveiligingsrisico's en -dreigingen, zoals opgenomen in het in bijlage I bij deze verordening opgenomen risicoregister, worden bestreken;

f) een proces voor het beheer van overige wijzigingen in nationale certificeringsregelingen.

([12]) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. De nationale certificeringsregelingen bevatten voorschriften voor het uitvoeren van evaluaties van momenteel gecertificeerde producten binnen een bepaalde periode na de herziening van de regeling of na de publicatie van nieuwe specificaties of normen, of nieuwe versies daarvan, waaraan de portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, moeten voldoen.

HOOFDSTUK III

VEREISTEN MET BETREKKING TOT DE REGELINGHOUDERS

Artikel 7

Algemene vereisten

1. Regelinghouders ontwikkelen en onderhouden nationale certificeringsregelingen en regelen de werking ervan.

2. Regelinghouders kunnen hun taken geheel of gedeeltelijk uitbesteden aan een derde partij. In geval van uitbesteding aan een particuliere partij stellen regelinghouders de taken en verantwoordelijkheden van alle partijen bij overeenkomst vast. Regelinghouders blijven verantwoordelijk voor alle uitbestede activiteiten die door hun subcontractanten worden uitgevoerd.

3. Regelinghouders voeren hun toezichtactiviteiten, indien van toepassing, ten minste op basis van de volgende informatie uit:

a) informatie afkomstig van certificerende instanties, nationale accreditatie-instanties en relevante markttoezichtautoriteiten;

b) informatie die voortvloeit uit audits en onderzoeken uitgevoerd door de eigen autoriteit of door een andere autoriteit;

c) klachten en beroepen op grond van artikel 15.

4. Regelinghouders stellen de samenwerkingsgroep in kennis van herzieningen van de nationale certificeringsregelingen. Die kennisgeving bevat adequate informatie voor de samenwerkingsgroep om aanbevelingen te kunnen doen aan de regelinghouders en adviezen uit te brengen over de geactualiseerde nationale certificeringsregelingen.

HOOFDSTUK IV

VEREISTEN MET BETREKKING TOT AANBIEDERS VAN PORTEMONNEE-OPLOSSINGEN EN HET STELSEL VAN ELECTRONISCHE IDENTIFICATIE OP GROND WAARVAN ZIJ WORDEN VERSTREKT

Artikel 8

Algemene vereisten

1. De nationale certificeringsregelingen bevatten cyberbeveiligingsvereisten op basis van een risicobeoordeling per specifieke ondersteunde architectuur. Die cyberbeveiligingsvereisten zijn gericht op de afhandeling van de vastgestelde cyberbeveiligingsrisico's en -bedreigingen, zoals vastgesteld in het in bijlage I beschreven risicoregister.

2. Overeenkomstig artikel 5 bis, lid 23, van Verordening (EU) nr. 910/2014 wordt in nationale certificeringsregelingen vereist dat portemonnee-oplossingen en de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt, met een betrouwbaarheidsniveau "hoog", in de zin van Uitvoeringsverordening (EU) 2015/1502 bestand zijn tegen aanvallers met een hoog aanvalspotentieel.

3. In de nationale certificeringsregelingen worden beveiligingscriteria vastgesteld, inclusief de volgende vereisten:

a) verordening cyberweerbaarheid, indien van toepassing, of vereisten die voldoen aan de beveiligingsdoelstellingen van artikel 51 van Verordening (EU) 2019/881;

b) de vaststelling en de uitvoering van beleid en procedures voor het beheren van risico's in verband met de werking van een portemonnee-oplossing, met inbegrip van de identificatie en de beoordeling van risico's en de beperking van de vastgestelde risico's;

c) de vaststelling en de uitvoering van beleid en procedures met betrekking tot het beheer van wijzigingen en het kwetsbaarheidsbeheer overeenkomstig artikel 5;

d) de vaststelling en de uitvoering van beleid en procedures voor personeelsbeheer, met inbegrip van vereisten inzake deskundigheid, betrouwbaarheid, ervaring, veiligheidsopleiding en kwalificaties van personeel dat betrokken is bij de ontwikkeling of werking van de portemonnee-oplossing;

e) vereisten met betrekking tot de operationele omgeving van de portemonnee-oplossing, onder meer in de vorm van veronderstellingen over de beveiliging van de apparaten en platforms waarop de softwarecomponenten van de portemonnee-oplossing draaien, met inbegrip van beveiligde cryptografische middelen voor portemonnees en, indien van toepassing en relevant, conformiteitsbeoordelingsvereisten om te bevestigen dat die veronderstellingen op de relevante apparaten en platforms worden geverifieerd;

f) voor elke veronderstelling die niet door een certificaat van overeenstemming of andere aanvaardbare zekerheidsinformatie wordt gestaafd, een beschrijving van het mechanisme dat de aanbieder van portemonnees gebruikt om de veronderstelling af te dwingen, alsmede een motivering dat het mechanisme toereikend is om ervoor te zorgen dat de veronderstelling wordt geverifieerd;

g) de vaststelling en de uitvoering van maatregelen om het gebruik van een momenteel gecertificeerde versie van de portemonnee-oplossing te waarborgen.

4. De nationale certificeringsregelingen bevatten functionele eisen met betrekking tot de actualiseringsmechanismen voor elke softwarecomponent van de portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij voor de in bijlage III vermelde activiteiten wordt verstrekt.

5. De nationale certificeringsregelingen vereisen dat de aanvrager voor certificering de volgende informatie en documentatie verstrekt of anderszins ter beschikking stelt van de certificerende instantie:

a) bewijsstukken met betrekking tot de in punt 1 van bijlage IV bedoelde informatie, met inbegrip van, indien nodig, bijzonderheden over de portemonnee-oplossing en de broncode ervan, waaronder:

— *informatie over de architectuur:* voor elke component van de portemonnee-oplossing (met inbegrip van product-, proces- en servicecomponenten), een beschrijving van de essentiële beveiligingseigenschappen, met inbegrip van de externe afhankelijkheden;

— *controles en betrouwbaarheidsniveaus:* voor elke beveiligingscontrole van de portemonnee-oplossing, een beschrijving van het controleniveau en het vereiste betrouwbaarheidsniveau, gebaseerd op de bijlage bij Uitvoeringsverordening (EU) 2015/1502, waarin een aantal technische specificaties en procedures zijn opgenomen die van toepassing zijn op de verschillende controles die door middel van elektronische identificatiemiddelen worden uitgevoerd;

— *een inventarisatie van de controles op de architectuurcomponenten:* een beschrijving van de wijze waarop de controles van de portemonnee worden uitgevoerd, met gebruikmaking van de verschillende componenten van de portemonnee-oplossing, op basis van een motivering waarin wordt uitgelegd waarom een bepaald betrouwbaarheidsniveau vereist is, en hoe de controle met alle vereiste beveiligingsaspecten op het passende niveau wordt uitgevoerd;

— *een motivering en onderbouwing van de risicodekking:* een motivering van:

— de inventaris van de controles per component;

— de geschiktheid van het voorgestelde evaluatieplan om alle controles op passende wijze te bestrijken;

— de dekking die wordt geboden door de controles van de cyberbeveiligingsrisico's en -dreigingen die in het risicoregister zijn vastgesteld, aangevuld met controles van risico's en bedreigingen die specifiek zijn voor de uitvoering, op het passende zekerheidsniveau.

b) de in bijlage V vermelde informatie;

c) een volledige lijst van de certificaten van overeenstemming en andere zekerheidsinformatie die bij de evaluatieactiviteiten als bewijs is gebruikt;

d) alle andere informatie die relevant is voor de evaluatieactiviteiten.

HOOFDSTUK V

VEREISTEN MET BETREKKING TOT CERTIFICERENDE INSTANTIES

Artikel 9

Algemene vereisten

1. Certificerende instanties worden geaccrediteerd door nationale accreditatie-instanties die uit hoofde van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad ([13]) zijn aangewezen overeenkomstig ISO/IEC EN 17065:2012, mits zij voldoen aan de vereisten die zijn vastgesteld in nationale certificeringsregelingen overeenkomstig lid 2.

2. Met het oog op accreditatie voldoen certificerende instanties aan de volgende eisen van bekwaamheid:

a) gedetailleerde en technische kennis van de relevante architecturen van een portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, alsmede van de dreigingen en risico's die relevant zijn voor die architecturen;

b) kennis van beschikbare beveiligingsoplossingen en van de eigenschappen ervan overeenkomstig de bijlage bij Uitvoeringsverordening (EU) 2015/1502;

c) kennis van de activiteiten die worden verricht op grond van certificaten van overeenstemming die worden toegepast op componenten van de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, als het voorwerp van de certificering;

d) gedetailleerde kennis van de toepasselijke nationale certificeringsregeling zoals vastgesteld overeenkomstig hoofdstuk II.

3. Certificerende instanties verrichten hun toezichtactiviteiten met name op basis van de volgende informatie:

a) informatie afkomstig van nationale accreditatie-instanties en relevante markttoezichtautoriteiten;

b) informatie die voortvloeit uit hun eigen audits en onderzoeken uitgevoerd of die van een andere autoriteit;

c) klachten en beroepen op grond van artikel 15.

Artikel 10

Uitbesteding

Certificerende instanties kunnen de in artikel 13 bedoelde evaluatieactiviteiten aan derden uitbesteden. Wanneer evaluatie-activiteiten worden uitbesteed, wordt in de nationale certificeringsregelingen het volgende vastgesteld:

1) alle subcontractanten van de certificerende instantie die evaluatieactiviteiten verrichten, moeten, voor zover van toepassing en passend voor de uit te voeren activiteiten, voldoen aan de eisen van geharmoniseerde normen zoals de ISO/IEC EN 17025:2017 voor tests, ISO/IEC EN 17020:2012 voor inspecties, ISO/IEC EN 17021-1:2015 voor audits en ISO/IEC EN 17029:2019 voor validering en verificatie;

2) certificerende instanties aanvaarden de verantwoordelijkheid voor alle evaluatieactiviteiten die aan andere instanties zijn uitbesteed en aantonen dat zij tijdens hun accreditatie passende maatregelen hebben genomen, onder meer door, in voorkomend geval, een beroep te doen op de eigen accreditatie van hun subcontractanten;

3) in hoeverre voorafgaande toestemming voor uitbesteding wordt verkregen van de regelinghouders of de afnemer van wie de portemonnee-oplossing in het kader van de certificeringsregeling wordt gecertificeerd.

([13]) 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, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artikel 11

Kennisgeving aan het toezichthoudend orgaan

Certificerende instanties stellen het in artikel 46 bis, lid 1, van Verordening (EU) nr. 910/2014 bedoelde toezichthoudende orgaan in kennis van de afgifte, de opschorting en de annulering van certificaten van overeenstemming van portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt.

Artikel 12

Incidenten- en kwetsbaarheidsbeheer

1. De certificerende instanties schorten het certificaat van overeenstemming van de portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, onverwijld op na de bevestiging dat het gemelde incident of de gemelde kwetsbaarheid een inbreuk vormt op of een schending betekent van de beveiliging van de portemonnee-oplossing of van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, die gevolgen heeft voor de conformiteit ervan met de vereisten van de nationale certificeringsregelingen.

2. De certificerende instanties annuleren het certificaat van overeenstemming dat is opgeschort naar aanleiding van een inbreuk op of schending van de beveiliging die niet tijdig is verholpen.

3. De certificerende instanties annuleren certificaten van overeenstemming als een vastgestelde kwetsbaarheid niet tijdig is verholpen in overeenstemming met de ernst en de mogelijke gevolgen ervan, overeenkomstig de artikelen 5 quater, lid 4, en 5 sexies, lid 2, van Verordening (EU) nr. 910/2014.

HOOFDSTUK VI

CONFORMITEITSBEOORDELING

Artikel 13

Evaluatieactiviteiten

1. De nationale certificeringsregelingen bevatten methoden en procedures die de conformiteitsbeoordelingsinstanties moeten volgen bij het uitvoeren van hun evaluatieactiviteiten overeenkomstig ISO/IEC EN 17065:2012, en ten minste betrekking hebben op de volgende aspecten:

a) de methoden en procedures voor het uitvoeren van evaluatieactiviteiten, met inbegrip van de methoden en procedures in verband met het beveiligd cryptografisch middel voor portemonnees, zoals uiteengezet in bijlage IV;

b) een audit van de uitvoering van de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, op basis van het in bijlage I beschreven risicoregister en waar nodig aangevuld met specifieke risico's voor de uitvoering;

c) functionele testactiviteiten, gebaseerd, indien beschikbaar en passend, op testreeksen die zijn gedefinieerd volgens technische specificaties of normen;

d) een beoordeling van het bestaan en de geschiktheid van onderhoudsprocessen, met inbegrip van ten minste versiebeheer, actualiseringsbeheer en kwetsbaarheidsbeheer;

e) een beoordeling van de operationele doeltreffendheid van de onderhoudsprocessen, met inbegrip van ten minste versiebeheer, actualiseringsbeheer en kwetsbaarheidsbeheer;

f) een door de aanbieder van portemonnees verstrekte afhankelijkheidsanalyse, met inbegrip van een methode om de aanvaardbaarheid van zekerheidsinformatie te beoordelen, die de in bijlage VI vermelde elementen omvat;

g) een kwetsbaarheidsbeoordeling, op het passende niveau, met inbegrip van:

— een evaluatie van het ontwerp van de portemonnee-oplossing en, indien van toepassing, van de broncode ervan;

— het testen van de weerstand van de portemonnee-oplossing voor betrouwbaarheidsniveau "hoog" in de zin van punt 2.2.1 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502 tegen aanvallers met een hoog aanvalspotentieel;

h) een beoordeling van de ontwikkeling van het dreigingslandschap en de gevolgen ervan voor de dekking van de risico's door de portemonnee-oplossing, om te bepalen welke evaluatieactiviteiten voor de verschillende componenten van de portemonnee-oplossing vereist zijn.

2. In de nationale certificeringsregelingen wordt een evaluatie opgenomen om te bepalen of de uitvoering van portemonnee-oplossingen en het stelsel voor elektronische identificatie in het kader waarvan die portemonnee-oplossingen worden verstrekt, overeenstemmen met de architectuur als bedoeld in artikel 3, lid 5, punt a), alsmede een evaluatie om te bepalen of het evaluatieplan dat samen met de uitvoering wordt voorgesteld, overeenstemt met het in artikel 3, lid 5, punt c), bedoelde evaluatieplan.

3. In de nationale certificeringsregelingen worden bemonsteringsvoorschriften vastgesteld om herhaling van identieke evaluatieactiviteiten te voorkomen en de nadruk te leggen op activiteiten die specifiek zijn voor een bepaalde variant. Op grond van die bemonsteringsvoorschriften mogen functionele en beveiligingstests alleen worden uitgevoerd op een monster van varianten van een doelcomponent van een portemonnee-oplossing en het stelsel voor elektronische identificatie in het kader waarvan zij worden verstrekt, en op een monster van doelapparaten. In de nationale certificeringsregelingen wordt vereist dat alle certificerende instanties hun gebruik van monsterneming rechtvaardigen.

4. Krachtens de nationale certificeringsregelingen evalueren de certificerende instantie de beveiligde cryptografische toepassing voor portemonnees op basis van de in bijlage IV beschreven methoden en procedures.

Artikel 14

Certificeringsactiviteiten

1. In de nationale certificeringsregelingen wordt een attesteringsactiviteit vastgesteld met als doel de afgifte van een certificaat van overeenstemming overeenkomstig deel V, punt a), van ISO/IEC EN 17067:2013, tabel 1, met inbegrip van de volgende aspecten:

a) de inhoud van het certificaat van overeenstemming zoals beschreven in bijlage VII;

b) de wijze waarop de resultaten van de evaluatie worden gerapporteerd in het openbaar certificeringsrapport, met inbegrip van ten minste een samenvatting van het voorlopige audit- en valideringsplan, zoals uiteengezet in bijlage VIII;

c) de inhoud van de in het certificeringsbeoordelingsverslag gerapporteerde evaluatieresultaten, met inbegrip van de in bijlage VIII vermelde elementen.

2. Het certificeringsbeoordelingsverslag kan ter beschikking worden gesteld van de samenwerkingsgroep en de Commissie.

Artikel 15

Klachten en beroep

De nationale certificeringsregelingen bevatten procedures of verwijzingen naar de toepasselijke nationale wetgeving, waarin het mechanisme wordt vastgesteld om klachten en beroepen in verband met de uitvoering van de certificeringsregeling of een afgegeven certificaat van overeenstemming doeltreffend in te dienen en te behandelen. Deze procedures bestaan uit het verstrekken van informatie aan de klager over de voortgang van de procedure en over het genomen besluit, en informatie aan de klager over het recht op een doeltreffende voorziening in rechte. In de nationale certificeringsregelingen wordt bepaald dat alle klachten en beroepen die niet door de certificerende instantie zijn of kunnen worden opgelost, ter beoordeling en afhandeling naar de regelinghouder worden doorgestuurd.

Artikel 16

Toezichtactiviteiten

1. In de nationale certificeringsregelingen wordt bepaald dat certificerende instanties toezichtactiviteiten uitvoeren die bestaan uit een evaluatie van het toezicht op processen in combinatie met willekeurige tests of inspecties.

2. In de nationale certificeringsregelingen worden eisen voor regelinghouders opgenomen om toezicht te houden op de naleving door certificerende instanties van hun verplichtingen krachtens Verordening (EU) nr. 910/2014 en, indien van toepassing, nationale certificeringsregelingen.

3. In de nationale certificeringsregelingen worden eisen voor certificerende instanties opgenomen om toezicht te houden op het volgende:

a) de naleving door houders van een certificaat van overeenstemming dat is afgegeven in het kader van nationale certificeringsregelingen van hun verplichtingen inzake certificering krachtens Verordening (EU) nr. 910/2014 en nationale certificeringsregelingen;

b) overeenstemming van de gecertificeerde portemonnee-oplossing met de vereisten van de nationale certificeringsregelingen.

Artikel 17

Gevolgen van niet-naleving

In de nationale certificeringsregelingen worden de gevolgen uiteengezet van de niet-nakoming van een gecertificeerde portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, met de voorschriften van deze verordening. Die gevolgen bestaan uit de volgende aspecten:

1) de verplichting voor de certificerende instantie om de houder van het certificaat van overeenstemming in te lichten en de houder van het certificaat van overeenstemming te verzoeken corrigerende maatregelen te nemen;

2) de verplichting voor de certificerende instantie om andere relevante markttoezichtautoriteiten in te lichten als de niet-naleving betrekking heeft op relevante Uniewetgeving;

3) de voorwaarden voor de uitvoering van corrigerende maatregelen door de houder van het certificaat van overeenstemming;

4) de voorwaarden voor de opschorting van een certificaat van overeenstemming door de certificerende instantie en voor het herstel van het certificaat van overeenstemming nadat de niet-naleving is verholpen;

5) de voorwaarden voor de annulering van een certificaat van overeenstemming door de certificerende instantie;

6) de gevolgen van niet-naleving door de certificerende instantie van de vereisten van de nationale certificeringsregeling.

HOOFDSTUK VII

CERTIFICERINGSCYCLUS

Artikel 18

Certificeringscyclus

1. De geldigheid van in het kader van nationale certificeringsregelingen afgegeven certificaten van overeenstemming wordt onderworpen aan regelmatige evaluatieactiviteiten door de certificerende instantie, uitgevoerd overeenkomstig de eisen van bijlage IX.

2. De nationale certificeringsregelingen bevatten een proces voor de hercertificering van portemonnee-oplossingen en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, op verzoek van de houder van het certificaat van overeenstemming vóór het verstrijken van het oorspronkelijke certificaat van overeenstemming. Dat proces voor hercertificering bevat een volledige evaluatie van de portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, met inbegrip van een kwetsbaarheidsbeoordeling, overeenkomstig de beginselen van bijlage IX.

3. De nationale certificeringsregelingen bevatten een proces voor het beheer van wijzigingen in een gecertificeerde portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt. Dat proces bevat regels om te bepalen of een wijziging moet worden gedekt door een bijzondere evaluatie als bedoeld in lid 4 of door de verificatie van de operationele doeltreffendheid van de onderhoudsprocessen als bedoeld in bijlage IV.

4. De nationale certificeringsregelingen bevatten een proces voor bijzondere evaluaties overeenkomstig ISO/IEC EN 17065:2012. Dat proces voor bijzondere evaluaties omvat een selectie van activiteiten die moeten worden uitgevoerd om het specifieke probleem aan te pakken dat aanleiding heeft gegeven tot de bijzondere evaluatie.

5. De nationale certificeringsregelingen bevatten regels voor de annulering van een certificaat van overeenstemming.

HOOFDSTUK VIII

REGISTRATIE EN BESCHERMING VAN INFORMATIE

Artikel 19

Bewaren van gegevens

1. De nationale certificeringsregelingen bevatten vereisten voor certificerende instanties met betrekking tot een registratiesysteem voor alle relevante informatie die is geproduceerd in verband met de conformiteitsbeoordelingsactiviteiten die zij uitvoeren, met inbegrip van gegevens die zijn afgegeven en ontvangen door aanbieders van portemonnee-oplossingen en de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt. De bestanden met deze informatie worden op een veilige manier opgeslagen. De bestanden kunnen elektronisch worden bewaard en blijven toegankelijk zo lang als vereist krachtens het Unierecht of het nationale recht, en gedurende ten minste vijf jaar na de annulering of het verstrijken van het desbetreffende certificaat van overeenstemming.

2. De nationale certificeringsregelingen bevatten voorschriften voor de houder van het certificaat van overeenstemming om de volgende informatie veilig op te slaan voor de toepassing van deze verordening, en gedurende ten minste vijf jaar na de annulering of het verstrijken van het desbetreffende certificaat van overeenstemming:

a) bestanden over de informatie die tijdens het certificeringsproces aan de certificerende instantie of haar subcontractanten is verstrekt;

b) monsters van hardwarecomponenten die zijn opgenomen in het toepassingsgebied van de certificering voor de portemonnee-oplossing.

3. De nationale certificeringsregelingen moeten vereisen dat de houder van het certificaat van overeenstemming de in lid 1 bedoelde informatie op verzoek ter beschikking stelt van het certificerende instantie of het toezichthoudende orgaan als bedoeld in artikel 46 bis, lid 1, van Verordening (EU) nr. 910/2014.

Artikel 20

Bescherming van informatie

In het kader van de nationale certificeringsregelingen waarborgen personen of organisaties aan wie bij de uitvoering van activiteiten in het kader van de nationale certificeringsregeling toegang tot informatie wordt verleend, de beveiliging en de bescherming van bedrijfsgeheimen en andere vertrouwelijke informatie, en intellectuele-eigendomsrechten en nemen zij de nodige en passende technische en organisatorische maatregelen om die vertrouwelijkheid te waarborgen.

HOOFDSTUK IX

SLOTBEPALINGEN

Artikel 21

Overgang naar een Europese regeling voor cyberbeveiligingscertificering

Deze verordening wordt herzien bij de vaststelling van de eerste Europese regeling voor cyberbeveiligingscertificering voor portemonnee-oplossingen en de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt, met als doel rekening te houden met de bijdrage van een dergelijke Europese regeling voor cyberbeveiligingscertificering aan de algemene certificering van portemonnee-oplossingen en de stelsels voor elektronische identificatie op grond waarvan zij worden verstrekt.

Artikel 22

Inwerkingtreding

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, 28 november 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE I

RISICOREGISTER VOOR EUROPESE PORTEMONNEES VOOR DIGITALE IDENTITEIT

Inleiding

In het risicoregister worden de belangrijkste risico's en dreigingen voor de veiligheid en privacy beschreven die van toepassing zijn op portemonnees en die naar behoren moeten worden aangepakt in elke architectuur en uitvoering van portemonnees. De **risico's van een hoog niveau** (deel I) hebben betrekking op het gebruik van portemonnees door gebruikers en vertrouwende partijen en houden verband met directe bedreigingen die gericht zijn op de activa in de portemonnees. Daarnaast worden enkele **risico's op systeemniveau** (deel II) voor portemonnees benoemd die doorgaans het gevolg zijn van een combinatie van bedreigingen die van toepassing zijn op het gehele systeem van portemonnees.

Soort risico	Risico-ID	Gerelateerde risicoaanduidingen
Risico's van een hoog niveau voor de portemonnees	R1	Aanmaken of gebruiken van een bestaande elektronische identiteit
	R2	Aanmaken of gebruiken van een valse elektronische identiteit
	R3	Aanmaken of gebruiken van valse attributen
	R4	Identiteitsdiefstal
	R5	Gegevensdiefstal
	R6	Openbaarmaking van gegevens
	R7	Gegevensmanipulatie
	R8	Gegevensverlies
	R9	Niet-toegestane transactie
	R10	Manipulatie van transacties
	R11	Afwijzing
	R12	Openbaarmaking van transactiegegevens
	R13	Verstoring van de dienstverlening
	R14	Toezicht
Systeemgerelateerde risico's	SR1	Grootschalig toezicht
	SR2	Reputatieschade
	SR3	Niet-naleving van de wettelijke voorschriften

In het register worden ook **technische bedreigingen** (deel III) vastgelegd die gericht zijn op de uitvoering van de portemonnee-oplossing. Deze bedreigingen houden verband met de risico's op hoog niveau, in die zin dat die bedreigingen kunnen worden gebruikt om vele risico's op hoog niveau te activeren.

Soort bedreiging	Bedreigings-ID	Gerelateerde bedreigingsaanduidingen	Subcategorieën van bedreigingen
Technische bedreiging	TT1	Fysieke aanvallen	1.1. *Diefstal*
			1.2. *Lekken van informatie*
			1.3 *Manipulatie*
	TT2	Fouten en verkeerde configuraties	2.1. *Fouten bij het beheer van een IT-systeem*
			2.2. *Fouten op toepassingsniveau of gebruiksfouten*
			2.3. *Ontwikkelingsfouten en verkeerde systeemconfiguraties*

Soort bedreiging	Bedreigings-ID	Gerelateerde bedreigingsaanduidingen	Subcategorieën van bedreigingen
	TT3	Gebruik van onbetrouwbare middelen	3.1. *Verkeerd gebruik of verkeerde configuratie van componenten van de portemonnee*
	TT4	Storing en uitval	4.1. *Storing of niet functioneren van apparatuur, apparaten of systemen*
			4.2. *Uitval van middelen*
			4.3 *Uitval van ondersteunende diensten*
	TT5	Kwaadwillige handelingen	5.1 *Onderschepping van informatie*
			5.2 *Phishing en spoofing*
			5.3 *Herhaling van berichten*
			5.4 *Bruteforceaanval*
			5.5 *Kwetsbaarheden in de software*
			5.6 *Aanvallen op de toeleveringsketen*
			5.7 *Malware*
			5.8 *Voorspelling van willekeurige getallen*

Ten slotte worden in het register de **directe bedreigingen voor de portemonnees** vermeld die worden gekoppeld aan een (niet-uitputtende) selectie van risico's (deel IV).

DEEL I

Risico's van een hoog niveau voor de portemonnees

R1. Aanmaken of gebruiken van een bestaande elektronische identiteit

Het aanmaken of gebruiken van een bestaande elektronische identiteit wordt gedefinieerd als het aanmaken van een elektronische identiteit in een portemonnee die in de echte wereld bestaat en aan een andere gebruiker wordt toegewezen. Dit risico leidt naar zijn aard tot de risico's van identiteitsdiefstal (R4) en niet-toegestane transacties (R9).

R2. Aanmaken of gebruiken van een valse elektronische identiteit

Het aanmaken of gebruiken van een valse elektronische identiteit wordt gedefinieerd als het aanmaken van een elektronische identiteit in een portemonnee die in de echte wereld niet bestaat.

R3. Aanmaken of gebruiken van valse attributen

Het aanmaken of gebruiken van valse attributen wordt gedefinieerd als het aanmaken of gebruiken van attributen waarvan niet kan kunnen worden gevalideerd dat ze zijn uitgegeven door de partij die beweert de aanbieder te zijn, en die daarom niet kunnen worden vertrouwd.

R4. Identiteitsdiefstal

Identiteitsdiefstal wordt gedefinieerd als de ongeoorloofde verwerving van de portemonnee-eenheid of het verlies van authenticatiefactoren die het mogelijk maken de identiteit van een persoon aan te nemen.

R5. Gegevensdiefstal

Gegevensdiefstal wordt gedefinieerd als de ongeoorloofde extractie van gegevens. Gegevensdiefstal houdt ook verband met bedreigingen, zoals het onderscheppen van gegevens (ongeoorloofd verzamelen van gegevens tijdens doorgifte) en gegevensontsleuteling (het ongeoorloofd decoderen van versleutelde gegevens), die in sommige gevallen waarschijnlijk zullen leiden tot openbaarmaking van gegevens (R6).

R6. Openbaarmaking van gegevens

Openbaarmaking van gegevens wordt gedefinieerd als het ongeoorloofd bekendmaken van persoonsgegevens, met inbegrip van bijzondere categorieën persoonsgegevens. Het risico op een inbreuk op de persoonlijke levenssfeer is zeer vergelijkbaar, wanneer dit risico wordt bekeken vanuit het oogpunt van de privacy en niet de veiligheid.

R7. Gegevensmanipulatie

Gegevensmanipulatie wordt gedefinieerd als het ongeoorloofd wijzigen van gegevens.

R8. Gegevensverlies

Gegevensverlies wordt gedefinieerd als de situatie waarin in de portemonnee opgeslagen gegevens verloren gaan door misbruik of kwaadwillige handelingen. Dit risico is vaak een secundair risico van gegevensmanipulatie (R7) of verstoring van de dienstverlening (R13), waarbij alle of een deel van de gegevens niet kunnen worden hersteld.

R9. Niet-toegestane transactie

Niet-toegestane transacties worden gedefinieerd als operationele activiteiten die worden uitgevoerd zonder toestemming of medeweten van de portemonneegebruiker. In veel gevallen kan een niet-toegestane transactie leiden tot identiteitsdiefstal (R4) of openbaarmaking van gegevens (R6). Ze houden ook verband met niet-toegestane transacties, zoals het misbruik van cryptografische sleutels.

R10. Manipulatie van transacties

Manipulatie van transacties wordt gedefinieerd als de ongeoorloofde wijziging van de activiteiten in de portemonnee. Manipulatie van transacties is een aanval op de integriteit en houdt verband met een inbreuk op de integriteit van gegevens.

R11. Afwijzing

Afwijzing wordt gedefinieerd als een situatie waarin een belanghebbende kan weigeren een actie uit te voeren of bij een transactie betrokken te zijn, en andere belanghebbenden niet over voldoende bewijs beschikken om dit te weerleggen.

R12. Openbaarmaking van transactiegegevens

Openbaarmaking van transactiegegevens wordt gedefinieerd als de openbaarmaking van informatie met betrekking tot informatie over een transactie tussen belanghebbenden.

R13. Verstoring van de dienstverlening

Verstoring van de dienstverlening wordt gedefinieerd als een onderbreking of verslechtering van de normale werking van de portemonnee. Een specifieke vorm van verstoring van de dienstverlening is de "user lock-out", waarbij een gebruiker geen toegang (meer) kan krijgen tot zijn account of zijn portemonnee.

R14. Toezicht

Toezicht, surveillance of monitoring wordt gedefinieerd als het onrechtmatig volgen of observeren van de activiteiten, de communicatie of de gegevens van een portemonneegebruiker. Toezicht houdt vaak verband met inferentie, wat wordt gedefinieerd als het afleiden van gevoelige of persoonlijke informatie uit ogenschijnlijk onschuldige gegevens.

DEEL II

Systeemgerelateerde risico's

Deze risico's worden niet gebruikt in de lijst van bedreigingen, aangezien zij gewoonlijk het gevolg zijn van meervoudige bedreigingen, die worden herhaald op een manier die het volledige systeem in gevaar brengt.

SR1. Grootschalig toezicht

Grootschalig toezicht wordt gedefinieerd als het volgen of observeren van de activiteiten van veel gebruikers via de communicatie of de gegevens van hun portemonnee. Grootschalig toezicht wordt vaak geassocieerd met toezicht (R14) en inferentie op mondiale schaal, waarbij informatie over veel gebruikers wordt gecombineerd om gevoelige of persoonsgegevens over gebruikers af te leiden of om statistische trends vast te stellen die kunnen worden gebruikt om nieuwe aanvallen voor te bereiden.

SR2. Reputatieschade

Reputatieschade wordt gedefinieerd als de schade die wordt toegebracht aan de reputatie van een organisatie of overheidsorgaan. Reputatieschade zal ook het gevolg zijn van andere risico's wanneer een inbreuk of incident in de media komt en de organisatie op ongunstige wijze wordt voorgesteld. Reputatieschade kan leiden tot verdere risico's, zoals verlies van vertrouwen als gevolg van gegronde twijfels van de gebruiker, en verlies van het ecosysteem wanneer het volledige ecosysteem bezwijkt.

SR3. Niet-naleving van de wettelijke voorschriften

Niet-naleving van de wettelijke voorschriften wordt gedefinieerd als een situatie waarin de toepasselijke wetgeving, voorschriften of normen niet kunnen worden nageleefd. In de context van portemonnees, waarvoor veiligheid en privacy van de oplossing wettelijke vereisten zijn, leiden alle bedreigingen waarschijnlijk tot een of andere vorm van niet-naleving van de wettelijke voorschriften.

DEEL III

Technische bedreigingen

De technische bedreigingen houden niet allemaal verband met specifieke risico's voor de portemonnees, omdat vele ervan middelen zijn die kunnen worden gebruikt om aanvallen uit te voeren waarbij sprake is of kan zijn van veel verschillende risico's.

TT1. Fysieke aanvallen

1.1. *Diefstal*

Diefstal wordt gedefinieerd als diefstal van apparaten die de goede werking van de portemonnee kunnen schaden (indien het apparaat wordt gestolen en de portemonnee-eenheid niet voldoende beschermd is). Dit kan bijdragen tot veel risico's, waaronder identiteitsdiefstal (R4), gegevensdiefstal (R5) en niet-toegestane transacties (R9).

1.2. *Lekken van informatie*

Lekken van informatie wordt gedefinieerd als de ongeoorloofde toegang, het openbaar maken of het delen van informatie na fysieke toegang tot de portemonnee. Dit kan met name bijdragen tot de openbaarmaking van gegevens (R6) en gegevensdiefstal (R5).

1.3. *Manipulatie*

Manipulatie wordt gedefinieerd als een schending van de integriteit van een of meer componenten van de portemonnee-eenheid of van de componenten die de portemonnee-eenheid nodig heeft, bv. het apparaat van de gebruiker of het besturingssysteem ervan. Dit kan met name bijdragen tot gegevensmanipulatie (R7), gegevensverlies (R8) en manipulatie van transacties (R10). Wanneer manipulatie gericht is op softwarecomponenten, kan dit tot veel risico's bijdragen.

TT2. Fouten en verkeerde configuraties

2.1. *Fouten bij het beheer van een IT-systeem*

Fouten bij het beheer van een IT-systeem worden gedefinieerd als het lekken of delen van informatie of schade, veroorzaakt door misbruik van IT-middelen door gebruikers (gebrek aan bekendheid met de functionaliteiten van de toepassing) of door onjuiste configuratie of beheer van IT-middelen.

2.2. *Fouten op toepassingsniveau of gebruiksfouten*

Fouten op toepassingsniveau of gebruiksfouten worden gedefinieerd als een storing in de werking van de toepassing als gevolg van een fout in de toepassing zelf of een fout van een van de gebruikers (portemonneegebruikers en vertrouwende partijen).

2.3. *Ontwikkelingsfouten en verkeerde systeemconfiguraties*

Ontwikkelingsfouten en verkeerde systeemconfiguraties worden gedefinieerd als storingen of kwetsbaarheden die worden veroorzaakt door slecht ontwikkelde of geconfigureerde IT-middelen of bedrijfsprocessen (ontoereikende specificaties van IT-producten, ontoereikende bruikbaarheid, onveilige interfaces, ongepaste beleids- en procedurestromen, ontwerpfouten).

TT3. Gebruik van onbetrouwbare middelen

Het gebruik van onbetrouwbare middelen wordt gedefinieerd als een activiteit die leidt tot onopzettelijke schade als gevolg van slecht gedefinieerde vertrouwensrelaties, zoals het vertrouwen van een aanbieder zonder dat voldoende zekerheid wordt geboden.

3.1. *Verkeerd gebruik of verkeerde configuratie van componenten van de portemonnee*

Een verkeerd gebruik of een verkeerde configuratie van componenten van de portemonnee wordt gedefinieerd als onopzettelijke schade aan componenten van portemonnees als gevolg van een verkeerd gebruik of een verkeerde configuratie door portemonneegebruikers of door onvoldoende opgeleide ontwikkelaars, of als gevolg van een gebrek aan aanpassing aan veranderingen in het dreigingslandschap, doorgaans het gebruik van kwetsbare componenten van derden of runtime-platforms.

TT4. Storing en uitval

4.1. *Storing of niet functioneren van apparatuur, apparaten of systemen*

Een storing of het niet functioneren van apparatuur wordt gedefinieerd als onopzettelijke schade aan IT-middelen als gevolg van een storing of het niet functioneren van apparatuur, met inbegrip van de infrastructuur van de aanbieder en de apparaten van de gebruiker.

4.2. *Uitval van middelen*

Uitval van middelen wordt gedefinieerd als een storing of het niet werken als gevolg van het niet beschikbaar zijn van dergelijke middelen, bijvoorbeeld onderdelen voor onderhoud.

4.3. *Uitval van ondersteunende diensten*

Uitval van ondersteunende diensten wordt gedefinieerd als een storing of het niet functioneren als gevolg van het niet beschikbaar zijn van ondersteunende diensten die nodig zijn voor de goede werking van het systeem, met inbegrip van netwerkconnectiviteit van de infrastructuur van de aanbieder en van de apparaten van de gebruiker.

TT5. Kwaadwillige handelingen

5.1. *Onderschepping van informatie*

Onderschepping van informatie wordt gedefinieerd als het verzamelen van informatie die bij de doorgifte onvoldoende is beveiligd, met inbegrip van “man-in-the-middle”-aanvallen.

5.2. *Phishing en spoofing*

Phishing wordt gedefinieerd als het verzamelen van informatie die door de gebruiker wordt verstrekt na een bedrieglijke interactie, vaak geassocieerd met spoofing van legitieme communicatiemiddelen en websites. Deze bedreigingen zijn gericht tegen de gebruiker en dragen doorgaans bij tot identiteitsdiefstal (R4) en niet-toegestane transacties (R9), vaak door middel van gegevensdiefstal (R5) of openbaarmaking van gegevens (R6).

5.3. *Herhaling van berichten*

Herhaling van berichten wordt gedefinieerd als het hergebruik van eerder onderschepte berichten om niet-toegestane transacties uit te voeren, vaak op protocolniveau. Deze technische bedreiging draagt voornamelijk bij tot niet-toegestane transacties, die vervolgens kunnen leiden tot andere risico’s, afhankelijk van de transactie.

5.4. *Bruteforceaanval*

Een bruteforceaanval wordt gedefinieerd als een inbreuk op de beveiliging, vaak de vertrouwelijkheid, door een groot aantal interacties uit te voeren totdat de reacties waardevolle informatie opleveren.

5.5. *Kwetsbaarheden in de software*

De dreiging in verband met kwetsbaarheden in de software is een inbreuk op de beveiliging door gebruik te maken van een kwetsbare plek in de componenten van de portemonnee of in de software- en hardwarecomponenten die bij de toepassing van de portemonnee worden gebruikt, met inbegrip van gepubliceerde en niet-gepubliceerde (zeroday)kwetsbaarheden.

5.6. *Aanvallen op de toeleveringsketen*

Een aanval op de toeleveringsketen wordt gedefinieerd als een inbreuk op de beveiliging door middel van aanvallen op de portemonneeaanbieder of zijn gebruikers om verdere aanvallen op de portemonnee zelf mogelijk te maken.

5.7. *Malware*

Malware wordt gedefinieerd als een inbreuk op de beveiliging door middel van kwaadwillige toepassingen die ongewenste en onrechtmatige acties op de portemonnee uitvoeren.

5.8. *Voorspelling van willekeurige getallen*

Voorspelling van willekeurige getallen wordt gedefinieerd als het mogelijk maken van bruteforceaanvallen door middel van een gedeeltelijke of volledige voorspelling van willekeurige gegenereerde getallen.

DEEL IV

Bedreigingen voor de portemonnees

Dit laatste deel bevat een selectie van typische bedreigingsscenario's die specifiek zijn voor de portemonnees en die in kaart worden gebracht op basis van de belangrijkste gerelateerde risico's van hoog niveau, zoals hiervoor vermeld. Deze lijst geeft aan welke bedreigingen moeten worden afgedekt, maar vormt geen uitputtende lijst van bedreigingen, die sterk afhankelijk is van de architectuur van de geselecteerde portemonnee-oplossing en van de ontwikkeling van het dreigingslandschap. Daarnaast kan de aanbieder van portemonnees bij de risicobeoordeling en de voorgestelde maatregelen alleen verantwoordelijk zijn voor de componenten die onder het toepassingsgebied van de certificering vallen (*).

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR1	Een aanvaller kan zonder gegronde reden pseudoniemen intrekken.	Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR2	Een aanvaller kan gefabriceerde elektronische identiteiten die niet bestaan, afgeven.	Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR3	Een aanvaller kan beginnen met het afgeven van niet-toegestane PID's.	Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR4	Een aanvaller kan een beheerder verzoeken een verkeerde PID-aanbieder in te voeren in de lijst van vertrouwde PID-aanbieders.	Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR5	Een aanvaller kan de dienst voor het bewijzen van identiteit op afstand omzeilen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR6	Een aanvaller kan de dienst voor het fysiek bewijzen van identiteit omzeilen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR7	Een aanvaller kan de dienst voor het bewijzen van identiteit in verband met het gebruik van een (gekwalificeerd) certificaat op afstand omzeilen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR8	Een aanvaller kan toegang krijgen tot een portemonnee die niet aan een persoon gebonden is.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR9	Een aanvaller kan technische en procedurele controles uitschakelen om verkeerde PID's aan te maken.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR10	Een aanvaller kan een nieuwe portemonnee activeren op een ongeldig beveiligd cryptografisch middel voor portemonnees.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)
TR11	Een aanvaller kan de dienst voor het bewijzen van identiteit in verband met het gebruik van bestaande eID-middelen omzeilen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transactie (R9)
TR12	Een aanvaller kan de verificatie door de PID-aanbieder dat de portemonnee door de gebruiker wordt gecontroleerd, omzeilen en een PID laten afgeven in een aangetaste portemonnee waar de aanvaller de controle over heeft.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transactie (R9)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR13	Een aanvaller kan een geldige PID krijgen in een ongeldige portemonnee-eenheid.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transactie (R9)
TR14	Een PID-aanbieder kan gefabriceerde identiteiten afgeven wanneer de identiteit verband houdt met een bestaande persoon.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transacties (R9)
TR15	Een aanvaller kan een PID koppelen aan de verkeerde portemonnee omdat de PID-aanbieder de PID niet aan de juiste portemonnee kan koppelen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transacties (R9)
TR16	Een aanvaller kan ervoor zorgen dat de gebruiker de activering van een nieuwe portemonnee(-instantie) waar de aanvaller de controle over heeft, goedkeurt, met daaropvolgende controle van attesteringen.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/Aanmaken of gebruiken van een valse elektronische identiteit (R2)/ Identiteitsdiefstal (R4)/Niet-toegestane transactie (R9)
TR17	Een aanvaller kan een PID van een andere staat afgeven om toegang te krijgen tot gegevens/digitale activa van de burgers waarop hij zijn aanval richt.	Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)/ Identiteitsdiefstal (R4)/Niet-toegestane transactie (R9)
TR18	Een aanvaller kan technische en procedurele controles uitschakelen om valse (gekwalificeerde) elektronische attesteringen van attributen aan te maken.	Aanmaken of gebruiken van valse attributen (R3)
TR19	Een aanvaller kan (gekwalificeerde) elektronische attesteringen van attributen weergeven die niet rechtsgeldig aan hem zijn afgegeven.	Aanmaken of gebruiken van valse attributen (R3)
TR20	Een aanvaller kan het cryptografisch koppelingsmechanisme van de portemonnee tussen de PID en een (gekwalificeerde) elektronische attestering van attributen die niet aan hem mag worden afgegeven, aanvallen.	Aanmaken of gebruiken van valse attributen (R3)
TR21	Een aanvaller kan een (gekwalificeerde) elektronische attestering van attributen gebruiken in een portemonnee, hoewel de fysieke tegenhanger ervan is verstreken of ongeldig is.	Aanmaken of gebruiken van valse attributen (R3)
TR22	Een aanvaller kan de verificatie door de aanbieder van de (gekwalificeerde) elektronische attesteringen dat de gebruiker controle heeft over de portemonnee omzeilen en een (gekwalificeerde) elektronische attestering van attributen laten afgeven in een aangetaste portemonnee waarover de aanvaller de controle heeft.	Aanmaken of gebruiken van valse attributen (R3)
TR23	Een aanvaller kan elektronische attesteringen van attributen vervalsen.	Aanmaken of gebruiken van valse attributen (R3)
TR24	Een aanvaller kan vervalste elektronische attesteringen van attributen in een portemonnee inbrengen.	Aanmaken of gebruiken van valse attributen (R3)
TR25	De portemonnee kan zonder goedkeuring van een gebruiker attributen weergeven aan een vertrouwende partij.	Openbaarmaking van gegevens (R6)
TR26	PID's, (gekwalificeerde) elektronische attesteringen van attributen of pseudoniemen kunnen aan een verkeerde vertrouwende partij worden weergegeven.	Openbaarmaking van gegevens (R6)
TR27	Een aanvaller kan een kwaadwillige verlenging van een elektronische attestering van attributen initiëren.	Openbaarmaking van gegevens (R6)
TR28	Een aanvaller kan een gebruiker ertoe brengen ten onrechte een verzoek om elektronische attesteringen van attributen goed te keuren (via phishing of een andere methode).	Openbaarmaking van gegevens (R6)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR29	Een aanvaller kan attributen van de portemonnee lekken en de portemonneegebruiker identificeren wanneer identificatie niet vereist/toegestaan is.	Openbaarmaking van gegevens (R6)
TR30	Een aanvaller kan technische en procedurele controles uitschakelen om gegevens te extraheren.	Openbaarmaking van gegevens (R6)
TR31	Een verzoek kan naar een aanvaller worden gelekt.	Openbaarmaking van gegevens (R6)
TR32	Een aanvaller kan kennis verkrijgen over het ingebed openbaarmakingsbeleid voor attributen en de attributen weergeven die in het huidige verzoek van portemonnee-eenheden aanwezig zijn.	Openbaarmaking van gegevens (R6)
TR33	Een aanvaller kan logboekgegevens of delen ervan achterhalen.	Openbaarmaking van gegevens (R6)
TR34	Een aanvaller kan achterhalen of een portemonnee is geïnstalleerd op hetzelfde apparaat dat hij gebruikt, of op een ander apparaat, en kan er informatie over achterhalen.	Openbaarmaking van gegevens (R6)
TR35	Een aanvaller kan een kennisfactor verkrijgen die wordt gebruikt om zich bij de beveiligde cryptografische toepassing voor portemonnees te authenticeren.	Openbaarmaking van gegevens (R6)
TR36	De elektronische attestering van attributen over een persoon die in meerdere transacties met een vertrouwende partij of tussen verschillende vertrouwende partijen wordt weergegeven, maakt het onbedoeld mogelijk om meerdere transacties aan de betrokken persoon te koppelen.	Openbaarmaking van gegevens (R6)
TR37	Een openbare lijst van ingetrokken attesteringen/ vertrouwende partijen kan informatie bevatten over het gebruik van de attestering door de gebruiker (bv. locatie, IP-adres enz.).	Openbaarmaking van gegevens (R6)
TR38	Aangezien vertrouwende partijen niet in staat zijn de toestemming van de gebruiker voor gedeelde attributen aan te tonen, kunnen zij de integriteit van logboekbestanden aantasten.	Openbaarmaking van gegevens (R6)
TR39	Een aanvaller kan onrechtmatig portemonneegebruikers traceren met behulp van unieke/traceerbare identificatiecodes.	Openbaarmaking van gegevens (R6)/Toezicht (R14)
TR40	Een vertrouwende partij die bestaat uit meerdere eenheden/ entiteiten die elk een ander toepassingsgebied hebben voor wat zij mogen opvragen/verwerken, kan gegevens opvragen en verwerken waarvoor zij geen rechtmatige gronden heeft.	Openbaarmaking van gegevens (R6)/Niet-toegestane transactie (R9)
TR41	Een aanvaller kan de integriteits- en authenticiteitscontroles van PID's door de portemonnee ondermijnen zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR42	Een aanvaller kan de uitvoering van controles door de portemonnee om de integriteit en authenticiteit van de gevraagde attributen te verifiëren, omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR43	Een aanvaller kan de uitvoering van controles door de portemonnee om alle gevraagde attributen van dezelfde gebruiker te verifiëren omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR44	Een aanvaller kan de uitvoering van controles door de portemonnee om na te gaan of de PID geldig is en afgegeven is door een vertrouwde PID-aanbieder, omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR45	Een aanvaller kan de uitvoering van controles door de portemonnee om na te gaan of een (gekwalificeerde) elektronische attestering van attributen geldig is en afgegeven is door een gekwalificeerde verlener van vertrouwensdiensten die is geregistreerd om die attestering af te geven, omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR46	Een aanvaller kan de uitvoering van controles door de portemonnee om na te gaan of de PID door de PID-aanbieder is ingetrokken, omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR47	Een aanvaller kan de uitvoering van controles door de portemonnee om na te gaan of de (gekwalificeerde) elektronische attestering van attributen door de aanbieder ervan is ingetrokken, omzeilen of ondermijnen, zodat deze altijd het gewenste resultaat geven.	Manipulatie van gegevens (R7)
TR48	Een aanvaller kan de inhoud van back-up- en herstelgegevens waarover uitsluitend de gebruiker controle zou moeten hebben, wijzigen.	Gegevensmanipulatie (R7)/Gegevensverlies (R8)
TR49	Een aanvaller kan de transactiegeschiedenis voor een bepaalde portemonnee-instantie wijzigen in de logboekbestanden.	Gegevensmanipulatie (R7)/Gegevensverlies (R8)
TR50	Een aanvaller kan de verbinding van de portemonnee naar vertrouwende partijen afluisteren.	Gegevensdiefstal (R5)/Openbaarmaking van gegevens (R6)
TR51	Een aanvaller kan een gebruiker ervan overtuigen persoonsgegevens (d.w.z. PID, elektronische attestering van attributen, pseudoniemen, elektronische handtekeningen, logboekbestanden en andere gegevens) te delen met de aanvaller of met een derde partij, terwijl de gebruiker niet van plan was dit te doen.	Gegevensdiefstal (R5)/Openbaarmaking van gegevens (R6)
TR52	Een aanvaller kan de transactiegeschiedenis van een bepaalde portemonnee-instantie lezen in de logboekbestanden.	Gegevensdiefstal (R5)/Openbaarmaking van gegevens (R6)
TR53	Een aanvaller kan cryptografische sleutels uit het cryptografische beveiligingsapparaat voor portemonnees exporteren of extraheren.	Gegevensdiefstal (R5)/Openbaarmaking van gegevens (R6)/Niet-toegestane transactie (R9)
TR54	Een aanvaller kan de inhoud van back-up- en herstelgegevens waarover uitsluitend de gebruiker controle zou moeten hebben, lezen.	Gegevensdiefstal (R5)/Openbaarmaking van gegevens (R6)
TR55	Een aanvaller kan de gebruikersauthenticatiemethode omzeilen om een pseudoniem te gebruiken dat door een portemonnee-eenheid wordt gegenereerd.	Identiteitsdiefstal (R4)
TR56	Een aanvaller kan aan gebruikers een toepassing voorstellen die een specifieke legitieme portemonnee nabootst.	Identiteitsdiefstal (R4)
TR57	Een aanvaller kan gegevens over portemonnees, waaronder PID, attesteringen of logboeken, exporteren.	Identiteitsdiefstal (R4)
TR58	Een aanvaller kan cryptografische bindingen exporteren.	Identiteitsdiefstal (R4)
TR59	Een aanvaller kan identiteiten overnemen via de cryptografische sleutels van de portemonnee.	Identiteitsdiefstal (R4)
TR60	Een aanvaller kan de persoonlijke portemonnee-eenheid van een andere gebruiker op zijn persoonlijke apparaat dupliceren en gebruiken.	Identiteitsdiefstal (R4)/Aanmaken of gebruiken van een bestaande elektronische identiteit (R1)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR61	De autoriteiten van een andere staat kunnen de gebruiker verzoeken alle gegevens van de portemonnee te tonen en/of te delen als hij in de buurt is, bijvoorbeeld bij het passeren van de grens van die staat.	Identiteitsdiefstal (R4)/Toezicht (R14)
TR62	Gebruikers kunnen hun transactielogboeken niet overdragen na een storing van een apparaat van de gebruiker, wat leidt tot een verlies van traceerbaarheid van eerdere transacties op de nieuwe portemonnee.	Afwijzing (R11)
TR63	Gebruikers kunnen hun transactielogboeken niet herstellen na een storing van een apparaat van de gebruiker, wat leidt tot een verlies van traceerbaarheid van eerdere transacties op de nieuwe portemonnee.	Afwijzing (R11)
TR64	Vertrouwende partijen kunnen moeite hebben om aan te tonen dat ze toestemming hebben verkregen voor elektronische handtekeningen op afstand.	Afwijzing (R11)
TR65	Een aanvaller kan tijdens het verbinden met vertrouwende partijen de verbinding(en) overspoelen met verzoeken.	Verstoring van de dienstverlening (R13)
TR66	Een aanvaller kan een dienst die statusgegevens afgeeft, overspoelen met verbindingen met vertrouwende partijen.	Verstoring van de dienstverlening (R13)
TR67	Een aanvaller kan het attribuut laten weergeven alsof het betwist/ontkend is, ofschoon de weergave van het attribuut de geldigheid ervan aangeeft.	Verstoring van de dienstverlening (R13)
TR68	Een aanvaller kan een PID zonder gegronde reden intrekken.	Verstoring van de dienstverlening (R13)
TR69	Een aanvaller kan een PID zonder toestemming van de gebruiker intrekken.	Verstoring van de dienstverlening (R13)
TR70	Een aanvaller kan een (gekwalificeerde) elektronische attestering van attributen zonder gegronde reden intrekken.	Verstoring van de dienstverlening (R13)
TR71	Een aanvaller kan een (gekwalificeerde) elektronische attestering van attributen intrekken zonder toestemming van de gebruiker.	Verstoring van de dienstverlening (R13)
TR72	Een aanvaller kan meerdere verzoeken tot identificatie indienen zonder dat deze als opzettelijk weesverzoeken worden erkend.	Verstoring van de dienstverlening (R13)
TR73	Een aanvaller kan meerdere verzoeken zonder vervolgtransactie verzenden.	Verstoring van de dienstverlening (R13)
TR74	Een aanvaller kan een vertrouwende partij in staat stellen te verzoeken om identificatie zonder bijbehorende identificatie (reactie) of volledige controle.	Verstoring van de dienstverlening (R13)
TR75	Een aanvaller kan na de time-out een reactie op een verzoek sturen, of soortgelijke situaties die tot een verstoring van de dienstverlening leiden.	Verstoring van de dienstverlening (R13)
TR76	Een vertrouwende partij kan meerdere ongeldige verzoeken verzenden.	Verstoring van de dienstverlening (R13)
TR77	Een aanvaller kan meerdere ongeldige verzoeken naar een aanbieder van portemonnees sturen.	Verstoring van de dienstverlening (R13)
TR78	Een aanvaller kan ervoor zorgen dat een lidstaat een niet-vertrouwde PID-aanbieder niet kan schrappen uit de lijst van vertrouwde PID-aanbieders.	Verstoring van de dienstverlening (R13)
TR79	Een aanvaller kan opschorting of intrekking van een portemonnee voorkomen.	Verstoring van de dienstverlening (R13)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR80	Een aanvaller kan transacties door vertrouwende partijen, gebruikers en/of PID-aanbieders blokkeren.	Verstoring van de dienstverlening (R13)
TR81	Een aanvaller kan een beveiligd cryptografisch middel voor portemonnees uitschakelen of onbeschikbaar maken.	Verstoring van de dienstverlening (R13)
TR82	Een aanvaller kan ervoor zorgen dat de PID-aanbieder niet in staat is PID's in te trekken of op te schorten.	Verstoring van de dienstverlening (R13)/ Niet-toegestane transactie (R9)
TR83	Een vertrouwende partij kan meer identiteitsgegevens van de gebruiker afleiden dan de gegevens die met de partij worden gedeeld.	Toezicht (R14)
TR84	Samenspannende vertrouwende partijen of PID-aanbieders kunnen meer identiteitsgegevens van de gebruiker afleiden dan de bij hen bekende gegevens.	Toezicht (R14)
TR85	Een aanvaller kan een gebruiker traceren en volgen aan de hand van persoonsidentificatiegegevens van de gebruiker als identificatie van de gebruiker niet vereist is.	Toezicht (R14)
TR86	Een aanvaller kan een "vervalste" weergave van combinaties van (gekwalificeerde) elektronische attesteringen van attributen maken.	Manipulatie van transacties (R10)
TR87	Een aanvaller kan de portemonnee op afstand activeren/ overnemen (bv. een bank-app waarin een authenticatie- of attesteringsverzoek is geïntegreerd) zonder de uitdrukkelijke toestemming of uitsluitende controle van de gebruiker, in gevallen waarin de gebruiker daar niet van op de hoogte is (bv. omdat hij slaapt) of de vertrouwende partij niet kan zien.	Manipulatie van transacties (R10)
TR88	Aanvallers kunnen wijzigingen aanbrengen in de metagegevens van een verzoek (naam van de dienst, gebruik enz.).	Manipulatie van transacties (R10)
TR89	Aanvallers kunnen wijzigingen aanbrengen in de responsinformatie (servicestatus, nonce enz.).	Manipulatie van transacties (R10)
TR90	Aanvallers kunnen wijzigingen aanbrengen in de informatie over de attributen van een verzoek (overvragen enz.).	Manipulatie van transacties (R10)
TR91	Een vertrouwende partij kan elementen van een vorige sessie in een andere sessie herhalen.	Manipulatie van transacties (R10)
TR92	Een aanvaller kan de PID vervangen of wijzigen tijdens de overdracht ervan van de PID-aanbieder naar de portemonnee-eenheid.	Manipulatie van transacties (R10)
TR93	Een aanvaller kan de PID vervangen of wijzigen tijdens de overdracht ervan van de portemonnee-eenheid naar de online vertrouwende partij.	Manipulatie van transacties (R10)
TR94	Een aanvaller kan de PID vervangen of wijzigen tijdens de overdracht ervan van de portemonnee-eenheid naar de offline vertrouwende partij.	Manipulatie van transacties (R10)
TR95	Een aanvaller kan een PID afgeven zonder toestemming van de gebruiker.	Niet-toegestane transactie (R9)
TR96	Een aanvaller kan gebruikmaken van ingetrokken of ongeldig ingebed openbaarmakingsbeleid, mogelijk zonder medeweten van de vertrouwende partijen.	Niet-toegestane transactie (R9)
TR97	Een aanvaller kan de portemonnee ertoe aanzetten verkeerde elektronische handtekeningen te verifiëren.	Niet-toegestane transactie (R9)
TR98	Een aanvaller kan de portemonnee gebruiken zonder dat de gebruiker daar controle over heeft.	Niet-toegestane transactie (R9)

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR99	Een aanvaller kan een gebruiker ervan overtuigen transacties met een aanvaller of onbevoegde derde te authenticeren en goed te keuren.	Niet-toegestane transactie (R9)
TR100	Een aanvaller kan een gebruiker een elektronische handtekening laten plaatsen zonder de inhoud aan de gebruiker weer te geven of na verkeerde inhoud te hebben weergegeven.	Niet-toegestane transactie (R9)
TR101	Een aanvaller kan de toegangscontrole voor het account van de gebruiker bij de aanbieder van portemonnees omzeilen.	Niet-toegestane transactie (R9)
TR102	Een aanvaller kan tijdens verbinden met vertrouwende partijen de identiteit van de vertrouwende partijen aannemen.	Niet-toegestane transactie (R9)/Openbaarmaking van gegevens (R6)
TR103	De gebruiker achter de verbinding tussen de vertrouwende partij en de browser kan verschillen van de gebruiker achter de verbinding tussen de vertrouwende partij en de portemonnee.	Niet-toegestane transactie (R9)/Openbaarmaking van gegevens (R6)/Identiteitsdiefstal (R4)
TR104	Een aanvaller kan de gebruiker ervan overtuigen de portemonnee van de gebruiker zonder reden in te trekken.	Niet-toegestane transactie (R9)/Verstoring van de dienstverlening (R13)
TR105	Een aanvaller kan "man-in-the-middle"-aanvallen uitvoeren.	Niet-toegestane transactie (R9)/Openbaarmaking van gegevens (R6)/Toezicht (R14)
TR106	Een aanvaller kan ongeldige of ingetrokken attributen weergeven van een portemonnee die niet regelmatig op het netwerk is aangesloten.	Effect voor verschillende risico's
TR107	Een aanvaller kan informatie van een gebruiker stelen door spoofing van een portemonnee.	Effect voor verschillende risico's
TR108	Een aanvaller kan de identiteit van de gebruiker aannemen door een verzoek om gegevens (bv. authenticatie) te herhalen of imiteren, dat er geldig uitziet.	Effect voor verschillende risico's
TR109	Een aanvaller kan ingebed openbaarmakingsbeleid ten aanzien van een gebruiker herhalen om een goedgekeurd verzoek na te bootsen.	Effect voor verschillende risico's
TR110	Een aanvaller kan misbruik maken van het gebrek aan informatie van portemonneegebruikers, of van onnodige vertragingen, na een inbreuk op of schending van de beveiliging.	Effect voor verschillende risico's
TR111	Een aanvaller kan een eerder geïnstalleerde rechtmatige portemonnee-instantie wijzigen om kwaadwillige kenmerken toe te voegen.	Effect voor verschillende risico's
TR112	Een aanvaller kan een rechtmatige portemonnee-instantie wijzigen en het als rechtmatige portemonnee-instantie aan gebruikers voorstellen.	Effect voor verschillende risico's
TR113	Een aanvaller kan het gebruikersauthenticatiemechanisme zelf uitschakelen om de authenticatie van de portemonneegebruiker te omzeilen.	Effect voor verschillende risico's
TR114	Een aanvaller kan kwaadwillige codes of backdoors (achterdeurtjes) in de portemonneecode invoeren tijdens het inzetten ervan op het apparaat van de gebruiker.	Effect voor verschillende risico's
TR115	Een aanvaller kan tijdens de ontwikkeling kwaadwillige codes of backdoors in de portemonneecode invoeren.	Effect voor verschillende risico's
TR116	Een aanvaller kan het genereren van willekeurige getallen manipuleren om de entropie ervan voldoende te verminderen om aanvallen mogelijk te maken.	Effect voor verschillende risico's

ID *Identificatiecode*	Beschrijving van de bedreiging *Beschrijving van de vastgestelde bedreiging (*)*	Risico *Gerelateerde risico's*
TR117	Een aanvaller kan apparaten van gebruikers in de toeleveringsketen manipuleren door codes of configuraties op te nemen die niet voldoen aan de voorwaarden voor het gebruik van de portemonnee.	Effect voor verschillende risico's
TR118	Een aanvaller kan een portemonnee-eenheid activeren met behulp van een vervalst beveiligd cryptografisch middel voor portemonnees die door de aanvallers wordt aangestuurd.	Effect voor verschillende risico's
TR119	Een aanvaller kan informatie lezen die naar de beveiligde cryptografische toepassing voor portemonnees en/of het cryptografische beveiligingsapparaat voor portemonnees is gestuurd.	Effect voor verschillende risico's
TR120	Een aanvaller kan willekeurige informatie naar de beveiligde cryptografische toepassing voor portemonnees sturen.	Effect voor verschillende risico's
TR121	Een aanvaller kan informatie stelen door de uitwisselingen tussen de beveiligde cryptografische toepassing voor portemonnees en het beveiligd cryptografisch middel voor portemonnees te onderscheppen.	Effect voor verschillende risico's
TR122	Een aanvaller kan willekeurige informatie naar het beveiligd cryptografisch middel voor portemonnees sturen.	Effect voor verschillende risico's
TR123	Een aanvaller kan informatie naar het beveiligd cryptografisch middel voor portemonnees sturen en de beveiligde cryptografische toepassing voor portemonnees omzeilen.	Effect voor verschillende risico's
TR124	Een aanvaller kan phishing gebruiken om gebruikers toegang te geven tot een vervalste portemonnee en een webtoepassing voor PID-beheer.	Effect voor verschillende risico's
TR125	Een aanvaller kan de sleutels van een portemonnee vervangen door andere sleutels om berichten te creëren die bij een andere aanval kunnen worden gebruikt.	Effect voor verschillende risico's
TR126	Een aanvaller kan de sleutels van een portemonnee wijzigen of vernietigen, waardoor sommige functies van de portemonnee onbruikbaar worden.	Effect voor verschillende risico's
TR127	Een aanvaller kan malware aansturen om toegang te krijgen tot in de portemonnee opgeslagen gegevens.	Effect voor verschillende risico's
TR128	Een aanvaller heeft toegang tot bewijsmateriaal dat in de portemonnee is gegenereerd.	Effect voor verschillende risico's
TR129	Portemonneeaanbieders hebben toegang tot objecten in de portemonnee.	Effect voor verschillende risico's
TR130	Portemonneeaanbieders hebben toegang tot bewijsmateriaal dat in de portemonnee is gegenereerd.	Effect voor verschillende risico's
TR131	Een aanvaller kan een onvergrendeld portemonneeapparaat stelen.	Effect voor verschillende risico's
TR132	Een aanvaller kan het systeem manipuleren om te voorkomen dat bepaalde gebeurtenissen worden geregistreerd.	Effect voor verschillende risico's
TR133	Een aanvaller kan de communicatie tussen de portemonnee-instantie en de beveiligde cryptografische toepassing voor portemonnees onderscheppen of een gebruiker herhalen/nabootsen (bv. door het authenticatiemechanisme te kapen).	Effect voor verschillende risico's

BIJLAGE II

CRITERIA VOOR DE BEOORDELING VAN DE AANVAARDBAARHEID VAN ZEKERHEIDSINFORMATIE

Benaming	Onderwerp	Aandachtspunten
EUCC	ICT-producten	Over de afgevende instantie: geen (geaccrediteerde certificerende instanties) Over het toepassingsgebied: — Controleer het beveiligingsprofiel en de beveiligingsdoelstelling — Controleer het betrouwbaarheidsniveau van de evaluatie en de uitbreidingen Over de zekerheid: — Controleer beperkingen in de gebruikersdocumentatie — Voor de samenstelling kan toegang tot het technische evaluatieverslag worden verlangd
EUCS (indien beschikbaar)	Clouddiensten	Over de afgevende instantie: geen (geaccrediteerde certificerende instanties) Over het toepassingsgebied: — Controleer de beschrijving van de clouddienst — Controleer het evaluatieniveau en de uitbreidingsprofielen Over de zekerheid: — Controleer de transparantie-informatie en, indien nodig, de informatie over de samenstelling
Gemeenschappelijke criteria-regelingen die in de EU worden toegepast, met inbegrip van SOG-IS-regelingen	ICT-producten	Over de afgevende instantie: geen (lidstaten) Over het toepassingsgebied: — Controleer het beveiligingsprofiel en de beveiligingsdoelstelling — Controleer het betrouwbaarheidsniveau van de evaluatie en de uitbreidingen Over de zekerheid: — Controleer beperkingen in de gebruikersdocumentatie — Voor de samenstelling kan toegang tot het technische evaluatieverslag worden verlangd
EN 17640:2018 (FITCEM, met inbegrip van CSPN, BSZ, LINCE, BSZA)	ICT-producten	Over de afgevende instantie: — Controleer de regeling en de vereisten voor certificerende instanties Over het toepassingsgebied: — Controleer de productbeschrijving — Controleer de veiligheidsclaims — Controleer het betrouwbaarheidsniveau Over de zekerheid: — Controleer de uitgevoerde activiteiten en de bevindingen in het verslag
Certificeringsregelingen voor gekwalificeerde middelen voor het aanmaken van handtekeningen overeenkomstig artikel 30 van Verordening (EU) nr. 910/2014	QSCD	Over de afgevende instantie: — Controleer de regeling en de vereisten voor certificerende instanties Over het toepassingsgebied: — Controleer de productbeschrijving — Controleer de veiligheidsclaims — Controleer het betrouwbaarheidsniveau Over de zekerheid: — Controleer de uitgevoerde activiteiten

Benaming	Onderwerp	Aandachtspunten
EN ISO/IEC 27001:2022	ISMS	Over de afgevende instantie: geen (geaccrediteerde certificerende instanties) Over het toepassingsgebied: — Controleer de beschrijving van het beheersysteem — Controleer de toepasbaarheidsverklaring Over de zekerheid: — Controleer de uitgevoerde activiteiten
SOC2	Organisaties	Over de afgevende instantie: — Controleer de status van hun accountant Over het toepassingsgebied: — Controleer de managementverklaring en de beschrijving van de controles — Controleer de toepasbaarheidsverklaring Over de zekerheid: — Controleer de bevindingen in het verslag — Controleer overbruggingsbrieven indien nodig
MDSCert (GSMA) (indien beschikbaar)	Mobiele apparaten	Over de afgevende instantie: — Controleer de vereisten voor certificerende instanties Over het toepassingsgebied: — Controleer het betrouwbaarheidsniveau van de beveiliging — Controleer de vereisten van de regeling Over de zekerheid: — Controleer de activiteiten en bevindingen in het verslag
Andere regelingen	Alle componenten	Over de regeling: — Controleer de relevantie en bepalingen van de regeling Over de afgevende instantie: — Controleer de vereisten voor certificerende instanties Over het toepassingsgebied: — Controleer de vereisten van de regeling — Controleer de beveiligingsdoelstelling of soortgelijk document waarin de functionele en zekerheidsvereisten voor de beveiliging worden beschreven — Controleer de productbeschrijving en de geselecteerde functionele vereisten voor de beveiliging Over de zekerheid: — Controleer de activiteiten en bevindingen in het verslag

BIJLAGE III

FUNCTIONELE VEREISTEN VOOR PORTEMONNEE-OPLOSSINGEN

Overeenkomstig artikel 5 bis, leden 4, 5, 8 en 14, van Verordening (EU) nr. 910/2014 bevatten de functionele criteria waaraan een gecertificeerde portemonnee-oplossing moet voldoen en het stelsel voor elektronische identificatie in het kader waarvan deze wordt verstrekte, de functionele vereisten voor de hierna vermelde handelingen:

1) Uitvoeringsverordening (EU) 2024/2979 van de Commissie ([1]) tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten,

2) Uitvoeringsverordening (EU) 2024/2982 van de Commissie ([2]) tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de protocollen en interfaces die moeten worden ondersteund door het Europees kader voor digitale identiteit,

3) Uitvoeringsverordening (EU) 2024/2977 van de Commissie ([3]) tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de persoonsidentificatiegegevens en elektronische attesteringen van attributen, afgegeven voor de Europese portemonnee voor digitale identiteit.

([1]) Uitvoeringsverordening (EU) 2024/2979 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit (PB L, 2024/2979, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Uitvoeringsverordening (EU) 2024/2982 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de protocollen en interfaces die moeten worden ondersteund door het Europees kader voor digitale identiteit (PB L, 2024/2982, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Uitvoeringsverordening (EU) 2024/2977 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de persoonsidentificatiegegevens en elektronische attesteringen van attributen, afgegeven voor de Europese portemonnee voor digitale identiteit (PB L, 2024/2977, 4.12.2024, ELI: https://data.europa.eu/eli/reg_impl/2024/2977/oj).

BIJLAGE IV

METHODEN EN PROCEDURES VOOR EVALUATIEACTIVITEITEN

1. **Controle van de uitvoering van een portemonnee-oplossing**

Een conformiteitsbeoordelingsactiviteit bestaat uit het selecteren van specifieke evaluatieactiviteiten.

In de nationale certificeringsregelingen moet een evaluatieactiviteit worden gespecificeerd om de verstrekte informatie te beoordelen, die ten minste het volgende omvat:

a) een analyse van de verstrekte informatie om te bevestigen dat deze geschikt is voor een van de in de nationale certificeringsregelingen gespecificeerde architecturen;

b) een analyse van de dekking van de cyberbeveiligingsrisico's en -bedreigingen die in het risicoregister van bijlage I zijn vastgesteld door middel van de beschreven beveiligingscontroles.

De in de punten a) tot en met b) bedoelde analyse berust op de door de aanbieder van portemonnees verstrekte motivering en onderbouwing.

2. **Evaluatieactiviteiten in verband met de cryptografisch beveiligingsapparaten voor portemonnees**

1) Kritieke handelingen, met inbegrip van cryptografische berekeningen, hoeven niet volledig te worden uitgevoerd in het cryptografische beveiligingsapparaat voor portemonnees. Het deel dat in het cryptografische beveiligingsapparaat voor portemonnees wordt toegepast als onderdeel van de portemonnee-oplossing, moet echter de bescherming waarborgen van de kritieke handelingen die het uitvoert tegen aanvallen door aanvallers met een hoog aanvalspotentieel, overeenkomstig Uitvoeringsverordening (EU) 2015/1502 van de Commissie ([1]).

2) Het cryptografische beveiligingsapparaat voor portemonnees of een deel ervan kan binnen het voorwerp van de certificering vallen als het wordt verstrekte door de certificaathouder of de aanvrager, of buiten het toepassingsgebied ervan als het is opgenomen in een door de eindgebruiker geleverd apparaat. Daarnaast worden in de nationale certificeringsregelingen de evaluatieactiviteiten gespecificeerd om de geschiktheid van het cryptografische beveiligingsapparaat voor portemonnees te verifiëren, in de volgende twee gevallen:

   a) indien de beveiligde cryptografische toepassing voor portemonnees afhankelijk is van het specifieke cryptografische beveiligingsapparaat voor portemonnees (d.w.z. of deze moet worden beoordeeld als een samengesteld product op basis van het cryptografische beveiligingsapparaat voor portemonnees), moet de evaluatie van de beveiligde cryptografische toepassing voor portemonnees toegang vereisen tot aanvullende informatie met betrekking tot de certificering van het cryptografische beveiligingsapparaat voor portemonnees, waaronder met name het technische evaluatieverslag;

   b) indien voor een architectuur die in de regeling in aanmerking wordt genomen, gebruik wordt gemaakt van verschillende beveiligde cryptografische middelen voor portemonnees, of indien sommige activiteiten met betrekking tot kritieke activa buiten het cryptografische beveiligingsapparaat voor portemonnees worden uitgevoerd, omvat de nationale certificeringsregelingen evaluatieactiviteiten om ervoor te zorgen dat de algemene oplossing het verwachte beveiligingsniveau biedt.

3) Als voorwaarde voor de certificering in het kader van nationale certificeringsregelingen moet het cryptografische beveiligingsapparaat voor portemonnees worden beoordeeld aan de hand van de vereisten van het betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502.

   Wanneer aan de voorwaarden van artikel 3, lid 3, punt b), is voldaan, moet de evaluatie van het cryptografische beveiligingsapparaat voor portemonnees of een deel ervan bestaan uit een kwetsbaarheidsbeoordeling zoals vastgesteld in ISO/IEC EN 15408-3:2022 op niveau AVA_VAN.5, zoals vastgesteld in bijlage I bij Uitvoeringsverordening (EU) 2024/482 van de Commissie ([2]), tenzij naar behoren aan de certificerende instantie wordt gemotiveerd dat de beveiligingskenmerken van de beveiligde cryptografische toepassing voor portemonnees het mogelijk maken een lager beoordelingsniveau te gebruiken met behoud van hetzelfde algemene betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502.

([1]) 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 (PB L 235 van 9.9.2015, blz. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Uitvoeringsverordening (EU) 2024/482 van de Commissie van 31 januari 2024 houdende uitvoeringsbepalingen van Verordening (EU) 2019/881 van het Europees Parlement en de Raad wat betreft de vaststelling van de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling (EUCC) (PB L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) Daarnaast worden in de nationale certificeringsregelingen in de documentatie met betrekking tot elke specifieke architectuur veronderstellingen voor deze evaluatie van het beveiligd cryptografisch middel voor portemonnees geformuleerd, op grond waarvan weerstand kan worden geboden tegen aanvallers met een hoog aanvalspotentieel overeenkomstig Uitvoeringsverordening (EU) 2015/1502 van de Commissie, en worden de evaluatieactiviteiten gespecificeerd om deze veronderstellingen te bevestigen, en na afgifte van het certificaat te bevestigen dat de veronderstellingen nog steeds zijn geverifieerd. In de nationale regelingen worden de certificeringskandidaten ook verplicht om deze veronderstellingen te verfijnen met het oog op de specifieke uitvoering ervan en om een beschrijving te geven van de maatregelen die zijn genomen om te garanderen dat de veronderstellingen gedurende de hele certificeringscyclus worden geverifieerd.

5) In alle gevallen omvatten de nationale certificeringsregelingen een evaluatieactiviteit om na te gaan of de voor het beveiligd cryptografisch middel voor portemonnees beschikbare zekerheidsinformatie geschikt is voor het doel van de portemonnee-oplossing, door middel van een analyse van de zekerheidsinformatie, zoals de beveiligingsdoelstelling voor EUCC-certificaten, met inbegrip van de volgende activiteiten:

   a) verifiëren dat het toepassingsgebied van de evaluatie geschikt is, wat voor EUCC-certificaten bijvoorbeeld betekent dat wordt nagegaan of de beveiligingsdoelstelling in overeenstemming is met een van de in de EUCC aanbevolen beveiligingsprofielen;

   b) verifiëren of de veronderstellingen over de operationele omgeving verenigbaar zijn met de portemonnee-oplossing, wat bijvoorbeeld voor EUCC-certificaten betekent dat deze veronderstellingen in de beveiligingsdoelstelling kunnen worden gevonden;

   c) verifiëren of de aanbevelingen in de gebruikershandleiding of documentatie verenigbaar zijn met de voorwaarden waaronder het cryptografische beveiligingsapparaat voor portemonnees in de portemonnee-oplossing moet worden gebruikt;

   d) verifiëren of de veronderstellingen in de nationale certificeringsregeling met betrekking tot beveiligde cryptografische middelen voor portemonnees worden geverifieerd en behandeld in de zekerheidsinformatie.

6) In gevallen waarin sommige verificaties niet volledig sluitend zijn, stellen de certificerende instanties volgens de nationale certificeringsregelingen in de evaluatie van de beveiligde cryptografische toepassing voor portemonnees compensatievereisten vast voor de beveiligde cryptografische toepassing voor portemonnees op basis van het cryptografische beveiligingsapparaat voor portemonnees. Indien dit niet mogelijk is, achten de nationale certificeringsregelingen het cryptografische beveiligingsapparaat voor portemonnees ongeschikt, wat betekent dat aan de portemonnee-oplossing geen certificaat van overeenstemming mag worden afgegeven.

3. **Evaluatieactiviteiten in verband met de beveiligde cryptografische toepassing voor portemonnees**

1) In de nationale certificeringsregelingen wordt vereist dat een beveiligde cryptografische toepassing voor portemonnees, als onderdeel van een portemonnee-oplossing, wordt beoordeeld aan de hand van de vereisten van ten minste het betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502.

2) Deze evaluatie bestaat uit een kwetsbaarheidsbeoordeling, zoals uiteengezet in ISO/IEC EN 15408-3:2022 op het niveau AVA_VAN.5, zoals vastgesteld in bijlage I bij Uitvoeringsverordening (EU) 2024/482, tenzij ten aanzien van de certificerende instantie naar behoren wordt gemotiveerd dat de beveiligingskenmerken van de beveiligde cryptografische toepassing voor portemonnees het toestaan een lager beoordelingsniveau te gebruiken met behoud van hetzelfde algemene betrouwbaarheidsniveau "hoog" in de zin van Uitvoeringsverordening (EU) 2015/1502.

3) Als de beveiligde cryptografische toepassing voor portemonnees niet door de aanbieder van portemonnees wordt verstrekt, formuleren de nationale certificeringsregelingen veronderstellingen voor deze evaluatie van de beveiligde cryptografische toepassing voor portemonnees, op grond waarvan weerstand kan worden geboden tegen aanvallers met een hoog aanvalspotentieel overeenkomstig Uitvoeringsverordening (EU) 2015/1502, en worden de evaluatieactiviteiten gespecificeerd om deze veronderstellingen te bevestigen, en na afgifte van het certificaat te bevestigen dat de veronderstellingen nog steeds zijn geverifieerd. In de nationale regelingen worden de certificeringskandidaten ook verplicht om deze veronderstellingen te verfijnen met het oog op de specifieke uitvoering ervan en om een beschrijving te geven van de maatregelen die zijn genomen om te garanderen dat de veronderstellingen gedurende de hele certificeringscyclus worden geverifieerd.

4) In alle gevallen omvatten de nationale certificeringsregelingen een evaluatieactiviteit om na te gaan of de voor de beveiligde cryptografische toepassing voor portemonnees beschikbare zekerheidsinformatie geschikt is voor het doel van de portemonnee-oplossing, door middel van een analyse van de zekerheidsinformatie, zoals de beveiligingsdoelstelling voor EUCC-certificaten, met inbegrip van de volgende activiteiten:

   a) verifiëren dat het toepassingsgebied van de evaluatie geschikt is, wat voor EUCC-certificaten bijvoorbeeld betekent dat wordt nagegaan of de beveiligingsdoelstelling in overeenstemming is met een van de in de EUCC aanbevolen beveiligingsprofielen;

   b) verifiëren of de veronderstellingen over de operationele omgeving verenigbaar zijn met de portemonnee-oplossing, wat bijvoorbeeld voor EUCC-certificaten betekent dat deze veronderstellingen in de beveiligingsdoelstelling kunnen worden gevonden;

c) verifiëren of de aanbevelingen in de gebruikershandleiding of documentatie verenigbaar zijn met de voorwaarden waaronder de beveiligde cryptografische toepassing voor portemonnees in de portemonnee-oplossing moet worden gebruikt;

d) verifiëren of de veronderstellingen in de nationale certificeringsregeling met betrekking tot beveiligde cryptografische toepassingen voor portemonnees worden geverifieerd en behandeld in de zekerheidsinformatie.

5) In de nationale certificeringsregelingen wordt vereist dat de evaluatie van de beveiligde cryptografische toepassing voor portemonnees betrekking heeft op alle beveiligingscontroles die door deze beveiligde cryptografische toepassing voor portemonnees worden uitgevoerd.

4. **Evaluatieactiviteiten in verband met het apparaat van de eindgebruiker**

Aangezien in het risicoregister, zoals beschreven in bijlage I bij deze verordening, risico's worden vastgesteld die rechtstreeks verband houden met de veiligheid van het apparaat van de eindgebruiker, moeten in de nationale certificeringsregelingen beveiligingsvereisten voor apparaten van eindgebruikers worden gespecificeerd. Aangezien deze apparaten echter door de eindgebruiker worden geleverd en niet door de aanbieder van portemonnees, worden hiervoor veronderstellingen gedaan.

Voor elke veronderstelling moet de portemonnee-oplossing een mechanisme omvatten om per portemonnee-eenheid te controleren of de onderliggende eindgebruiker aan de veronderstelling voldoet. Dergelijke mechanismen worden beschouwd als beveiligingscontroles en vallen onder evaluatieactiviteiten om de geschiktheid en de doeltreffendheid op het passende betrouwbaarheidsniveau aan te tonen.

Hier volgen twee voorbeelden:

a) een apparaat van de eindgebruiker kan een gecertificeerd beveiligd cryptografisch middel voor portemonnees bevatten, wat moet worden aangetoond. Dit zou doorgaans gebeuren door gebruik te maken van een cryptografisch mechanisme om na te gaan of het gecertificeerde cryptografische beveiligingsapparaat voor portemonnees een cryptografisch geheim bevat dat alleen beschikbaar is in het gecertificeerde cryptografische beveiligingsapparaat voor portemonnees. In dat geval moet dit cryptografische geheim worden beschouwd als een kritiek middel en onder de certificering van het cryptografische beveiligingsapparaat voor portemonnees en/of de beveiligde cryptografische toepassing voor portemonnees vallen;

b) een typisch vereiste voor apparaten van de eindgebruiker is dat de apparaten beveiligingsupdates moeten ontvangen. Aangezien dit vereiste verband houdt met de portemonnee-instantie, hoeft het mechanisme dat wordt gebruikt om de beschikbaarheid van beveiligingsupdates te verifiëren alleen te worden gedekt door evaluatieactiviteiten met een betrouwbaarheidsniveau dat geschikt is voor de portemonnee-instantie, met name omdat het waarschijnlijk in de portemonnee-instantie zal worden geïntegreerd.

5. **Evaluatieactiviteiten in verband met de portemonnee-instantie**

1) Bij de evaluatie van de portemonnee-instantie worden de volgende twee belangrijke uitdagingen in aanmerking genomen:

a) de portemonnee-instantie komt waarschijnlijk voor in varianten van dezelfde basistoepassing, waarbij elke variant bedoeld is voor een specifieke categorie apparaten van eindgebruikers;

b) de verschillende varianten van de portemonnee-instantie worden waarschijnlijk vaak bijgewerkt om de ontwikkeling van het onderliggende beveiligingsplatform te volgen, bijvoorbeeld wanneer kwetsbaarheden worden vastgesteld die wijzigingen in de toepassingen vereisen.

2) Bij de evaluatie van de portemonnee-instantie wordt rekening gehouden met deze specifieke uitdagingen. Een van de onmiddellijke gevolgen is dat het kader van gemeenschappelijke criteria niet in alle gevallen geschikt is. Daarom worden waar nodig alternatieve evaluatiemethoden in overweging genomen. In de nationale certificeringsregelingen wordt rekening gehouden met het gebruik van de EN 17640:2018-methode voor het volgende:

a) als onderdeel van de regeling zelf;

b) via nationale regelingen op basis van de methode;

c) door middel van nationale regelingen die gebaseerd zijn op soortgelijke beginselen, maar die zijn opgezet vóór de ontwikkeling van de EN 17640:2018-methode.

3) Aangezien het uitvoeren van een volledige specifieke evaluatie van elke variant beperkte toegevoegde waarde kan hebben, moet in de nationale certificeringsregelingen bovendien worden overwogen criteria vast te stellen die het mogelijk maken monsters te nemen, teneinde herhaling van identieke evaluatieactiviteiten te voorkomen en de nadruk te leggen op activiteiten die specifiek zijn voor een bepaalde variant. In de nationale certificeringsregelingen moet worden vereist dat alle certificerende instanties hun gebruik van monsterneming rechtvaardigen.

4) In de nationale certificeringsregelingen worden actualiseringen van de portemonnee-instantie in het algemene veranderingsbeheerproces dat voor de portemonnee-oplossing is gespecificeerd, opgenomen. Ook moeten regels worden vastgesteld voor de procedures die door de aanbieder van portemonnees voor elke actualisering worden uitgevoerd (bv. een analyse van de gevolgen van de wijzigingen voor de beveiligingscontroles) en voor de evaluatieactiviteiten die door de certificerende instantie worden uitgevoerd bij actualiseringen onder bepaalde voorwaarden (bv. het beoordelen van de operationele doeltreffendheid van een gewijzigde beveiligingscontrole). Het veranderingsbeheerproces is een van de processen waarvan de operationele doeltreffendheid overeenkomstig artikel 18, lid 3, jaarlijks wordt gecontroleerd.

6. **Evaluatieactiviteiten in verband met de diensten en processen die worden gebruikt voor de levering en de werking van de portemonnee-oplossing**

1) Voor de evaluatie van diensten en processen die een rol spelen bij de levering en werking van de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, verzamelt het evaluatieteam bewijsmateriaal door evaluatieactiviteiten uit te voeren die onder meer controle-, inspectie-, verificatie- en valideringsactiviteiten kunnen omvatten.

2) De certificerende instantie moet de toereikendheid en de geschiktheid van de bewijsstukken bevestigen om voldoende zekerheid te bieden dat de diensten en processen aan de certificeringseisen voldoen, door het volgende te bevestigen:

   a) de nauwkeurigheid van de informatie in de beschrijving van de processen en diensten;

   b) de geschiktheid van het ontwerp en de controles van de processen en diensten om aan de evaluatiecriteria te voldoen;

   c) de operationele doeltreffendheid van de uitvoering van deze controles gedurende een bepaalde periode voorafgaand aan de evaluatie.

3) De nauwkeurigheid van de beschrijving en de operationele doeltreffendheid van de uitvoering van controles kunnen worden beschouwd als verificatiedoelstellingen, in de zin van ISO/IEC EN 17000:2020, van de overeenkomstige claims van de aanbieder van portemonnees (d.w.z. bevestiging van de correctheid van gebeurtenissen die zich reeds hebben voorgedaan of resultaten die reeds zijn verkregen), en de geschiktheid van het ontwerp en de controles van de diensten en processen om aan de evaluatiecriteria te voldoen, kunnen worden beschouwd als een valideringsdoelstelling, in de zin van ISO/IEC EN 17000:2020, van de overeenkomstige claim van de aanbieder van portemonnees (d.w.z. bevestiging van de plausibiliteit met betrekking tot een beoogd toekomstig gebruik of verwacht resultaat).

4) Aangezien een portemonnee-oplossing niet mag functioneren voordat zij is gecertificeerd, kan de operationele doeltreffendheid niet worden bevestigd op basis van de daadwerkelijke werking van de oplossing. Daarom moet dit worden bevestigd aan de hand van bewijsmateriaal dat tijdens tests of proefprojecten is verzameld.

5) Er kunnen al nationale certificeringsregelingen bestaan voor specifieke diensten en processen, bijvoorbeeld voor het instappen van gebruikers. Het gebruik van dergelijke regelingen moet in voorkomend geval in het kader van nationale certificeringsregelingen worden overwogen.

7. **Evaluatieactiviteiten in verband met de ICT-diensten die worden gebruikt voor de levering en de werking van de portemonnee-oplossing**

1) Sommige portemonneearchitecturen kunnen afhankelijk zijn van specifieke ICT-diensten, waaronder clouddiensten voor de levering en de werking van een portemonnee-oplossing, en deze diensten kunnen zowel gevoelige gegevens als gevoelige activiteiten hosten. In dat geval worden in de nationale certificeringsregelingen beveiligingsvereisten voor deze ICT-diensten gespecificeerd.

2) Er bestaan al veel certificeringsregelingen voor ICT-diensten, clouddiensten en andere bronnen van zekerheidsinformatie, waaronder de in bijlage II vermelde bronnen. De nationale certificeringsregelingen moeten, voor zover beschikbaar en van toepassing, berusten op die bestaande mechanismen door middel van een van de volgende mechanismen:

   a) het verplicht stellen van het gebruik van een bepaalde regeling of van een selectie van regelingen, door de voorwaarden te specificeren waaronder de ICT- of clouddiensten aan de hand van deze regelingen moeten worden beoordeeld;

   b) de keuze van de beoordeling overlaten aan de aanbieder van portemonnees en de afhankelijkheidsanalyse gebruiken om de geschiktheid van de via deze beoordelingen verkregen zekerheidsinformatie te analyseren.

3) In beide gevallen worden in de nationale certificeringsregelingen de aanvullende evaluatieactiviteiten gespecificeerd die nodig zijn om de via deze regelingen verkregen informatie te analyseren of aan te vullen.

BIJLAGE V

LIJST VAN OPENBAAR BESCHIKBARE INFORMATIE OVER PORTEMONNEES

1. De informatie die overeenkomstig artikel 8, lid 5, openbaar wordt gemaakt, bestaat ten minste uit het volgende:

   a) eventuele beperkingen op het gebruik van een portemonnee-oplossing;

   b) richtsnoeren en aanbevelingen van de aanbieder van portemonnees om eindgebruikers te helpen bij de veilige configuratie, installatie, uitrol, werking en onderhoud van portemonnees;

   c) de periode gedurende welke beveiligingsondersteuning zal worden verstrekt aan eindgebruikers, met name inzake de beschikbaarheid van actualiseringen in verband met cyberbeveiliging;

   d) de contactgegevens van de fabrikant of aanbieder en aanvaarde methoden voor de ontvangst van kwetsbaarheidsinformatie van eindgebruikers en beveiligingsonderzoekers;

   e) een verwijzing naar onlineregisters met een overzicht van openbaar gemaakte kwetsbaarheden in verband met portemonnees en alle relevante adviezen op het gebied van cyberbeveiliging.

2. De in lid 1 bedoelde informatie wordt op duidelijke, volledige en gemakkelijk toegankelijke wijze, op een voor het publiek toegankelijke plaats, ter beschikking gesteld aan eenieder die gebruik wenst te maken van een portemonnee-oplossing.

BIJLAGE VI

METHODE OM DE AANVAARDBAARHEID VAN ZEKERHEIDSINFORMATIE TE BEOORDELEN

1. Beoordeling van de beschikbaarheid van zekerheidsdocumentatie

De beoordelaars vermelden de zekerheidsdocumentatie die beschikbaar is voor elke relevante component van de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt. Vervolgens beoordelen de beoordelaars de algemene relevantie van elk zekerheidsdocument voor de afhankelijkheidsevaluatie.

Bij de analyse worden de volgende aspecten in aanmerking genomen:

1) over de zekerheidsdocumentatie zelf:

   a) het soort zekerheidsdocumentatie, met alle vereiste details,

      (voorbeelden van dergelijke documenten zijn certificaten van overeenstemming overeenkomstig ISO/IEC EN 27001:2022 of type 1 of 2 voor ISAE-verslagen);

   b) de bestreken periode of geldigheidsduur,

      (deze periode kan worden aangevuld met een overbruggingsbrief (een document dat een periode bestrijkt tussen de einddatum van de verslagperiode van het huidige ISAE-verslag en de publicatie van een nieuw ISAE-verslag) of een soortgelijke verklaring);

   c) het toepasselijke kader (bv. bestaande norm);

   d) of de zekerheidsdocumentatie een overzicht bevat van de vereisten van de regeling;

2) over de vakbekwaamheid en de onpartijdigheid van de partij die het zekerheidsverslag afgeeft:

   a) de naam van de certificerende instantie en, indien beschikbaar, de naam van de hoofdbeoordelaar;

   b) het bewijs van de bekwaamheid van de certificerende instantie en de beoordelaar (bv. accreditatie, persoonlijke certificering enz.);

   c) het bewijs van onpartijdigheid van de certificerende instantie en de beoordelaar (bv. accreditatie enz.).

2. Beoordeling van de zekerheid met betrekking tot individuele vereisten

De beoordelaars verifiëren of de zekerheidsdocumentatie die beschikbaar is voor de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, toereikend is om te bepalen of de portemonnee-oplossing voldoet aan de verwachtingen met betrekking tot de afzonderlijke vereisten van de certificeringsregeling.

Deze beoordeling wordt uitgevoerd voor elke relevante component van de portemonnee-oplossing en het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt, door een veronderstelling te formuleren voor de beveiligingscontroles van de portemonnee-oplossing.

Voor elk van deze veronderstellingen bepaalt het evaluatieteam of de zekerheid die in de beschikbare zekerheidsdocumentatie wordt geboden, al dan niet toereikend is.

De vaststelling dat de zekerheid toereikend is, wordt gebaseerd op het volgende:

1) de vereiste informatie, met het verwachte betrouwbaarheidsniveau, is beschikbaar in de zekerheidsdocumentatie;

2) de in de zekerheidsdocumentatie beschikbare informatie bestrijkt niet het volledige toepassingsgebied van de vereiste, maar aanvullende controles of compenserende controles (d.w.z. interne controles die het risico op bestaande of potentiële kwetsbaarheiden in de controle verminderen) die worden uitgevoerd in de portemonnee-oplossing of in het stelsel voor elektronische identificatie op grond waarvan zij worden verstrekt, stellen de beoordelaars in staat te bepalen dat de informatie toereikend is;

3) de informatie in de zekerheidsdocumentatie biedt niet het verwachte betrouwbaarheidsniveau, maar de controles die worden uitgevoerd om de aanbieder van portemonnees te beoordelen en te monitoren, stellen de beoordelaars in staat te bepalen of de informatie toereikend is;

4) indien in de zekerheidsdocumentatie melding wordt gemaakt van niet-naleving bij het ontwerp of de uitvoering van de controles die worden gebruikt om aan een veronderstelling te voldoen, moeten de corrigerende maatregelen die door de aanbieder van portemonnees worden voorgesteld en uitgevoerd en door zijn beoordelaars worden beoordeeld, toereikend zijn om te garanderen dat aan de veronderstelling wordt voldaan.

BIJLAGE VII

INHOUD VAN HET CERTIFICAAT VAN OVEREENSTEMMING

1. Een unieke identificatiecode die wordt toegekend door de certificerende instantie die het certificaat van overeenstemming afgeeft.

2. Informatie over de gecertificeerde portemonnee-oplossing en de stelsels voor elektronische identificatie op grond waarvan zij wordt verstrekt, en over de houder van het certificaat van overeenstemming, met inbegrip van het volgende:
   a) de naam van de portemonnee-oplossing;
   b) de naam van de stelsels voor elektronische identificatie in het kader waarvan de portemonnee-oplossing wordt verstrekt;
   c) de versie van de portemonnee-oplossing die is geëvalueerd;
   d) de naam, het adres en de contactgegevens van de houder van het certificaat van overeenstemming;
   e) de link naar de website van de houder van het certificaat van overeenstemming met de informatie die openbaar moet worden gemaakt.

3. Informatie met betrekking tot de evaluatie en de certificering van de portemonnee-oplossing en de stelsels voor elektronische identificatie op grond waarvan zij wordt verstrekt, waaronder:
   a) de naam, het adres en de contactgegevens van de certificerende instantie die het certificaat van overeenstemming heeft afgegeven;
   b) indien afwijkend van de certificerende instantie, de naam van de conformiteitsbeoordelingsinstantie die de evaluatie heeft uitgevoerd, samen met informatie over de accreditatie ervan;
   c) de naam van de regelinghouder;
   d) verwijzingen naar Verordening (EU) nr. 910/2014 en naar deze verordening;
   e) een verwijzing naar het certificeringsrapport bij het certificaat van overeenstemming;
   f) een verwijzing naar het certificeringsbeoordelingsverslag bij het certificaat van overeenstemming;
   g) een verwijzing naar de voor de evaluatie gebruikte normen, met inbegrip van de versies ervan;
   h) de datum van afgifte van het certificaat van overeenstemming;
   i) de geldigheidsduur van het certificaat van overeenstemming.

BIJLAGE VIII

INHOUD VAN HET OPENBARE CERTIFICERINGSRAPPORT EN HET CERTIFICERINGSBEOORDELINGSVERSLAG

1. Het openbare certificeringsrapport bestaat ten minste uit de volgende aspecten:

   a) een samenvatting;

   b) het benoemen van de portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt;

   c) een beschrijving van de portemonnee-oplossing en van het stelsel voor elektronische identificatie op grond waarvan zij wordt verstrekt;

   d) de beveiligingsinformatie die openbaar moet worden gemaakt, zoals beschreven in bijlage V, of een verwijzing naar deze informatie;

   e) een samenvatting van het voorlopige controle- en valideringsplan;

   f) een samenvatting van de evaluatie en het certificeringsbesluit.

2. Het certificeringsbeoordelingsverslag bestaat ten minste uit:

   a) een beschrijving van het ontwerp van de portemonnee-oplossing, het identificatiesysteem en het instapproces, samen met de risicobeoordeling en het specifieke valideringsplan;

   b) een beschrijving van de wijze waarop de portemonnee-oplossing voldoet aan de vereisten inzake het betrouwbaarheidsniveau “hoog” en van de wijze waarop dit wordt aangetoond door de resultaten van de overeenkomstig deze verordening uitgevoerde certificeringsbeoordeling van de portemonnee-oplossing;

   c) een beschrijving van het resultaat van de beoordeling van de overeenstemming van de portemonnee-oplossing en van het stelsel voor elektronische identificatie in het kader waarvan de overeenkomstige portemonnee-eenheden worden verstrekt, met name de overeenstemming met het volgende:

      — de vereisten als uiteengezet in artikel 5 bis, leden 4, 5 en 8, van Verordening (EU) nr. 910/2014;

      — het vereiste van logische scheiding als bedoeld in artikel 5 bis, lid 14, van Verordening (EU) nr. 910/2014;

      — indien van toepassing, de in artikel 5 bis, lid 24, van Verordening (EU) nr. 910/2014 bedoelde normen en technische specificaties, waarbij wordt beschreven hoe deze vereisten zich verhouden tot de overeenkomstige normatieve vereisten die door de nationale certificeringsregelingen zijn gespecificeerd;

   d) een samenvatting van het resultaat van de uitvoering van het valideringsplan, met inbegrip van alle vastgestelde gevallen van niet-naleving.

BIJLAGE IX

TIJDSCHEMA VOOR VERPLICHTE EVALUATIES VAN HET TOEZICHT

1. In artikel 18 worden de vereisten voor de certificeringscyclus, met name de uitvoering van regelmatige evaluatieactiviteiten, gespecificeerd. Die activiteiten bestaan ten minste uit het volgende:

   a) een volledige evaluatie van het voorwerp van de conformiteitsbeoordeling bij de eerste evaluatie en bij elke evaluatie voor hercertificering, met inbegrip van actualiseringen van productcomponenten;

   b) een kwetsbaarheidsbeoordeling bij de eerste evaluatie en bij elke evaluatie voor hercertificering, en ten minste om de twee jaar bij de toezichtevaluaties, die ten minste betrekking heeft op de veranderingen in het voorwerp van de conformiteitsbeoordeling en de veranderingen in het dreigingslandschap sinds de laatste kwetsbaarheidsbeoordeling;

   c) aanvullende activiteiten zoals penetratietests in geval van een verhoogd risiconiveau of het ontstaan van nieuwe bedreigingen;

   d) ten minste eenmaal per jaar een evaluatie van de operationele doeltreffendheid van onderhoudsprocessen bij toezichtevaluaties en evaluaties voor hercertificering, die ten minste betrekking heeft op processen voor versiecontrole, actualisering en kwetsbaarheidsbeheer;

   e) na een succesvolle evaluatie en een certificeringsbesluit, de afgifte van een certificaat van overeenstemming na de eerste beoordeling en na elke evaluatie voor hercertificering.

2. In tabel 1 is een referentieschema opgenomen op basis van een cyclus van vier jaar, waarbij:

   a) het jaar 1 begint wanneer het certificaat van overeenstemming voor het eerst wordt afgegeven, en

   b) alle evaluatieactiviteiten binnen twaalf maanden na de evaluatie van het voorgaande jaar moeten worden uitgevoerd.

3. Het tijdschema in tabel 1 is een aanbeveling om te zorgen voor tijdige hercertificering en om verstoringen in de levering van de portemonnee-oplossing te voorkomen. Andere schema's kunnen mogelijk zijn, zo lang het certificaat van overeenstemming niet langer dan vijf jaar geldig is, zoals bepaald in artikel 5 quater, lid 4, van Verordening (EU) nr. 910/2014.

4. Naast de regelmatige evaluaties kan op verzoek van de certificerende instantie of de houder van het certificaat van overeenstemming een bijzondere evaluatie in gang worden gezet na een aanzienlijke wijziging van het voorwerp van de certificering of van het dreigingslandschap.

5. Elke evaluatie, met inbegrip van toezichtevaluaties en bijzondere evaluaties, kan leiden tot de afgifte van een nieuw certificaat van overeenstemming, met name in geval van belangrijke wijzigingen in het voorwerp van de certificering, maar met dezelfde vervaldatum als het oorspronkelijke certificaat van overeenstemming.

Tabel 1

Een volledige evaluatiecyclus van 4 jaar

Tijdstip	Soort evaluatie	Activiteiten
Jaar 0	Initieel	— Volledige evaluatie van het voorwerp van de certificering, met inbegrip van kwetsbaarheidsbeoordeling — — Met inbegrip van een functie om actualiseringen uit te voeren voor elke softwarecomponent — Evaluatie van de onderhoudsprocessen, met uitzondering van de operationele doeltreffendheid ervan — Afgifte van het certificaat van overeenstemming en begin van de cyclus van 4 jaar
Jaar 1	Toezicht	— Evaluatie van de operationele doeltreffendheid van de onderhoudsprocessen — — Ten minste versiecontrole, actualisering, kwetsbaarheidsbeheer — Evaluatie van veranderingen die van invloed zijn op de veiligheid van het product

Tijdstip	Soort evaluatie	Activiteiten
Jaar 2	Toezicht	— Kwetsbaarheidsbeoordeling van de volledige oplossing — Evaluatie van de operationele doeltreffendheid van de onderhoudsprocessen — Ten minste versiecontrole, actualisering, kwetsbaarheidsbeheer — Evaluatie van veranderingen die van invloed zijn op de veiligheid van het product
Jaar 3	Toezicht	— Evaluatie van de operationele doeltreffendheid van de onderhoudsprocessen — Ten minste versiecontrole, actualisering, kwetsbaarheidsbeheer — Evaluatie van veranderingen die van invloed zijn op de veiligheid van het product
Jaar 4	Hercertificering	1) Volledige evaluatie van het voorwerp van de certificering, met inbegrip van kwetsbaarheidsbeoordeling 2) Vereenvoudigde evaluatie voor functies/processen die niet zijn gewijzigd 3) Met inbegrip van een functie om actualiseringen uit te voeren voor elke softwarecomponent 4) Evaluatie van de onderhoudsprocessen, met inbegrip van de operationele doeltreffendheid ervan 5) Afgifte van een nieuw certificaat van overeenstemming