Europeiska unionens
officiella tidning

SV
L-serien

2024/2981

4.12.2024

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/2981

av den 28 november 2024

om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller certifiering av EU:s digitala identitetsplånböcker

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG ([1]), särskilt artikel 5c.6, och

av följande skäl:

(1) Enligt artikel 5c i förordning (EU) nr 910/2014 ska certifieringen av EU:s digitala identitetsplånböcker (*plånböcker*) ske i enlighet med krav på funktion, cybersäkerhet och dataskydd för att säkerställa en hög nivå av säkerhet och förtroende för plånböckerna. Dessa certifieringskrav måste harmoniseras mellan medlemsstaterna för att förhindra en fragmentering av marknaden och för att bygga upp en kraftfull ram.

(2) Europaparlamentets och rådets förordning (EU) 2016/679 ([2]) och, i förekommande fall, Europaparlamentets och rådets direktiv 2002/58/EG ([3]) är tillämpliga på behandlingen av personuppgifter enligt denna förordning.

(3) Kommissionen utvärderar regelbundet ny teknik, nya metoder, standarder eller tekniska specifikationer. För att säkerställa största möjliga harmonisering bland medlemsstaterna för utveckling och certifiering av plånböcker bygger de tekniska specifikationerna i denna förordning på det arbete som utförts på grundval av kommissionens rekommendation (EU) 2021/946 av den 3 juni 2021 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet ([4]), särskilt den arkitektur och referensram som ingår i den. I enlighet med skäl 75 i Europaparlamentets och rådets förordning (EU) 2024/1183 ([5]) bör kommissionen vid behov se över och uppdatera denna genomförandeförordning för att hålla den i linje med den globala utvecklingen, arkitekturen och referensramen och för att följa praxis på den inre marknaden.

(4) För att intyga överensstämmelse med de cybersäkerhetskrav som ingår i certifieringsramen bör certifieringen av plånbokslösningar, i förekommande och tillämpliga fall, hänvisa till de europeiska ordningar för cybersäkerhetscertifiering som införts i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881 ([6]). Om sådana ordningar saknas, eller om de delvis omfattar cybersäkerhetskrav, fastställs i denna förordning de allmänna krav som gäller för nationella certifieringsordningar och som omfattar krav på funktion, cybersäkerhet och dataskydd.

([1]) EUT L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.
([2]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), (EUT L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).
([3]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), (EGT L 201, 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).
([4]) EUT L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj?locale=sv.
([5]) Europaparlamentets och rådets förordning (EU) 2024/1183 av den 11 april 2024 om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av ett europeiskt ramverk för digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).
([6]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) Enligt artikel 5a.11 i förordning (EU) nr 910/2014 ska plånböckerna certifieras i förhållande till tillitsnivå hög i enlighet med förordning (EU) nr 910/2014 och kommissionens genomförandeförordning (EU) 2015/1502 ([7]). Denna tillitsnivå måste uppnås av den övergripande plånbokslösningen. Enligt denna förordning får vissa komponenter i plånbokslösningen certifieras i förhållande till en lägre tillitsnivå, förutsatt att detta är vederbörligen motiverat och utan att det påverkar den tillitsnivå hög som ska uppnås av den övergripande lösningen.

(6) Alla nationella certifieringsordningar bör utse en systemägare som ska ansvara för utvecklingen och underhållet av certifieringsordningen. Systemägaren kan vara ett organ för bedömning av överensstämmelse, ett statligt organ eller en statlig myndighet, en branschorganisation, en grupp organ för bedömning av överensstämmelse eller ett annat lämpligt organ och kan vara ett annat organ än det som driver den nationella certifieringsordningen.

(7) Certifieringsobjektet bör omfatta plånbokslösningens programvarukomponenter, såsom plånboksinstansen. Krypteringsapplikationen, krypteringshårdvaran och de plattformar på vilka dessa programvarukomponenter körs, bör, även om den ingår i driftsmiljön, endast inkluderas i certifieringsobjektet när den tillhandahålls av plånbokslösningen. I andra fall, och särskilt när denna hårdvara och dessa plattformar tillhandahålls av slutanvändare, bör tillhandahållarna fastställa antaganden om plånbokslösningens driftsmiljö, inbegripet på denna hårdvara och dessa plattformar, och vidta åtgärder för att bekräfta att dessa antaganden verifieras i praktiken. För att säkerställa skyddet av kritiska tillgångar med hjälp av hårdvara och systemprogramvara som används för att hantera och skydda krypteringsnycklar som skapats, lagrats eller bearbetats av krypteringshårdvaran måste denna hårdvara uppfylla höga certifieringsstandarder, som återspeglas i internationella standarder såsom Common Criteria (EUCC), som inrättades genom kommissionens genomförandeförordning (EU) 2024/482 ([8]), genom EAL4-utvärdering och avancerad metodisk sårbarhetsanalys, till exempel jämförbar med AVA_VAN.5. Dessa certifieringsstandarder bör användas senast när certifieringen av plånböckernas överensstämmelse utförs enligt en europeisk ordning för cybersäkerhetscertifiering som antagits i enlighet med förordning (EU) 2019/881.

(8) Helt mobila, säkra och användarvänliga plånböcker stöds av tillgången till standardiserade och certifierade manipuleringssäkra lösningar, till exempel inbyggda säkerhetskomponenter, externa anordningar såsom smartkort, eller inbyggda SIM-plattformar i mobila enheter. Det är viktigt att säkerställa snabb tillgång till inbyggda säkerhetskomponenter för nationella medel för elektronisk identifiering och plånböcker, och att samordna medlemsstaternas insatser på detta område. Den europeiska samarbetsgruppen för digital identitet som inrättats i enlighet med artikel 46e.1 i förordning (EU) nr 910/2014 (*samarbetsgruppen*) bör därför inrätta en särskild undergrupp för detta ändamål. I samråd med berörda parter bör denna undergrupp komma överens om en gemensam färdplan för tillgång till inbyggda säkerhetskomponenter som ska beaktas av kommissionen i samband med rapporten om översynen av förordning (EU) nr 910/2014. För att underlätta användningen av plånboken på nationell nivå bör kommissionen dessutom, i samarbete med medlemsstaterna, utarbeta och kontinuerligt uppdatera en handbok för användningsfall som en del av arkitekturen och referensramen.

(9) Nationella certifieringsordningars certifieringsobjekt bör också omfatta de processer som används för att tillhandahålla och driva plånbokslösningen, även om definitionen eller genomförandet av dessa processer läggs ut på tredje part. För att visa att processerna uppfyller systemens krav får tillitsinformation användas som bevis, förutsatt att en beroendeanalys används för att avgöra om tillitsinformationen är tillräcklig. Det finns många olika former av tillitsinformation, bland annat rapporter och intyg om överensstämmelse, som kan vara privata, nationella, europeiska eller internationella och som bygger på standarder eller tekniska specifikationer. Syftet med beroendeanalysen är att bedöma kvaliteten på den tillitsinformation som finns tillgänglig om en plånboks komponenter.

([7]) Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (EUT L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([8]) Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) I enlighet med de förfaranden som inrättats för detta ändamål bör samarbetsgruppen kunna avge yttranden och rekommendationer om de utkast till nationella certifieringssystem som lämnats in till den. Dessa nationella certifieringsordningar bör vara specifika för plånbokens arkitektur och det bör finnas särskilda profiler för varje specifik arkitektur som stöds.

(11) För att säkerställa att det finns en samsyn om och ett harmoniserat tillvägagångssätt för bedömningen av de mest kritiska risker som kan påverka tillhandahållandet och driften av plånböcker bör det upprättas ett register över risker och hot som bör beaktas vid utformningen av plånbokslösningar oberoende av deras specifika arkitektur. De cybersäkerhetsmål som beskrivs i förordning (EU) nr 910/2014, såsom plånbokslösningens konfidentialitet, integritet och tillgänglighet, samt användarnas och uppgifternas integritet, bör beaktas vid identifieringen av vilka risker som ska föras in i registret. Vederbörlig hänsyn till de risker och hot som finns med i detta riskregister bör ingå i kraven på de nationella certifieringsordningarna. För att hålla jämna steg med den ständigt föränderliga hotbilden bör riskregistret underhållas och regelbundet uppdateras i samarbete med samarbetsgruppen.

(12) När systemägarna inrättar sina certifieringsordningar bör de göra en riskbedömning för att förfina och komplettera de risker och hot som förtecknas i registret med risker och hot som är specifika för plånbokslösningens arkitektur eller genomförande. Vid riskbedömningen bör man överväga hur tillämpliga risker och hot kan hanteras på lämpligt sätt. Plånbokstillhandahållarna bör komplettera ordningens riskbedömning för att identifiera eventuella risker och hot som är specifika för dess genomförande och föreslå lämpliga behandlingsåtgärder som utvärderas av certifieringsorganet.

(13) För att visa att en plånbokslösnings arkitektur uppfyller de tillämpliga säkerhetskraven bör varje arkitekturspecifik ordning eller profil innehålla åtminstone en beskrivning av plånbokslösningens arkitektur, en förteckning över de säkerhetskrav som är tillämpliga på plånbokslösningens arkitektur, en utvärderingsplan som bekräftar att en plånbokslösning baserad på denna arkitektur uppfyller dessa krav samt en riskbedömning. De nationella certifieringsordningarna bör kräva att plånbokstillhandahållare visar hur utformningen av den plånbokslösning som de tillhandahåller överensstämmer med referensarkitekturen och beskriver säkerhetskontrollerna och valideringsplanerna för den specifika plånbokslösningen. De nationella certifieringsordningarna bör också fastställa en bedömning av överensstämmelse för att kontrollera att plånbokens utformning korrekt återspeglar den valda profilens referensarkitektur. De nationella certifieringsordningarna bör uppfylla kraven i artikel 51 i förordning (EU) 2019/881, med undantag för leden e och f, som rör loggning.

(14) När det gäller certifiering av produkter bör det vara tillåtet att använda intyg om överensstämmelse som utfärdats inom ramen för den europeiska ordningen för cybersäkerhetscertifiering EUCC, och intyg om överensstämmelse som utfärdats inom ramen för nationella certifieringsordningar enligt det avtal om ömsesidigt erkännande som överenskommits av gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS). Dessutom bör det vara tillåtet att använda andra nationella certifieringsordningar för mindre känsliga produktkomponenter, till exempel de som inrättats enligt standarden CEN EN 17640 om en fast utvärderingsmetod för cybersäkerhet.

(15) EU:s förtroendemärke för digitala identitetsplånböcker (*förtroendemärket*) bör användas för att på ett tydligt, enkelt och igenkännligt sätt ange att en plånbok har tillhandahållits i enlighet med förordning (EU) nr 910/2014. Det bör därför betraktas som ett överensstämmelsemärke för en plånbokslösning som certifierats enligt nationella certifieringsordningar. Nationella certifieringsordningar bör inte fastställa några andra överensstämmelsemärken.

(16) För att motverka bedrägerier bör de nationella certifieringsordningarna fastställa vilka åtgärder som ska vidtas om någon på falska grunder ansöker om certifiering inom ramen för ordningen.

(17) För att säkerställa en effektiv hantering av anmälningar av sårbarheter bör tillhandahållare av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls fastställa och genomföra förfaranden för att utvärdera hur allvarliga sårbarheterna är och vilka konsekvenser de kan ha. De nationella certifieringsordningarna bör fastställa en tröskel över vilken en anmälan ska göras till certifieringsorganet. Ett sådant anmälningskrav bör inte påverka de kriterier som fastställs i dataskyddslagstiftningen och av medlemsstaternas dataskyddsmyndigheter för anmälan av personuppgiftsincidenter. Möjliga synergier skulle kunna skapas mellan den obligatoriska anmälan av incidenter mot eller äventyrande av plånbokslösningar och anmälan av personuppgiftsincidenter i enlighet med förordning (EU) 2016/679. Certifieringsorganets bedömning av en konsekvensanalysrapport om sårbarheter bör inte påverka en dataskyddsmyndighets bedömning av en konsekvensbedömning avseende dataskydd i enlighet med artiklarna 35 och 36 i förordning (EU) 2016/679.

(18) tillhandahållarna av plånbokslösningar och det system för elektronisk identifiering enligt vilket de tillhandahålls bör underrätta systemägaren om eventuella motiveringar till undantag från den sårbarhetsanalys som krävs för utvärderingen av krypteringshårdvaran och krypteringsapplikationen, i enlighet med bilaga IV.

(19) Annulering av ett intyg om överensstämmelse kan få allvarliga konsekvenser, till exempel återkallelse av alla införda plånboksenheter. Certifieringsorganen bör därför endast överväga annulering om en sårbarhet som inte åtgärdats sannolikt avsevärt kommer att påverka plånbokslösningens tillförlitlighet eller en annan plånbokslösnings tillförlitlighet.

(20) Ett särskilt förfarande för uppdatering av nationella certifieringsordningar bör införas för att hantera övergången till nya versioner av ordningen, särskilt när det gäller åtgärder som intygsinnehavaren ska vidta när det gäller kommande utvärderingar, underhåll, omcertifiering och särskilda utvärderingar.

(21) För att underlätta transparens bör plånbokstillhandahållare offentligt utbyta säkerhetsinformation om sin plånbokslösning.

(22) Om de nationella certifieringsordningarna förlitar sig på tillitsinformation från andra certifieringsordningar eller källor bör en beroendeanalys genomföras för att kontrollera att tillitsdokumentationen, till exempel tillitsrapporter och intyg om överensstämmelse, är tillgänglig och lämplig för plånbokslösningarna och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls. Grunden för denna beroendeanalys bör vara riskbedömningen av plånbokslösningarna och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls. Vid utvärderingen bör ställning tas till om den tillitsdokumentation som finns tillgänglig för en viss plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls är tillräcklig för att ge garantier som motsvarar den avsedda utvärderingsnivån. Vid utvärderingen bör det även göras en uppdatering av beroendeanalysen eller vid behov en fullständig omprövning av den.

(23) Certifieringsorganen bör utfärda intyg om överensstämmelse i nationella certifieringsordningar, tillsammans med en offentlig certifieringsrapport, i enlighet med artikel 5d.2 a i förordning (EU) nr 910/2014. Den tillhörande rapporten om certifieringsbedömningen bör göras tillgänglig för samarbetsgruppen.

(24) De nationella certifieringsordningarna bör fastställa årliga kontrollutvärderingar för att säkerställa att processerna kring förvaltningen och underhållet av plånböckerna fungerar effektivt, vilket innebär att de fungerar i enlighet med de riktlinjer som fastställer processerna. Den sårbarhetsbedömning som ska göras vartannat år är ett krav som följer av förordning (EU) nr 910/2014, för att säkerställa att plånbokslösningen fortsätter att på lämpligt sätt täcka de cybersäkerhetsrisker och cyberhot som identifierats i riskregistret, inbegripet alla förändringar av hotbilden. Kontrollutvärderingar, omcertifieringsutvärderingar och särskilda utvärderingar bör definieras på samma sätt som i EN ISO/IEC 17021–1:2015.

(25) En certifieringscykel avslutas när intyget om överensstämmelse löper ut eller när ett nytt intyg om överensstämmelse utfärdas efter en framgångsrik omcertifieringsutvärdering. Omcertifieringsutvärderingen bör omfatta en utvärdering av alla komponenter i certifieringsobjektet, inbegripet en utvärdering av effektiviteten och, i tillämpliga fall, en sårbarhetsbedömning. Vid omcertifieringen bör det vara möjligt att återanvända resultatet från tidigare utvärderingar av komponenter som inte har ändrats.

(26) När en europeisk ordning för cybersäkerhetscertifiering antas bör nationella certifieringsordningar med samma tillämpningsområde upphöra att utfärda certifieringar efter en fastställd övergångsperiod i enlighet med artikel 57.1 i förordning (EU) 2019/881.

(27) De nationella certifieringsordningarna bör bygga på befintliga ramar och återanvända bevis när så är lämpligt för att säkerställa harmonisering och interoperabilitet. Medlemsstaterna får ingå avtal om gränsöverskridande återanvändning av certifieringsordningar eller delar av dessa. Europeiska kommissionen och Enisa bör i samarbete med samarbetsgruppen stödja medlemsstaterna i arbetet med att utveckla och upprätthålla deras nationella certifieringsordningar för att säkerställa kunskapsutbyte och bästa praxis.

(28) Samråd med Europeiska datatillsynsmannen har skett i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([9]) och avgav ett yttrande den 30 september 2024.

(29) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som avses i artikel 48.1 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll och tillämpningsområde

I denna förordning fastställs referensstandarder och specifikationer och förfaranden för att bygga upp en kraftfull ram för certifiering av plånböcker som regelbundet ska uppdateras för att hållas i linje med utvecklingen av teknik och standarder och med det arbete som utförs på grundval av rekommendation (EU) 2021/946 om en unionsgemensam verktygslåda för en samordnad strategi för en europeisk ram för digital identitet, särskilt arkitekturen och referensramen.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

(1) *plånbokslösning*: en kombination av programvara, hårdvara, tjänster, inställningar och konfigureringar, inklusive plånboksinstanser, en eller flera krypteringsapplikationer och en eller flera krypteringshårdvaror.

(2) *systemägare*: en organisation som ansvarar för att utveckla och underhålla en certifieringsordning.

(3) *certifieringsobjekt*: produkter, processer och tjänster eller en kombination av dessa som omfattas av specificerade krav.

(4) *krypteringsapplikation*: en applikation som hanterar kritiska tillgångar genom att vara kopplad till och använda de kryptografiska och icke-kryptografiska funktioner som tillhandahålls av krypteringshårdvaran.

(5) *plånboksinstans*: den applikation som är installerad och konfigurerad på en plånboksanvändares hårdvara eller i en plånboksanvändares miljö, som ingår i en plånboksenhet och som plånboksanvändaren använder för att interagera med plånboksenheten.

([9]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(6) *krypteringshårdvara*: manipuleringssäker hårdvara som tillhandahåller en miljö som är kopplad till och används av krypteringsapplikationen för att skydda kritiska tillgångar och tillhandahålla kryptografiska funktioner för att säkert kunna utföra kritiska operationer.

(7) *riskregister*: en förteckning över information som är relevant för certifieringsprocessen om identifierade risker.

(8) *plånbokstillhandahållare*: en fysisk eller juridisk person som tillhandahåller plånbokslösningar.

(9) *certifieringsorgan*: ett tredjepartsorgan för bedömning av överensstämmelse som driver certifieringsordningar.

(10) *plånboksenhet*: en unik konfigurering av en plånbokslösning som omfattar plånboksinstanser, krypteringsapplikationer och krypteringshårdvara som en plånbokstillhandahållare tillhandahåller en enskild plånboksanvändare.

(11) *kritiska tillgångar*: tillgångar inom eller i samband med en plånboksenhet som är av sådan extraordinär betydelse att det, om deras konfidentialitet, integritet och tillgänglighet äventyrades, skulle få en mycket allvarlig, funktionsnedsättande inverkan på förmågan att förlita sig på plånboksenheten.

(12) *plånboksanvändare*: en användare som kontrollerar plånboksenheten.

(13) *incident*: en incident enligt definitionen i artikel 6.6 i Europaparlamentets och rådets direktiv (EU) 2022/2555 ([10]).

(14) *inbyggd policy för utlämnande*: en uppsättning regler som en tillhandahållare av ett elektroniskt attributsintyg byggt in i intyget och som anger de villkor som en förlitande part måste uppfylla för att få tillgång till det elektroniska attributsintyget.

KAPITEL II

NATIONELLA CERTIFIERINGSORDNINGAR

Artikel 3

Inrättande av nationella certifieringsordningar

1. Medlemsstaterna ska utse en systemägare för varje nationell certifieringsordning.

2. Det certifieringsobjekt som fastställs i de nationella certifieringsordningarna ska vara tillhandahållandet och driften av plånbokslösningar och av de system för elektronisk identifiering inom ramen för vilka de tillhandahålls.

3. I enlighet med genomförandeförordning (EU) 2015/1502 ska certifieringsobjektet i de nationella certifieringsordningarna omfatta följande delar:

a) Programvarukomponenter, inbegripet inställningar och konfigureringar för en plånbokslösning och det system för elektronisk identifiering inom ramen för vilket plånbokslösningen tillhandahålls.

b) Hårdvarukomponenter och hårdvaruplattformar som de programvarukomponenter som avses i punkt (b) körs på eller är beroende av för kritiska operationer, i fall där de direkt eller indirekt tillhandahålls genom plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls och när de krävs för att uppnå önskad tillitsnivå för dessa programvarukomponenter. Om hårdvarukomponenterna och hårdvaruplattformarna inte tillhandahålls av plånbokstillhandahållaren ska de nationella certifieringsordningarna formulera antaganden för utvärdering av hårdvarukomponenterna och hårdvaruplattformarna, enligt vilka motstånd mot angripare med stor angreppspotential i enlighet med genomförandeförordning (EU) 2015/1502 kan tillhandahållas, och specificera den utvärderingsverksamhet som ska bekräfta dessa antaganden enligt bilaga IV.

([10]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) Processer som stöder tillhandahållandet och driften av en plånbokslösning, inbegripet den anslutningsprocess som avses i artikel 5a i förordning (EU) nr 910/2014, som åtminstone omfattar inskrivning, hantering av medel för elektronisk identifiering och organisation enligt avsnitten 2.1, 2.2, och 2.4 i bilaga I till genomförandeförordning (EU) 2015/1502.

4. De nationella certifieringsordningarna ska innehålla en beskrivning av den specifika arkitekturen för plånbokslösningarna och för det system för elektronisk identifiering inom ramen för vilket de tillhandahålls. Om de nationella certifieringsordningarna omfattar mer än en specifik arkitektur ska de innehålla en profil för varje specifik arkitektur.

5. För varje profil ska de nationella certifieringsordningarna innehålla minst följande:

a) Den specifika arkitekturen för en plånbokslösning och för det system för elektronisk identifiering inom ramen för vilket den tillhandahålls.

b) De säkerhetskontroller som är förenade med de tillitsnivåer som anges i artikel 8 i förordning (EU) nr 910/2014.

c) En utvärderingsplan som utarbetats i enlighet med avsnitt 7.4.1 i EN ISO/IEC 17065;2012.

d) De säkerhetskrav som är nödvändiga för att hantera de cybersäkerhetsrisker och cybersäkerhetshot som förtecknas i det riskregister som anges i bilaga I till denna förordning, upp till den tillitsnivå som krävs för att, i tillämpliga fall, uppfylla de mål som fastställs i artikel 51 i förordning (EU) 2019/881.

e) En kartläggning av de kontroller som avses i led (b) i denna punkt till arkitekturens komponenter.

f) En beskrivning av hur de säkerhetskontroller, den kartläggning, de säkerhetskrav och den utvärderingsplan som avses i leden (b) till (c) gör det möjligt för tillhandahållare av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls att på lämpligt sätt hantera de cybersäkerhetsrisker och cybersäkerhetshot som identifierats i det riskregister som avses i led (d), upp till den tillitsnivå som krävs, på grundval av en riskbedömning för att förfina och komplettera de risker och hot som förtecknas i registret med risker och hot som är specifika för arkitekturen.

6. I den utvärderingsplan som avses i punkt 5 (c) ska anges den utvärderingsverksamhet som ska ingå i utvärderingen av plånbokslösningar och av det system för elektronisk identifiering inom ramen för vilket de tillhandahålls.

7. För den utvärderingsverksamhet som avses i punkt 6 ska det krävas att tillhandahållare av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls tillhandahåller information som uppfyller kraven i bilaga II.

Artikel 4

Allmänna villkor

1. De nationella certifieringsordningarna ska omfatta krav på funktion, cybersäkerhet och dataskydd genom att, i förekommande och tillämpliga fall, använda följande certifieringsordningar:

a) Europeiska ordningar för cybersäkerhetscertifiering som inrättats i enlighet med förordning (EU) 2019/881, inbegripet EUCC.

b) Nationella ordningar för cybersäkerhetscertifiering som omfattas av EUCC i enlighet med artikel 49 i genomförandeförordning (EU) 2024/482.

2. Nationella certifieringsordningar får dessutom, i förekommande och tillämpliga fall, hänvisa till

a) andra relevanta nationella certifieringsordningar,

b) internationella, europeiska och nationella standarder,

c) tekniska specifikationer som uppfyller kraven i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([11]).

3. De nationella certifieringsordningarna ska

a) specificera de delar som förtecknas i avsnitt 6.5 i EN ISO/IEC 17067:2013,

b) genomföras som en typ 6-ordning i enlighet med avsnitt 5.3.8 i EN ISO/IEC 17067:2013.

4. De nationella certifieringsordningarna ska uppfylla följande krav:

a) Endast tillhandahållare som avses i artikel 5a.2 i förordning (EU) nr 910/2014 har rätt att bli utfärdade certifikat inom ramen för de nationella certifieringsordningarna.

b) Endast förtroendemärket används som överensstämmelsemärke.

c) tillhandahållare av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls inkluderar hänvisningar till förordning (EU) nr 910/2014 och denna förordning när de hänvisar till ordningen.

d) Tillhandahållare av plånbokslösningar och det system för elektronisk identifiering enligt vilket de tillhandahålls, kompletterar systemets riskbedömning enligt artikel 3.5 f för att identifiera risker och hot som är specifika för deras genomförande och föreslå lämpliga behandlingsåtgärder för alla relevanta risker och hot.

e) Skyldigheter och rättsliga åtgärder fastställs och innehåller hänvisningar till tillämplig nationell lagstiftning, som fastställer skyldigheter och eventuella rättsliga åtgärder, om certifiering inom ramen för ordningen används på ett bedrägligt sätt.

5. Den bedömning som avses i punkt 4 (d) ska delas med certifieringsorganet för utvärdering.

Artikel 5

Hantering av incidenter och sårbarheter

1. De nationella certifieringsordningarna ska innehålla krav på hantering av incidenter och sårbarheter i enlighet med punkterna 2–9.

2. Innehavaren av ett intyg om överensstämmelse för en plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls ska utan onödigt dröjsmål underrätta sitt certifieringsorgan om varje incident eller äventyrande av plånbokslösningen, eller av det system för elektronisk identifiering inom ramen för vilket den tillhandahålls, som sannolikt kommer att påverka dess överensstämmelse med kraven i de nationella certifieringsordningarna.

3. Innehavaren av ett intyg om överensstämmelse ska fastställa, upprätthålla och tillämpa en policy och förfaranden för hantering av sårbarheter, med beaktande av de förfaranden som anges i befintliga europeiska och internationella standarder, inklusive EN ISO/IEC 30111:2019.

4. Innehavaren av intyget om överensstämmelse ska anmäla sårbarheter och förändringar som påverkar plånbokslösningen till det utfärdande certifieringsorganet, baserat på fastställda kriterier för konsekvenserna av dessa sårbarheter och förändringar.

5. Innehavaren av intyget om överensstämmelse ska utarbeta en konsekvensanalysrapport om sårbarhet för eventuella sårbarheter som påverkar plånbokslösningens programvarukomponenter. Rapporten ska innehålla information om följande:

a) Sårbarhetens inverkan på den certifierade plånbokslösningen.

b) Möjliga risker som är förbundna med närheten av eller sannolikheten för en attack.

([11]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut nr 1673/2006/EG (EUT L 316, 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) Huruvida sårbarheten kan avhjälpas med tillgängliga medel.

d) Möjliga sätt att avhjälpa sårbarheten, i det fall sårbarheten kan avhjälpas med tillgängliga medel.

6. Om anmälan krävs enligt punkt 4 ska innehavaren av intyget om överensstämmelse utan onödigt dröjsmål översända den konsekvensanalysrapport om sårbarhet som avses i punkt 5 till certifieringsorganet.

7. Innehavaren av ett intyg om överensstämmelse ska fastställa, upprätthålla och tillämpa en policy för sårbarhetshantering som uppfyller kraven i bilaga I till förordningen om cyberresiliens ([12]).

8. Nationella certifieringsordningar ska innehålla krav på redovisning av sårbarheter som är tillämpliga på certifieringsorgan.

9. Innehavaren av ett intyg om överensstämmelse ska redovisa och registrera alla allmänt kända och avhjälpta sårbarheter i plånbokslösningen eller i någon av de förteckningar online som avses i bilaga V.

Artikel 6

Underhåll av nationella certifieringsordningar

1. De nationella certifieringsordningarna ska innehålla ett förfarande för regelbunden översyn av hur de fungerar. Detta förfarande ska syfta till att bekräfta deras lämplighet och identifiera aspekter som behöver förbättras, med beaktande av återkoppling från berörda parter.

2. De nationella certifieringsordningarna ska innehålla bestämmelser om deras underhåll. Detta förfarande ska inkludera minst följande krav:

a) Regler för styrningen av de nationella certifieringsordningarnas definition och krav.

b) Fastställande av tidsfrister för utfärdande av intyg efter antagandet av uppdaterade versioner av de nationella certifieringsordningarna, både för nya intyg om överensstämmelse och för tidigare utfärdade intyg.

c) En regelbunden översyn av de nationella certifieringsordningarna för att säkerställa att de nationella certifieringsordningarnas krav tillämpas konsekvent, med beaktande av minst följande aspekter:

— Frågor till systemägaren om förtydligande av kraven i den nationella certifieringsordningen.

— Återkoppling från berörda parter och andra intresserade parter.

— Benägenheten hos systemägaren för den nationella certifieringsordningen att besvara förfrågningar om information.

d) Regler för övervakning av referensdokument och förfaranden för utveckling av de nationella certifieringsordningarnas referensversioner, inbegripet åtminstone övergångsperioder.

e) En process för att säkerställa att de senaste cybersäkerhetsrisker och cybersäkerhetshot som förtecknas i riskregistret i bilaga I till denna förordning omfattas.

f) Ett förfarande för att hantera andra förändringar i de nationella certifieringsordningarna.

([12]) Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen), (EUT L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj?locale=sv).

3. De nationella certifieringsordningarna ska innehålla krav på att göra utvärderingar av för närvarande certifierade produkter inom en viss period efter översynen av ordningen, eller efter utgivningen av nya specifikationer eller standarder, eller nya versioner av dessa, som ska uppfyllas av plånbokslösningarna och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls.

KAPITEL III

KRAV PÅ SYSTEMÄGARE

Artikel 7

Allmänna villkor

1. Systemägarna ska utveckla och upprätthålla nationella certifieringsordningar och styra deras verksamhet.

2. Systemägarna får lägga ut hela eller delar av sina uppgifter på en tredje part. Vid underentreprenad till en privat part ska systemägarna fastställa alla parters skyldigheter och ansvar genom avtal. Systemägarna ska förbli ansvariga för all verksamhet som läggs ut på entreprenad och som utförs av deras underleverantörer.

3. Systemägarna ska i tillämpliga fall utföra sin övervakningsverksamhet på grundval av åtminstone följande information:

a) Information från certifieringsorgan, nationella ackrediteringsorgan och berörda marknadskontrollmyndigheter.

b) Information som framkommer genom sina egna eller andra myndigheters kontroller och utredningar.

c) Klagomål och överklaganden som mottagits i enlighet med artikel 15.

4. Systemägarna ska informera samarbetsgruppen om revideringar av de nationella certifieringsordningarna. De ska tillhandahålla tillräckligt med information så att samarbetsgruppen kan utfärda rekommendationer till systemägarna och yttranden om de uppdaterade nationella certifieringsordningarna.

KAPITEL IV

KRAV PÅ tillhandahållare AV PLÅNBOKSLÖSNINGAR OCH DET SYSTEM FÖR ELEKTRONISK IDENTIFIERING INOM RAMEN FÖR VILKET DE TILLHANDAHÅLLS

Artikel 8

Allmänna villkor

1. De nationella certifieringsordningarna ska innehålla cybersäkerhetskrav på grundval av en riskbedömning av varje specifik arkitektur som stöds. Dessa cybersäkerhetskrav ska syfta till att behandla identifierade cybersäkerhetsrisker och cyberhot, i enlighet med det riskregister som anges i bilaga I.

2. I enlighet med artikel 5a.23 i förordning (EU) nr 910/2014 ska de nationella certifieringsordningar kräva att plånbokslösningar och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls är motståndskraftiga mot angripare med stor angreppspotential för tillitsnivå hög i enlighet med genomförandeförordning (EU) 2015/1502.

3. De nationella certifieringsordningarna ska fastställa säkerhetskriterier som ska omfatta följande krav:

a) Cyberresiliensakten, i tillämpliga fall, eller krav som uppfyller de säkerhetsmål som anges i artikel 51 i förordning (EU) 2019/881.

b) Fastställande och genomförande av riktlinjer och förfaranden för hantering av risker förenade med driften av en plånbokslösning, inbegripet identifiering och bedömning av risker och begränsning av identifierade risker.

c) Fastställande och genomförande av riktlinjer och förfaranden för hantering av förändringar och hantering av sårbarheter i enlighet med artikel 5 i denna förordning.

d) Fastställande och genomförande av riktlinjer och förfaranden för personalförvaltning, inbegripet krav på sakkunskap, tillförlitlighet, erfarenhet, säkerhetsutbildning och kvalifikationer för personal som deltar i utvecklingen eller driften av plånbokslösningen.

e) Krav på plånbokslösningens driftsmiljö, inbegripet i form av antaganden om säkerheten i den hårdvara och på de plattformar som plånbokslösningens programvarukomponenter körs på, inbegripet krypteringshårdvara och, i tillämpliga och förekommande fall, krav på bedömning av överensstämmelse för att bekräfta att dessa antaganden kontrolleras på hårdvaran och plattformarna i fråga.

f) För varje antagande som inte stöds av ett intyg om överensstämmelse eller annan godtagbar tillitsinformation, en beskrivning av den mekanism som plånbokstillhandahållaren använder för att verkställa antagandet, samt en motivering av att mekanismen är tillräcklig för att säkerställa att antagandet kontrolleras.

g) Fastställande och genomförande av åtgärder för att säkerställa användningen av en för närvarande certifierad version av plånbokslösningen.

4. De nationella certifieringsordningarna ska innehålla funktionskrav avseende uppdateringsmekanismer för varje programvarukomponent i plånbokslösningarna och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls för de verksamheter som anges i bilaga III.

5. De nationella certifieringsordningarna ska kräva att den som ansöker om certifiering tillhandahåller eller på annat sätt gör tillgänglig för certifieringsorganet följande information och dokumentation:

a) Bevis för den information som avses i punkt 1 i bilaga IV, vid behov inbegripet uppgifter om plånbokslösningen och dess källkod, bland annat följande:

— *Information om arkitekturen:* för varje komponent i plånbokslösningen (inklusive produkt-, process- och tjänstekomponenter) en beskrivning av dess väsentliga säkerhetsegenskaper, inbegripet dess externa beroenden.

— *Kontroller och tillitsnivåer:* för varje säkerhetskontroll av plånbokslösningen en beskrivning av kontrollen och den erforderliga tillitsnivån, baserat på bilagan till genomförandeförordning (EU) 2015/1502, som innehåller ett antal tekniska specifikationer och förfaranden för de olika kontroller som genomförs med hjälp av medel för elektronisk identifiering.

— *Kartläggning av kontroller i förhållande till arkitekturens komponenter:* en beskrivning av hur kontrollerna av plånboken genomförs utifrån plånbokslösningens olika komponenter, baserat på en förklaring till varför det krävs en viss tillitsnivå och hur kontrollen genomförs med alla erforderliga säkerhetsaspekter på lämplig nivå.

— *Förklaring och motivering till risktäckningen:* en motivering av

  — kartläggningen av kontroller i förhållande till komponenterna,

  — den föreslagna utvärderingsplanens lämplighet för att täcka alla kontroller,

  — kontrollernas täckning av de cybersäkerhetsrisker och cybersäkerhetshot som identifierats i riskregistret, kompletterat med kontroller av risker och hot som är specifika för genomförandet, på lämplig tillitsnivå.

b) De uppgifter som anges i bilaga V.

c) En fullständig förteckning över intyg om överensstämmelse och annan tillitsinformation som används som bevis under utvärderingsverksamheten.

d) All annan information som är relevant för utvärderingsverksamheten.

KAPITEL V

KRAV PÅ CERTIFIERINGSORGAN

Artikel 9

Allmänna villkor

1. Certifieringsorganen ska ackrediteras av nationella ackrediteringsorgan som utsetts i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ([13]) i enlighet med EN ISO/IEC 17065:2012, förutsatt att de uppfyller de krav som fastställs i nationella certifieringsordningar i enlighet med punkt 2.

2. När det gäller ackreditering ska certifieringsorganen uppfylla samtliga av följande kompetenskrav:

a) Detaljerad och teknisk kunskap om en plånbokslösnings relevanta arkitekturer och om det system för elektronisk identifiering inom ramen för vilket de tillhandahålls, samt om de hot och risker som är relevanta för dessa arkitekturer.

b) Kunskap om tillgängliga säkerhetslösningar och deras egenskaper i enlighet med bilagan till genomförandeförordning (EU) 2015/1502.

c) Kunskap om den verksamhet som bedrivs med stöd av intyg om överensstämmelse som tillämpas på komponenter i plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls, som certifieringsobjekt.

d) Detaljerad kunskap om den tillämpliga nationella certifieringsordning som inrättats i enlighet med kapitel II.

3. Certifieringsorganen ska särskilt bedriva sin kontrollverksamhet på grundval av följande information:

a) Information från nationella ackrediteringsorgan och berörda marknadskontrollmyndigheter.

b) Information som framkommer genom deras egna eller andra myndigheters kontroller och utredningar.

c) Klagomål och överklaganden som mottagits i enlighet med artikel 15.

Artikel 10

Underentreprenad

Certifieringsorganen får lägga ut utvärderingsverksamheten, i enlighet med artikel 13, på tredje part. Om utvärderingsverksamhet läggs ut på entreprenad ska de nationella certifieringsordningarna fastställa följande:

(1) Alla underleverantörer till certifieringsorganet som bedriver utvärderingsverksamhet ska, beroende på vad som är tillämpligt och lämpligt för den verksamhet som ska utföras, uppfylla kraven i harmoniserade standarder som EN ISO/IEC 17025:2017 för provning, EN ISO/IEC 17020:2012 för kontroll, EN ISO/IEC 1–17021:2015 för revision och EN ISO/IEC 17029:2019 för validering och verifiering.

(2) Certifieringsorganen ska ta ansvar för all utvärderingsverksamhet som läggs ut på andra organ och visa att de har vidtagit lämpliga åtgärder under ackrediteringen, bland annat genom att i tillämpliga fall förlita sig på sina underleverantörers egen ackreditering.

(3) I vilken utsträckning förhandssamtycke till underentreprenad ska inhämtas från systemägare eller den klient vars plånbokslösning certifieras enligt certifieringsordningen.

([13]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artikel 11

Anmälan till tillsynsorganet

Certifieringsorganen ska underrätta det tillsynsorgan som avses i artikel 46a.1 i förordning (EU) nr 910/2014 om utfärdande, tillfälligt upphävande och annulering av intyg om överensstämmelse för plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls.

Artikel 12

Hantering av incidenter och sårbarheter

1. Certifieringsorganen ska utan onödigt dröjsmål tillfälligt upphäva intyget om överensstämmelse för plånbokslösningarna och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls, efter att de bekräftat att den säkerhetsöverträdelse eller det äventyrande av säkerheten som anmälts påverkar överensstämmelsen hos plånbokslösningarna, eller hos det system för elektronisk identifiering inom ramen för vilket de tillhandahålls, med kraven i de nationella certifieringsordningarna.

2. Certifieringsorganen ska annulera det intyg om överensstämmelse som tillfälligt har upphävts till följd av en säkerhetsöverträdelse eller ett äventyrande av säkerheten som inte har åtgärdats inom lämplig tid.

3. Certifieringsorganen ska annulera intyg om överensstämmelse, om en identifierad sårbarhet inte har åtgärdats inom lämplig tid i förhållande till dess allvarlighetsgrad och potentiella inverkan, i enlighet med artikel 5c.4 och 5e.2 i förordning (EU) nr 910/2014.

KAPITEL VI

BEDÖMNING AV ÖVERENSSTÄMMELSE

Artikel 13

Utvärderingsverksamhet

1. De nationella certifieringsordningarna ska innehålla metoder och förfaranden som organen för bedömning av överensstämmelse ska använda när de bedriver sin utvärderingsverksamhet i enlighet med EN ISO/IEC 17065:2012 och som ska omfatta minst följande aspekter:

a) Metoder och förfaranden för att bedriva utvärderingsverksamhet, inbegripet sådana som rör krypteringshårdvara, i enlighet med bilaga IV.

b) Granskning av genomförandet av plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls på grundval av det riskregister som anges i bilaga I och som vid behov kompletteras med genomförandespecifika risker.

c) Funktionsprovningar som, när så är möjligt och lämpligt, baseras på provningsserier som definieras i enlighet med tekniska specifikationer eller standarder.

d) Bedömning av underhållsförfarandenas existens och lämplighet, inbegripet åtminstone versionshantering, uppdateringshantering och sårbarhetshantering.

e) Bedömning av underhållsförfarandenas driftseffektivitet, inbegripet åtminstone versionshantering, uppdateringshantering och sårbarhetshantering.

f) Beroendeanalys som plånbokstillhandahållaren tillhandahåller, inbegripet en metod för att bedöma tillitsinformationens godtagbarhet, som ska omfatta de delar som anges i bilaga VI.

g) Sårbarhetsbedömning på lämplig nivå, inbegripet följande:

— En översyn av plånbokslösningens utformning och, i tillämpliga fall, av dess källkod.

— Provning av plånbokslösningens motståndskraft mot angripare med stor angreppspotential för tillitsnivå hög i enlighet med avsnitt 2.2.1 i bilagan till genomförandeförordning (EU) 2015/1502.

h) Bedömning av hotmiljöns utveckling och dess inverkan på plånbokslösningens risktäckning, för att fastställa vilken utvärderingsverksamhet som krävs för plånbokslösningens olika komponenter.

2. De nationella certifieringsordningarna ska innehålla en utvärdering för att avgöra om genomförandet av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket dessa plånbokslösningar tillhandahålls överensstämmer med den arkitektur som anges i artikel 3.5 a, samt en utvärdering för att avgöra om den utvärderingsplan som föreslås tillsammans med genomförandet överensstämmer med den utvärderingsplan som avses i artikel 3.5 c.

3. De nationella certifieringsordningarna ska fastställa urvalsregler för att undvika att identiska utvärderingsverksamheter upprepas och för att fokusera på verksamheter som är specifika för en viss variant. Dessa urvalsregler ska göra det möjligt att utföra funktions- och säkerhetsprov endast på ett urval av varianter av en målkomponent i en plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls och på ett urval av målenheter. De nationella certifieringsordningarna ska kräva att alla certifieringsorgan motiverar sin användning av urval.

4. De nationella certifieringssystemen ska kräva att certifieringsorganet utvärderar krypteringsapplikationen på grundval av de metoder och förfaranden som anges i bilaga IV.

Artikel 14

Certifieringsverksamhet

1. De nationella certifieringsordningarna ska fastställa en attesteringsverksamhet i syfte att utfärda ett intyg om överensstämmelse, i enlighet med tabell 1 i avsnitt V a i EN ISO/IEC 17067:2013, inbegripet följande aspekter:

a) Innehållet i intyget om överensstämmelse i enlighet med bilaga VII.

b) Hur resultatet av utvärderingen ska rapporteras i den offentliga certifieringsrapporten, inklusive åtminstone en sammanfattning av den preliminära revisions- och valideringsplanen, i enlighet med bilaga VIII.

c) Innehållet i det utvärderingsresultat som redovisas i rapporten om certifieringsbedömningen, inbegripet de delar som anges i bilaga VIII.

2. Rapporten om certifieringsbedömningen får göras tillgänglig för samarbetsgruppen och kommissionen.

Artikel 15

Klagomål och överklaganden

De nationella certifieringsordningarna ska innehålla förfaranden eller hänvisningar till tillämplig nationell lagstiftning, som fastställer mekanismen för att effektivt lämna in och hantera klagomål och överklaganden i samband med deras genomförande av certifieringsordningen eller ett utfärdat intyg om överensstämmelse. Dessa förfaranden ska omfatta information till den klagande om hur förfarandet fortskrider och om det beslut som fattats samt information till den klagande om rätten till ett effektivt rättsmedel. De nationella certifieringsordningarna ska kräva att alla klagomål och överklaganden som inte har lösts eller inte kan lösas av certifieringsorganet skickas till systemägaren för bedömning och lösning.

Artikel 16

Kontrollverksamhet

1. De nationella certifieringsorganen ska kräva att certifieringsorganen genomför kontrollverksamhet som består av kontrollutvärdering av förfaranden i kombination med stickprover eller inspektioner.

2. De nationella certifieringsordningarna ska innehålla krav på att systemägarna övervakar att certifieringsorganen fullgör sina skyldigheter enligt förordning (EU) nr 910/2014 och, i tillämpliga fall, enligt nationella certifieringsordningar.

3. De nationella certifieringsordningarna ska innehålla krav på att certifieringsorganen övervakar följande:

a) Att innehavare av ett intyg om överensstämmelse som utfärdats inom ramen för nationella certifieringsordningar uppfyller sina skyldigheter i fråga om certifiering enligt förordning (EU) nr 910/2014 och nationella certifieringsordningar.

b) Att den certifierade plånbokslösningen uppfyller kraven i de nationella certifieringsordningarna.

Artikel 17

Konsekvenser vid bristande efterlevnad

De nationella certifieringsordningarna ska fastställa konsekvenserna av att en certifierad plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls inte uppfyller kraven i denna förordning. Dessa konsekvenser ska omfatta följande aspekter:

(1) Certifieringsorganets skyldighet att informera innehavaren av intyget om överensstämmelse och att begära att innehavaren av intyget om överensstämmelse vidtar korrigerande åtgärder.

(2) Certifieringsorganets skyldighet att informera andra relevanta marknadskontrollmyndigheter om den bristande överensstämmelsen rör relevant unionslagstiftning.

(3) Villkoren för när innehavaren av intyget om överensstämmelse ska vidta korrigerande åtgärder.

(4) Villkoren för certifieringsorganets tillfälliga upphävande av ett intyg om överensstämmelse och för återställande av intyget om överensstämmelse efter det att den bristande överensstämmelsen har korrigerats.

(5) Villkoren för certifieringsorganets annulering av ett intyg om överensstämmelse.

(6) Konsekvenserna av att certifieringsorganet inte uppfyller kraven i den nationella certifieringsordningen.

KAPITEL VII

CERTIFIERINGENS LIVSCYKEL

Artikel 18

Certifieringens livscykel

1. Giltigheten för intyg om överensstämmelse som utfärdats inom ramen för nationella certifieringsordningar ska regelbundet utvärderas av certifieringsorganet i enlighet med kraven i bilaga IX.

2. De nationella certifieringsordningarna ska innehålla ett förfarande för omcertifiering av plånbokslösningar och det system för elektronisk identifiering inom ramen för vilket de tillhandahålls, på begäran av innehavaren av intyget om överensstämmelse innan det ursprungliga intyget om överensstämmelse löper ut. Detta förfarande för omcertifiering ska omfatta en fullständig utvärdering av plånbokslösningen och av det system för elektronisk identifiering inom ramen för vilket den tillhandahålls, inbegripet en sårbarhetsbedömning, i enlighet med de principer som anges i bilaga IX.

3. De nationella certifieringsordningarna ska innehålla ett förfarande för hantering av ändringar i en certifierad plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls. Detta förfarande ska omfatta regler för att avgöra om en ändring ska omfattas av en särskild utvärdering enligt punkt 4 eller av kontrollen av underhållsförfarandets driftseffektivitet enligt bilaga IV.

4. De nationella certifieringsordningarna ska innehålla ett förfarande för särskilda utvärderingar i enlighet med EN ISO/IEC 17065:2012. Detta förfarande för särskilda utvärderingar ska omfatta ett urval av åtgärder som ska genomföras för att hantera den specifika fråga som föranledde den särskilda utvärderingen.

5. De nationella certifieringsordningarna ska fastställa regler för annulering av ett intyg om överensstämmelse.

KAPITEL VIII

REGISTERFÖRING OCH SKYDD AV UPPGIFTER

Artikel 19

Registerföring

1. De nationella certifieringsordningarna ska innehålla krav för certifieringsorgan avseende ett registersystem för all relevant information som tas fram i samband med den bedömning av överensstämmelse som de utför, inbegripet uppgifter som utfärdats och mottagits av tillhandahållare av plånbokslösningar och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls. Registren över sådan information ska lagras på ett säkert sätt. Registren får bevaras elektroniskt och ska vara tillgängliga så länge som krävs enligt unionsrätten eller nationell rätt och i minst fem år efter det att det relevanta intyget om överensstämmelse har annulerats eller löpt ut.

2. De nationella certifieringsordningarna ska innehålla krav på att innehavaren av intyget om överensstämmelse ska lagra följande information på ett säkert sätt vid tillämpningen av denna förordning och i minst fem år efter det att det relevanta intyget om överensstämmelse har annulerats eller löpt ut:

a) Register över den information som lämnats till certifieringsorganet eller någon av dess underleverantörer under certifieringsprocessen.

b) Exempel på hårdvarukomponenter som har inkluderats i certifieringen för plånbokslösningen.

3. De nationella certifieringsordningarna ska kräva att innehavaren av intyget om överensstämmelse på begäran gör den information som avses i punkt 1 tillgänglig för certifieringsorganet eller det tillsynsorgan som avses i artikel 46a.1 i förordning (EU) nr 910/2014.

Artikel 20

Skydd av information

Enligt de nationella certifieringsordningarna ska alla personer eller organisationer som beviljas tillgång till information vid utförandet av verksamhet inom ramen för den nationella certifieringsordningen vara skyldiga att säkerställa säkerheten för och skyddet av företagshemligheter och annan konfidentiell information, samt att bevara immateriella rättigheter, och vidta nödvändiga och lämpliga tekniska och organisatoriska åtgärder för att säkerställa denna konfidentialitet.

KAPITEL IX

SLUTBESTÄMMELSER

Artikel 21

Övergång till en europeisk ordning för cybersäkerhetscertifiering

Denna förordning ska ses över vid antagandet av den första europeiska ordningen för cybersäkerhetscertifiering för plånbokslösningar och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls, i syfte att beakta hur en sådan europeisk ordning för cybersäkerhetscertifiering bidragit till den övergripande certifieringen av plånbokslösningar och de system för elektronisk identifiering inom ramen för vilka de tillhandahålls.

Artikel 22

Ikraftträdande

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 28 november 2024.

På kommissionens vägnar
Ursula VON DER LEYEN
Ordförande

BILAGA I

RISKREGISTER FÖR EU:S DIGITALA IDENTITETSPLÅNBÖCKER

Inledning

I riskregistret beskrivs de huvudsakliga risker och hot som är förenade med plånböckers säkerhet och integritet och som alltid ska hanteras på lämpligt sätt i plånböckernas arkitektur och genomförande. **Högnivårisker** (avsnitt I) är förenade med användares och förlitande parters användning av plånböcker och är förknippade med direkta hot mot plånböckernas tillgångar. Dessutom identifieras några **systemrisker** (avsnitt II) för plånböcker, som i regel är resultatet av en kombination av hot som riktar sig mot hela plånbokssystemet.

Risktyp	Risk-id	Relaterade riskbenämningar
Högnivårisker för plånböcker	R1	Skapande eller användning av en befintlig e-legitimation
	R2	Skapande eller användning av en förfalskad e-legitimation
	R3	Skapande eller användning av förfalskade attribut
	R4	Identitetsstöld
	R5	Datastöld
	R6	Utlämnande av uppgifter
	R7	Datamanipulering
	R8	Dataförlust
	R9	Obehörig transaktion
	R10	Manipulering av transaktioner
	R11	Avvisande
	R12	Utlämnande av transaktionsuppgifter
	R13	Störning
	R14	Övervakning
Systemrelaterade risker	SR1	Övervakning i grossistledet
	SR2	Skadat anseende
	SR3	Överträdelse av lagstiftningen

I registret identifieras också **tekniska hot** (avsnitt III) mot genomförandet av plånbokslösningen. Dessa hot hänger samman med högnivåriskerna i den meningen att varje hot skulle kunna användas för att utlösa många högnivårisker.

Typ av hot	Hot-id	Relaterade hotbenämningar	Underkategorier av hot
Tekniska hot	TT1	Fysiska angrepp	1.1 *Stöld*
			1.2 *Informationsläckage*
			1.3 *Manipulering*
	TT2	Fel och felkonfigureringar	2.1 *Fel som begåtts vid hanteringen av ett it-system*
			2.2 *Fel på applikationsnivå eller användningsfel*
			2.3 *Utvecklingstidsfel och felkonfigureringar av system*

Typ av hot	Hot-id	Relaterade hotbenämningar	Underkategorier av hot
	TT3	Användning av otillförlitliga resurser	3.1 *Felaktig användning eller konfigurering av plånbokskomponenter*
	TT4	Fel och avbrott	4.1 *Fel eller funktionsfel i utrustning, hårdvara eller system*
			4.2 *Förlust av resurser*
			4.3 *Förlust av stödtjänster*
	TT5	Illvilliga handlingar	5.1 *Avläsning av information*
			5.2 *Nätfiske och spoofing*
			5.3 *Återuppspelning av meddelanden*
			5.4 *Uttömmande attack*
			5.5 *Programvarusårbarheter*
			5.6 *Leveranskedjeattacker*
			5.7 *Sabotageprogram*
			5.8 *Prediktion av slumptal*

I registret förtecknas slutligen **direkta hot mot plånböckerna**, och varje hot är förknippat med ett (icke uttömmande) riskurval (avsnitt IV).

AVSNITT I

Högnivårisker för plånböcker

R1. Skapande eller användning av en befintlig e-legitimation

Med skapande eller användning av en befintlig e-legitimation avses skapande av en e-legitimation i en plånbok som finns i verkligheten och tilldelas en annan användare. Denna risk leder i huvudsak till risker för identitetsstöld (R4) och obehöriga transaktioner (R9).

R2. Skapande eller användning av en förfalskad e-legitimation

Med skapande eller användning av en förfalskad e-legitimation avses skapande av en e-legitimation i en plånbok som inte finns i verkligheten.

R3. Skapande eller användning av förfalskade attribut

Med skapande eller användning av förfalskade attribut avses skapande eller användning av attribut som inte kan valideras för att utfärdas av den påstådda tillhandahållaren och inte är tillförlitliga.

R4. Identitetsstöld

Med identitetsstöld avses obehörigt förvärv av plånboksenheten eller förlust av autentiseringsfaktorer som gör det möjligt att utge sig för att vara en person.

R5. Datastöld

Med datastöld avses obehörig hämtning av data. Datastöld är också förknippad med hot, såsom dataavläsning (obehörig insamling av data under överföring) och dekryptering av data (obehörig avkodning av krypterade data), som i vissa fall sannolikt kommer att leda till utlämnande av uppgifter (R6).

R6. Utlämnande av uppgifter

Med utlämnande av uppgifter avses obehörig exponering av personuppgifter, inbegripet särskilda kategorier av personuppgifter. Risken för integritetsintrång är mycket snarlik, sett ur ett integritetsperspektiv snarare än ett säkerhetsperspektiv.

R7. Datamanipulering

Med datamanipulering avses obehörig ändring av data.

R8. Dataförlust

Med dataförlust avses en situation där data som lagras i plånboken går förlorade genom missbruk eller illvillig handling. Denna risk är ofta en sekundär risk till datamanipulering (R7) eller störning (R13), där alla eller delar av data inte kan återställas.

R9. Obehörig transaktion

Med obehöriga transaktioner avses operativ verksamhet som utförs utan plånboksanvändarens tillstånd eller vetskap. I många fall kan en obehörig transaktion leda till identitetsstöld (R4) eller utlämnande av uppgifter (R6). Det är också förknippat med obehöriga transaktioner, såsom missbruk av krypteringsnycklar.

R10. Manipulering av transaktioner

Med manipulering av transaktioner avses obehörig ändring av operationer i plånboken. Manipulering av transaktioner är ett integritetsangrepp och är kopplad till ett dataintegritetsintrång.

R11. Avvisande

Med avvisande avses en situation där en berörd part kan förneka att den begått en handling eller deltagit i en transaktion, och där andra berörda parter inte har tillräckliga bevis för att motsäga den.

R12. Utlämnande av transaktionsuppgifter

Med utlämnande av transaktionsuppgifter avses utlämnande av information om en transaktion mellan berörda parter.

R13. Störning

Med störning avses ett avbrott eller en försämring av plånbokens normala drift. En specifik typ av störning är utestängning av användare, som avser att en användare inte kan få tillgång till sitt konto eller sin plånbok.

R14. Övervakning

Med övervakning, eller bevakning, avses obehörig spårning eller observation av en plånboksanvändares aktivitet, kommunikation eller data. Övervakning är ofta förknippad med inferens, med vilket det avses att känslig eller personlig information härleds från till synes offentliga uppgifter.

AVSNITT II

Systemrelaterade risker

Dessa risker används inte i förteckningen över hot, eftersom de vanligtvis är en följd av flera hot, som upprepas på ett sätt som hotar hela systemet.

SR1 Övervakning i grossistledet

Med övervakning i grossistledet avses spårning eller observation av många användares aktivitet genom deras plånboks kommunikation eller data. Övervakning i grossistledet är ofta förknippad med övervakning (R14) och inferens på global nivå, där information om många användare kombineras för att härleda känsliga eller personliga uppgifter om användare eller för att identifiera statistiska trender som kan användas för att utforma ytterligare attacker.

SR2 Skadat anseende

Med skadat anseende avses den skada som åsamkats en organisations eller ett statligt organs anseende. Skadat anseende uppstår också till följd av andra risker när en överträdelse eller incident rapporteras i medierna och får organisationen att framstå i ett ofördelaktigt ljus. Skadat anseende kan leda till ytterligare risker, såsom förlorat förtroende, till följd av användarens rimliga tvivel, och förlust av ekosystem när hela ekosystemet kollapsar.

SR3 Överträdelse av lagstiftningen

Med överträdelse av lagstiftningen avses en situation där tillämpliga lagar, förordningar eller standarder inte kan följas. När det gäller plånboken kommer alla hot sannolikt att leda till någon form av överträdelse av lagstiftningen, eftersom lösningens säkerhet och integritet är rättsliga krav.

AVSNITT III:

Tekniska hot

Alla tekniska hot är inte kopplade till specifika risker med plånböckerna, eftersom många av dem är medel som kan användas för att genomföra attacker som är förknippade med många olika risker.

TT1 Fysiska angrepp

1.1 *Stöld*

Med stöld avses stöld av hårdvara som kan ändra plånbokens funktion (om hårdvaran är stulen och plånboksenheten inte är tillräckligt skyddad). Detta kan bidra till många risker, bland annat identitetsstöld (R4), datastöld (R5) och obehöriga transaktioner (R9).

1.2 *Informationsläckage*

Med informationsläckage avses obehörig åtkomst, exponering eller delning av information efter fysisk åtkomst till plånboken. Detta kan särskilt bidra till utlämnande av uppgifter (R6) och datastöld (R5).

1.3 *Manipulering*

Med manipulering avses en kränkning av integriteten hos en eller flera komponenter i plånboksenheten eller hos de komponenter som plånboksenheten är beroende av, till exempel användarenheten eller dess operativsystem. Detta kan särskilt bidra till datamanipulering (R7), dataförlust (R8) och manipulering av transaktioner (R10). När manipuleringen är inriktad på programvarukomponenter kan den bidra till många risker.

TT2 Fel och felkonfigureringar

2.1 *Fel som begåtts vid hanteringen av ett it-system*

Med fel som begåtts vid hanteringen av ett it-system avses informationsläckage, delning eller skada som orsakas av användarnas missbruk av it-tillgångar (bristande medvetenhet om applikationsfunktioner) eller av felaktig konfigurering eller förvaltning av it-tillgångar.

2.2 *Fel på applikationsnivå eller användningsfel*

Med fel på applikationsnivå eller användningsfel avses funktionsfel i applikationen på grund av ett fel i själva applikationen eller ett fel som begåtts av en av användarna (plånboksanvändare och förlitande parter).

2.3 *Utvecklingstidsfel och felkonfigureringar av system*

Med utvecklingstidsfel och felkonfigureringar av system avses funktionsfel eller sårbarheter som orsakas av felaktigt utvecklade eller konfigurerade it-tillgångar eller affärsprocesser (otillräckliga specifikationer av it-produkter, otillräcklig användbarhet, osäkra gränssnitt, olämpliga policy- och förfarandeflöden, konstruktionsfel).

TT3 Användning av otillförlitliga resurser

Med användning av otillförlitliga resurser avses en verksamhet som leder till oavsiktlig skada på grund av bristfälligt definierade förtroendeförhållanden, till exempel förtroende för en tredjepartsleverantör utan tillräcklig säkerhet.

3.1 *Felaktig användning eller konfigurering av plånbokskomponenter*

Med felaktig användning eller konfigurering av plånbokskomponenter avses oavsiktlig skada på plånbokskomponenter på grund av plånboksanvändares felaktiga användning eller felkonfigurering eller av otillräckligt utbildade utvecklare, eller på grund av bristande anpassning till förändringar i hotbilden, i regel användning av sårbara tredjepartskomponenter eller exekveringsplattformar.

TT4 Fel och avbrott

4.1 *Fel eller funktionsfel i utrustning, hårdvara eller system*

Med fel eller funktionsfel i utrustning avses oavsiktlig skada på it-tillgångar på grund av fel eller funktionsfel i utrustningen, inbegripet tillhandahållarens infrastruktur och användarenheter.

4.2 *Förlust av resurser*

Med förlust av resurser avses avbrott eller funktionsfel på grund av att sådana resurser inte är tillgängliga, till exempel som underhållsdelar.

4.3 *Förlust av stödtjänster*

Med förlust av stödtjänster avses avbrott eller funktionsfel på grund av att de stödtjänster som krävs för korrekt drift av systemet inte är tillgängliga, inbegripet nätkonnektivitet för tillhandahållarens infrastruktur och användarenheten.

TT5 Illvilliga handlingar

5.1 *Avläsning av information*

Med avläsning av information avses insamling av information som på ett otillbörligt sätt förvärvats vid överföring, inbegripet man-i-mitten-attacker.

5.2 *Nätfiske och spoofing*

Med nätfiske avses insamling av information som tillhandahålls av användaren efter en bedräglig interaktion, ofta kopplad till spoofing av legitima kommunikationsmedel och webbplatser. Dessa hot riktar sig mot användaren och bidrar i regel till identitetsstöld (R4) och obehöriga transaktioner (R9), ofta genom datastöld (R5) eller utlämnande av uppgifter (R6).

5.3 *Återuppspelning av meddelanden*

Med återuppspelning av meddelanden avses återanvändning av tidigare avlästa meddelanden för att utföra obehöriga transaktioner, ofta på protokollnivå. Detta tekniska hot bidrar främst till obehöriga transaktioner, vilket sedan kan leda till andra risker beroende på transaktionen.

5.4 *Uttömmande attack*

Med uttömmande attack avses en säkerhetsöverträdelse, ofta en konfidentialitetsincident, till följd av ett stort antal interaktioner tills svaren ger värdefull information.

5.5 *Programvarusårbarheter*

Hot i form av programvarusårbarheter är en säkerhetsöverträdelse till följd av ett utnyttjande av en programvarusårbarhet i plånbokens komponenter eller i de programvaru- och hårdvarukomponenter som används vid genomförandet av plånboken, inbegripet offentliggjorda och icke offentliggjorda sårbarheter (0 dagar).

5.6 *Leveranskedjeattacker*

Med leveranskedjeattack avses en säkerhetsöverträdelse till följd av attacker mot plånbokstillhandahållaren eller dess användare för att möjliggöra ytterligare attacker mot själva plånboken.

5.7 *Sabotageprogram*

Med sabotageprogram avses en säkerhetsöverträdelse till följd av skadliga applikationer som utför oönskade och obehöriga handlingar mot plånboken.

5.8 *Prediktion av slumptal*

Med prediktion av slumptal avses möjligheten till uttömmande attacker genom att helt eller delvis förutspå genererade slumpmässiga tal.

AVSNITT IV

Hot mot plånböckerna

I detta sista avsnitt presenteras ett urval av typiska hotscenarier som är specifika för plånböckerna och som är indelade efter de viktigaste relaterade högnivåriskerna enligt ovan. Denna förteckning innehåller hot som måste täckas, men den utgör inte någon uttömmande förteckning över hot, som i hög grad är beroende av den valda plånbokslösningens struktur och hotmiljöns utveckling. I riskbedömningen och de föreslagna åtgärderna kan plånbokstillhandahållaren dessutom endast ansvara för de komponenter som omfattas av certifieringen*.

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR1	En angripare kan återkalla pseudonymer utan motiverade skäl.	Skapande eller användning av en förfalskad e-legitimation (R2)
TR2	En angripare kan utfärda förfalskade e-legitimationer som inte finns.	Skapande eller användning av en förfalskad e-legitimation (R2)
TR3	En angripare kan börja utfärda obehöriga personidentifieringsuppgifter.	Skapande eller användning av en förfalskad e-legitimation (R2)
TR4	En angripare kan få en administratör att föra in fel tillhandahållare av personidentifieringsuppgifter i förteckningen över betrodda tillhandahållare av personidentifieringsuppgifter.	Skapande eller användning av en förfalskad e-legitimation (R2)
TR5	En angripare kan kringgå förfarandet för styrkande av identitet på distans.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR6	En angripare kan kringgå det fysiska förfarandet för styrkande av identitet.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR7	En angripare kan kringgå förfarandet för styrkande av identitet som är kopplat till användningen av ett (kvalificerat) certifikat på distans.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR8	En angripare kan få tillgång till en plånbok som inte är bunden till en person.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR9	En angripare kan överlista tekniska och förfarandemässiga kontroller för att skapa fel personidentifieringsuppgifter.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR10	En angripare kan aktivera en ny plånbok på en ogiltig krypteringshårdvara.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)
TR11	En angripare kan kringgå förfarandet för styrkande av identitet som är kopplat till användningen av ett befintligt medel för elektronisk identifiering.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR12	En angripare kan kringgå den kontroll som tillhandahållaren av personidentifieringsuppgifter gör av att plånboken står under användarens kontroll och kan få en personidentifieringsuppgift utfärdad för en kompromitterad plånbok under angriparens kontroll.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR13	En angripare kan få in en giltig personidentifieringsuppgift i en ogiltig plånboksenhet.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR14	En tillhandahållare av personidentifieringsuppgifter kan utfärda förfalskade identiteter där identiteten är förknippad med en befintlig person.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR15	En angripare kan koppla en personidentifieringsuppgift till fel plånbok eftersom tillhandahållaren av personidentifieringsuppgifter inte kan koppla personidentifieringsuppgiften till rätt plånbok.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR16	En angripare kan få användaren att godkänna aktiveringen av en ny plånboksenhet/plånboksinstans under angriparens kontroll – även med efterföljande kontroll av intyg.	Skapande eller användning av en befintlig e-legitimation (R1)/Skapande eller användning av en förfalskad e-legitimation (R2)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR17	En angripare kan utfärda en personidentifieringsuppgift från en annan stat för att få tillgång till berörda medborgares uppgifter/digitala tillgångar.	Skapande eller användning av en befintlig e-legitimation (R1)/Identitetsstöld (R4)/Obehörig transaktion (R9)
TR18	En angripare kan överlista tekniska och förfarandemässiga kontroller för att skapa felaktiga (kvalificerade) elektroniska attributsintyg.	Skapande eller användning av förfalskade attribut (R3)
TR19	En angripare kan uppvisa (kvalificerade) elektroniska attributsintyg som inte har utfärdats på ett giltigt sätt till dem.	Skapande eller användning av förfalskade attribut (R3)
TR20	En angripare kan angripa plånbokens kryptografiska länkningsmekanism mellan personidentifieringsuppgiften och ett (kvalificerat) elektroniskt attributsintyg som inte bör utfärdas till den.	Skapande eller användning av förfalskade attribut (R3)
TR21	En angripare kan använda ett (kvalificerat) elektroniskt attributsintyg i en plånbok, även om den fysiska motsvarigheten till det (kvalificerade) elektroniska attributsintyget har löpt ut eller är ogiltigt.	Skapande eller användning av förfalskade attribut (R3)
TR22	En angripare kan kringgå den kontroll som tillhandahållaren av det (kvalificerade) attributsintyget gör av att plånboken står under användarens kontroll och kan få ett (kvalificerat) attributsintyg utfärdat för en komprometterad plånbok under angriparens kontroll.	Skapande eller användning av förfalskade attribut (R3)
TR23	En angripare kan förfalska elektroniska attributsintyg.	Skapande eller användning av förfalskade attribut (R3)
TR24	En angripare kan föra in förfalskade elektroniska attributsintyg i en plånbok.	Skapande eller användning av förfalskade attribut (R3)
TR25	Plånboken kan uppvisa attribut för en förlitande part utan användarens godkännande.	Utlämnande av uppgifter (R6)
TR26	Personidentifieringsuppgifter, (kvalificerade) elektroniska attributsintyg eller pseudonymer kan uppvisas för fel förlitande part.	Utlämnande av uppgifter (R6)
TR27	En angripare kan inleda en illasinnad förnyelse av ett elektroniskt attributsintyg.	Utlämnande av uppgifter (R6)
TR28	En angripare kan få en användare att felaktigt godkänna en begäran om elektroniska attributsintyg (nätfiske eller annat).	Utlämnande av uppgifter (R6)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR29	En angripare kan läcka attribut från plånboken och identifiera plånboksanvändaren om identifiering inte krävs/är tillåten.	Utlämnande av uppgifter (R6)
TR30	En angripare kan överlista tekniska och förfarandemässiga kontroller för att hämta uppgifter.	Utlämnande av uppgifter (R6)
TR31	En begäran kan läcka till en angripare.	Utlämnande av uppgifter (R6)
TR32	En angripare kan få kunskap om den inbyggda policyn för utlämnande för attribut och presentera attribut som ingår i plånboksenheternas aktuella begäran.	Utlämnande av uppgifter (R6)
TR33	En angripare kan hämta loggar eller delar av dem.	Utlämnande av uppgifter (R6)
TR34	En angripare kan veta om en plånbok är installerad på samma enhet som han eller hon använder, eller på en annan enhet, och få information om den.	Utlämnande av uppgifter (R6)
TR35	En angripare kan få en kunskapsfaktor som används för användarautentisering av krypteringsapplikationen.	Utlämnande av uppgifter (R6)
TR36	Det elektroniska attributsintyget om en person som uppvisas i flera transaktioner med en förlitande part, eller mellan olika förlitande parter, gör det oavsiktligt möjligt att koppla flera transaktioner till den berörda personen.	Utlämnande av uppgifter (R6)
TR37	En offentlig förteckning över återkallelser av intyg/förlitande parter kan innehålla information om användarens användning av intyget (t.ex. plats, IP-adress osv.).	Utlämnande av uppgifter (R6)
TR38	Eftersom förlitande parter inte kan bevisa användarens samtycke till delade attribut kan de påverka loggarnas integritet.	Utlämnande av uppgifter (R6)
TR39	En angripare kan olagligen spåra plånboksanvändare med hjälp av unika/spårbara identifieringskoder.	Utlämnande av uppgifter (R6)/Övervakning (R14)
TR40	En förlitande part som består av flera enheter som var och en får begära/behandla olika mycket, kan begära och behandla uppgifter som de inte har laglig grund för.	Utlämnande av uppgifter (R6)/Obehörig transaktion (R9)
TR41	En angripare kan undergräva plånbokens integritets- och äkthetskontroller av personidentifieringsuppgifter för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR42	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar de begärda attributens integritet och äkthet för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR43	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar alla begärda attribut som tillhör samma användare för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR44	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar att personidentifieringsuppgiften är giltig och har utfärdats av en betrodd tillhandahållare av personidentifieringsuppgifter för att alltid få ett positivt resultat.	Datamanipulering (R7)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR45	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar att ett kvalificerat elektroniskt attributsintyg är giltigt och har utfärdats av en kvalificerad tillhandahållare av betrodda tjänster som är registrerad för att utfärda det kvalificerade elektroniska attributsintyget för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR46	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar om personidentifieringsuppgiften har återkallats av tillhandahållaren av personidentifieringsuppgifter för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR47	En angripare kan kringgå eller undergräva plånbokens kontroller som verifierar om det (kvalificerade) elektroniska attributsintyget har återkallats av tillhandahållaren av (kvalificerade) elektroniska attributsintyg för att alltid få ett positivt resultat.	Datamanipulering (R7)
TR48	En angripare kan ändra innehållet i säkerhetskopierings- och återställningsdata som uteslutande bör stå under användarens kontroll.	Datamanipulering (R7)/Dataförlust (R8)
TR49	En angripare kan ändra transaktionshistoriken för en viss plånboksinstans från aktivitetsloggarna.	Datamanipulering (R7)/Dataförlust (R8)
TR50	En angripare kan avläsa data under anslutningen från plånboken till förlitande parter.	Datastöld (R5)/Utlämnande av uppgifter (R6)
TR51	En angripare kan övertyga en användare om att dela personuppgifter (dvs. personidentifieringsuppgifter, elektroniska attributsintyg, pseudonymer, elektroniska underskrifter, loggar och andra uppgifter) med angriparen eller med en tredje part som användaren inte hade för avsikt att dela uppgifterna med.	Datastöld (R5)/Utlämnande av uppgifter (R6)
TR52	En angripare kan läsa transaktionshistoriken för en viss plånboksinstans från aktivitetsloggarna.	Datastöld (R5)/Utlämnande av uppgifter (R6)
TR53	En angripare kan exportera eller hämta kryptografiskt nyckelmaterial utanför krypteringshårdvaran.	Datastöld (R5)/Utlämnande av uppgifter (R6)/Obehörig transaktion (R9)
TR54	En angripare kan läsa innehållet i säkerhetskopierings- och återställningsdata som uteslutande bör stå under användarens kontroll.	Datastöld (R5)/Utlämnande av uppgifter (R6)
TR55	En angripare kan kringgå metoden för användarautentisering för att använda en pseudonym som genereras av en plånboksenhet.	Identitetsstöld (R4)
TR56	En angripare kan föreslå en applikation som efterliknar en viss legitim plånbok för användarna.	Identitetsstöld (R4)
TR57	En angripare kan exportera plånboksdata, inklusive personidentifieringsuppgifter, (kvalificerade) elektroniska attributsintyg eller loggar.	Identitetsstöld (R4)
TR58	En angripare kan exportera kryptografiskt bindningsmaterial.	Identitetsstöld (R4)
TR59	En angripare kan överta identiteter genom plånbokens krypteringsnycklar.	Identitetsstöld (R4)
TR60	En angripare kan kopiera en annan användares personliga plånboksenhet på sin personliga enhet och använda den.	Identitetsstöld (R4)/Inrättande eller användning av en befintlig e-legitimation (R1)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR61	Myndigheterna i en annan stat kan be användaren att visa och/eller dela alla plånboksuppgifter i en närhetssituation, t.ex. när användaren passerar den statens gräns.	Identitetsstöld (R4)/Övervakning (R14)
TR62	Användarna kan inte överföra sina transaktionsloggar efter fel på en användarenhet, vilket leder till att tidigare transaktioner inte längre kan spåras på den nya plånboken.	Avvisande (R11)
TR63	Användarna kan inte återställa sina transaktionsloggar efter fel på en användarenhet, vilket leder till att tidigare transaktioner inte längre kan spåras på den nya plånboken.	Avvisande (R11)
TR64	Förlitande parter kan ha svårt att bevisa samtycke till elektroniska underskrifter på distans.	Avvisande (R11)
TR65	En angripare kan översvämma anslutningen med begäranden under anslutningen till förlitande parter.	Störning (R13)
TR66	En angripare kan översvämma en statustjänst med anslutningar till förlitande parter.	Störning (R13)
TR67	En angripare kan få attributet att se ut som om det är ifrågasatt/avvisat, trots att det står att attributet är giltigt.	Störning (R13)
TR68	En angripare kan återkalla en personidentifieringsuppgift utan motiverade skäl.	Störning (R13)
TR69	En angripare kan återkalla en personidentifieringsuppgift utan användarens samtycke.	Störning (R13)
TR70	En angripare kan återkalla ett (kvalificerat) elektroniskt attributsintyg utan motiverade skäl.	Störning (R13)
TR71	En angripare kan återkalla ett (kvalificerat) elektroniskt attributsintyg utan användarens samtycke.	Störning (R13)
TR72	En angripare kan utlösa flera begäranden om identifiering utan att de erkänns som avsiktliga herrelösa förfrågningar.	Störning (R13)
TR73	En angripare kan skicka flera begäranden utan uppföljande transaktion.	Störning (R13)
TR74	En angripare kan låta en förlitande part begära identifiering utan matchande identifiering (svar) och fullständig kontroll.	Störning (R13)
TR75	En angripare kan skicka ett svar på en begäran efter det att svarstiden har gått ut, eller liknande situationer som leder till en störning.	Störning (R13)
TR76	En förlitande part kan skicka flera ogiltiga begäranden.	Störning (R13)
TR77	En angripare kan skicka flera ogiltiga begäranden till en plånbokstillhandahållare.	Störning (R13)
TR78	En angripare kan göra så att en medlemsstat inte kan återkalla en icke-betrodd tillhandahållare av personidentifieringsuppgifter från förteckningen över betrodda tillhandahållare av personidentifieringsuppgifter.	Störning (R13)
TR79	En angripare kan förhindra tillfälligt upphävande eller återkallelse av en plånbok.	Störning (R13)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR80	En angripare kan blockera transaktioner av förlitande parter, användare och/eller tillhandahållare av personidentifieringsuppgifter.	Störning (R13)
TR81	En angripare kan avaktivera eller göra en krypteringshårdvara otillgänglig.	Störning (R13)
TR82	En angripare kan göra så att tillhandahållaren av personidentifieringsuppgifter inte kan återkalla eller tillfälligt upphäva personidentifieringsuppgifter.	Störning (R13)/Obehörig transaktion (R9)
TR83	En förlitande part kan härleda fler av användarens identitetsuppgifter än de uppgifter som delas med den.	Övervakning (R14)
TR84	En grupp samverkande förlitande parter eller tillhandahållare av personidentifieringsuppgifter kan härleda fler av användarens identitetsuppgifter än de uppgifter som de känner till.	Övervakning (R14)
TR85	En angripare kan spåra en användare genom att använda användarens personidentifieringsuppgifter om identifiering av användaren inte krävs.	Övervakning (R14)
TR86	En angripare kan sammanställa en förfalskad presentation av (kvalificerade) elektroniska attributsintygskombinationer.	Manipulering av transaktioner (R10)
TR87	En angripare kan aktivera/överta plånboken på distans (t.ex. en bankapp med en inbyggd begäran om autentisering eller attestering) utan användarens uttryckliga samtycke eller exklusiva kontroll, i situationer där användaren inte känner till (t.ex. sover) eller inte kan se den förlitande parten.	Manipulering av transaktioner (R10)
TR88	En angripare kan göra ändringar i en begärans metadata (tjänstens namn, användning osv.).	Manipulering av transaktioner (R10)
TR89	En angriparna kan göra ändringar i svarsinformationen (tjänstens status, engångsnycklar osv.).	Manipulering av transaktioner (R10)
TR90	En angripare kan göra ändringar i en begärans attributinformation (efterfråga för mycket information osv.).	Manipulering av transaktioner (R10)
TR91	En förlitande part kan återuppspela delar från en tidigare session vid en annan session.	Manipulering av transaktioner (R10)
TR92	En angripare kan ersätta eller ändra en personidentifieringsuppgift under överföringen från tillhandahållaren av personidentifieringsuppgifter till plånboksenheten.	Manipulering av transaktioner (R10)
TR93	En angripare kan ersätta eller ändra en personidentifieringsuppgift under överföringen från plånboksenheten till den förlitande parten online.	Manipulering av transaktioner (R10)
TR94	En angripare kan ersätta eller ändra en personidentifieringsuppgift under överföringen från plånboksenheten till den förlitande parten offline.	Manipulering av transaktioner (R10)
TR95	En angripare kan utfärda en personidentifieringsuppgift utan användarens samtycke.	Obehörig transaktion (R9)
TR96	En angripare kan använda återkallade eller ogiltiga inbyggda policyer för utlämnande, eventuellt utan de förlitande parternas vetskap.	Obehörig transaktion (R9)
TR97	En angripare kan lura plånboken att verifiera felaktiga elektroniska underskrifter.	Obehörig transaktion (R9)
TR98	En angripare kan använda plånboken utanför användarens kontroll.	Obehörig transaktion (R9)

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR99	En angripare kan övertyga en användare om att autentisera och godkänna transaktioner med en angripare eller en obehörig tredje part.	Obehörig transaktion (R9)
TR100	En angripare kan få en användare att underteckna elektroniskt utan att presentera innehållet för användaren eller efter att ha presenterat fel innehåll.	Obehörig transaktion (R9)
TR101	En angripare kan kringgå åtkomstkontrollen av användarens konto hos plånbokstillhandahållaren.	Obehörig transaktion (R9)
TR102	En angripare kan utge sig för att vara en förlitande part under anslutningen till förlitande parter.	Obehörig transaktion (R9)/Utlämnande av uppgifter (R6)
TR103	Användaren bakom den förlitande partens webbläsaranslutning kan skilja sig från användaren bakom den förlitande partens plånboksanslutning.	Obehörig transaktion (R9)/Utlämnande av uppgifter (R6)/Identitetsstöld (R4)
TR104	En angripare kan övertyga användaren om att återkalla användarens plånbok utan anledning.	Obehörig transaktion (R9)/Störning (R13)
TR105	En angripare kan utföra man-i-mitten-attacker.	Obehörig transaktion (R9)/Utlämnande av uppgifter (R6)/Övervakning (R14)
TR106	En angripare kan uppvisa ogiltiga eller återkallade attribut från en plånbok som inte regelbundet ansluts till nätet.	Påverkan på olika risker
TR107	En angripare kan stjäla information från en användare genom att manipulera en plånbok.	Påverkan på olika risker
TR108	En angripare kan utge sig för att vara användaren genom att återuppspela/efterlikna en begäran om data (t.ex. autentisering), som framstår som giltig.	Påverkan på olika risker
TR109	En angripare kan återuppspela en inbyggd policy för utlämnande för en användare för att efterlikna en godkänd begäran.	Påverkan på olika risker
TR110	En angripare kan utnyttja plånboksanvändarnas brist på information eller oskäliga dröjsmål efter en säkerhetsöverträdelse eller ett äventyrande av säkerheten.	Påverkan på olika risker
TR111	En angripare kan ändra en tidigare installerad legitim plånboksinstans för att lägga till skadliga egenskaper.	Påverkan på olika risker
TR112	En angripare kan ändra en legitim plånboksinstans och presentera den för användarna som en legitim sådan.	Påverkan på olika risker
TR113	En angripare kan överlista själva mekanismen för användarautentisering för att kringgå autentiseringen av plånboksanvändaren.	Påverkan på olika risker
TR114	En angripare kan lägga in skadlig kod eller bakdörrar i plånbokskoden under dess införande i användarenheten.	Påverkan på olika risker
TR115	En angripare kan lägga in skadlig kod eller bakdörrar i plånbokskoden under dess utveckling.	Påverkan på olika risker
TR116	En angripare kan manipulera genereringen av slumptal för att minska entropin tillräckligt för att möjliggöra attacker.	Påverkan på olika risker

ID *Identifieringskod*	Hotbeskrivning *Beskrivning av det identifierade hotet**	Riskbenämning *Relaterade risker*
TR117	En angripare kan manipulera användarenheter i leveranskedjan för att inkludera kod eller konfigureringar som inte uppfyller plånbokens användningsvillkor.	Påverkan på olika risker
TR118	En angripare kan aktivera en plånboksenhet med hjälp av manipulerad krypteringshårdvara som kontrolleras av angriparna.	Påverkan på olika risker
TR119	En angripare kan läsa information som skickas till krypteringsapplikationen och/eller krypteringshårdvaran.	Påverkan på olika risker
TR120	En angripare kan skicka godtycklig information till krypteringsapplikationen.	Påverkan på olika risker
TR121	En angripare kan stjäla information genom att avläsa utbytet mellan krypteringsapplikationen och krypteringshårdvaran.	Påverkan på olika risker
TR122	En angripare kan skicka godtycklig information till krypteringshårdvaran.	Påverkan på olika risker
TR123	En angripare kan skicka information till krypteringshårdvaran och kringgå krypteringsapplikationen.	Påverkan på olika risker
TR124	En angripare kan använda nätfiske för att få användare till en falsk plånbok och webbapplikation för hantering av personidentifieringsuppgifter.	Påverkan på olika risker
TR125	En angripare kan ersätta en plånboks nycklar med andra nycklar för att skapa meddelanden som ska användas vid en annan attack.	Påverkan på olika risker
TR126	En angripare kan ändra eller förstöra en plånboks nycklar, vilket gör vissa funktioner i plånboken oanvändbara.	Påverkan på olika risker
TR127	En angripare kan kontrollera ett sabotageprogram för att få tillgång till uppgifter som lagras i plånboken.	Påverkan på olika risker
TR128	En angripare kan få tillgång till bevis som genereras i plånboken.	Påverkan på olika risker
TR129	Plånbokstillhandahållare kan få tillgång till objekt i plånboken.	Påverkan på olika risker
TR130	Plånbokstillhandahållare kan få tillgång till bevis som genereras i plånboken.	Påverkan på olika risker
TR131	En angripare kan stjäla en olåst plånboksenhet.	Påverkan på olika risker
TR132	En angripare kan manipulera systemet för att förhindra att vissa händelser loggas.	Påverkan på olika risker
TR133	En angripare kan avläsa kommunikationen mellan plånboksinstansen och krypteringsapplikationen eller återuppspela/efterlikna en användare (t.ex. genom att kapa autentiseringsmekanismen).	Påverkan på olika risker

BILAGA II

KRITERIER FÖR BEDÖMNING AV HURUVIDA TILLITSINFORMATIONEN ÄR GODTAGBAR

Namn	Objekt	Viktiga punkter
EUCC	IKT-produkter	Om utfärdaren: inga (ackrediterade certifieringsorgan) Om omfattningen: — Kontrollera skyddsprofil och säkerhetsmål — Kontrollera nivån av tillförlitlighet hos utvärderingen och ökningarna Om tillförlitligheten: — Kontrollera begränsningar i användardokumentationen — För sammansättningen kan det krävas tillgång till den tekniska utvärderingsrapporten.
EU:s certifieringsordning för molntjänster (EUCS) (när den är tillgänglig)	Molntjänster	Om utfärdaren: inga (ackrediterade certifieringsorgan) Om omfattningen: — Kontrollera beskrivningen av molntjänsten — Kontrollera tillitsnivå och tilläggsprofiler Om tillförlitligheten: — Kontrollera informationen om öppenhet och, vid behov, informationen om sammansättning
Common Criteria-system som drivs i EU, inklusive SOG-IS-system	IKT-produkter	Om utfärdaren: inga (medlemsstater) Om omfattningen: — Kontrollera skyddsprofil och säkerhetsmål — Kontrollera tillitsnivå och höjningar Om tillförlitligheten: — Kontrollera begränsningar i användardokumentationen — För sammansättningen kan det krävas tillgång till den tekniska utvärderingsrapporten.
EN 17640:2018 (FITCEM, inklusive CSPN, BSZ, LINCE och BSZA)	IKT-produkter	Om utfärdaren: — Kontrollera systemet och kraven för certifieringsorgan Om omfattningen: — Kontrollera produktbeskrivningen — Kontrollera säkerhetspåståenden — Kontrollera tillitsnivån Om tillförlitligheten: — Kontrollera den bedrivna verksamheten och resultaten i rapporten
Certifieringssystem för anordningar för skapande av kvalificerade underskrifter i enlighet med artikel 30 i förordning (EU) nr 910/2014	Anordning för skapande av kvalificerade underskrifter	Om utfärdaren: — Kontrollera systemet och kraven för certifieringsorgan Om omfattningen: — Kontrollera produktbeskrivningen — Kontrollera säkerhetspåståenden — Kontrollera tillitsnivån Om tillförlitligheten: — Kontrollera den bedrivna verksamheten

Namn	Objekt	Viktiga punkter
EN ISO/IEC 27001:2022	LIS	Om utfärdaren: inga (ackrediterade certifieringsorgan) Om omfattningen: — Kontrollera beskrivningen av förvaltningssystemet — Kontrollera försäkran om tillämplighet Om tillförlitligheten: — Kontrollera den bedrivna verksamheten
SOC2	Organisationer	Om utfärdaren: — Kontrollera revisionsstatus Om omfattningen: — Kontrollera förvaltningsredogörelsen och beskrivningen av kontrollerna — Kontrollera försäkran om tillämplighet Om tillförlitligheten: — Kontrollera resultaten i rapporten — Kontrollera mellanliggande rapporter vid behov
MDSCert (GSMA) (när den är tillgänglig)	Mobila enheter	Om utfärdaren: — Kontrollera kraven för certifieringsorgan Om omfattningen: — Kontrollera tillitsnivån — Kontrollera systemets krav Om tillförlitligheten: — Kontrollera verksamheten och resultaten i rapporten
Andra system	Alla komponenter	Om systemet: — Kontrollera systemets relevans och bestämmelser Om utfärdaren: — Kontrollera kraven för certifieringsorgan Om omfattningen: — Kontrollera systemets krav — Kontrollera säkerhetsmålet eller liknande dokument som beskriver kraven rörande säkerhetsfunktioner och rörande tillförlitlighet — Kontrollera produktbeskrivningen och de valda säkerhetsfunktionskraven Om tillförlitligheten: — Kontrollera verksamheten och resultaten i rapporten

BILAGA III

FUNKTIONSKRAV FÖR PLÅNBOKSLÖSNINGAR

Enligt artikel 5a.4, 5a.5, 5a.8 och 5a.14 i förordning (EU) nr 910/2014 ska de funktionella kriterier som ska uppfyllas av en certifierad plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls omfatta funktionskraven för de verksamheter som förtecknas i följande rättsakter:

(1) Kommissionens genomförandeförordning (EU) 2024/2979 ([1]) om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller integritet och centrala funktioner.

(2) Kommissionens genomförandeförordning (EU) 2024/2982 ([2]) om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller protokoll och gränssnitt som ska stödjas av det europeiska ramverket för digital identitet.

(3) Kommissionens genomförandeförordning (EU) 2024/2977 ([3]) om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller personidentifieringsuppgifter och elektroniska attributsintyg som utfärdats för EU:s digitala identitetsplånböcker.

([1]) Kommissionens genomförandeförordning (EU) 2024/2979 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller integritet och centrala funktioner hos EU:s digitala identitetsplånböcker (EUT L, 2024/2079, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) Kommissionens genomförandeförordning (EU) 2024/2982 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller protokoll och gränssnitt som ska stödjas av det europeiska ramverket för digital identitet (EUT L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([3]) Kommissionens genomförandeförordning (EU) 2024/2977 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller personidentifieringsuppgifter och elektroniska attributsintyg som utfärdats för EU:s digitala identitetsplånböcker (EUT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

BILAGA IV

METODER OCH FÖRFARANDEN FÖR UTVÄRDERINGSVERKSAMHETEN

1. **Granskning av genomförandet av en plånbokslösning**

I en bedömning av överensstämmelse ingår att välja ut specifika utvärderingsverksamheter.

I de nationella certifieringsordningarna ska anges vilken utvärderingsverksamhet som ska användas för att bedöma den information som tillhandahålls och den ska åtminstone omfatta följande:

a) En analys av den information som lämnats för att bekräfta att den är lämplig för en av de arkitekturer som anges i de nationella certifieringsordningarna.

b) En analys av täckningen av de cybersäkerhetsrisker och cybersäkerhetshot som identifierats i riskregistret i bilaga I vid de beskrivna säkerhetskontrollerna.

Den analys som nämns i leden a–b ska bygga på den förklaring och motivering som plånbokstillhandahållaren ger.

2. **Utvärdering av krypteringshårdvaran**

(1) Kritiska operationer, inbegripet kryptografiska beräkningar, behöver inte genomföras fullt ut i krypteringshårdvaran. Den del som genomförs i krypteringshårdvaran ska dock, när den används som en del av plånbokslösningen, garantera skyddet av kritiska operationer mot angrepp från angripare med hög angreppspotential i enlighet med kommissionens genomförandeförordning (EU) 2015/1502 ([1]).

(2) Krypteringshårdvaran eller en del av denna kan ingå i certifieringsobjektet när den tillhandahålls av intygsinnehavaren eller sökanden, eller ligga utanför detta när den är inbyggd i hårdvara som tillhandahålls av slutanvändaren. Dessutom ska det i de nationella certifieringsordningarna anges vilken utvärderingsverksamhet som ska användas för att kontrollera krypteringshårdvarans lämplighet i följande två fall:

   a) Om krypteringsapplikationen är beroende av viss krypteringshårdvara (dvs. om den behöver utvärderas som en sammansatt produkt baserad på krypteringshårdvaran) ska det vid utvärderingen av krypteringsapplikationen krävas tillgång till ytterligare information om certifieringen av krypteringshårdvaran, särskilt dess tekniska utvärderingsrapport.

   b) Om en arkitektur som beaktas i ordningen använder flera krypteringshårdvaror, eller om några av operationerna för kritiska tillgångar utförs utanför krypteringshårdvaran, ska de nationella certifieringsordningarna omfatta utvärderingsverksamhet för att säkerställa att den övergripande lösningen tillhandahåller den förväntade säkerhetsnivån.

(3) Som ett villkor för certifiering inom ramen för nationella certifieringsordningar ska krypteringshårdvaran bedömas utifrån kraven på tillitsnivå hög enligt genomförandeförordning (EU) 2015/1502.

   När villkoren i artikel 3.3 b är uppfyllda ska utvärderingen av krypteringshårdvaran eller en del av denna omfatta en sårbarhetsbedömning enligt EN ISO/IEC 15408–3:2022 på AVA_VAN.5-nivå, i enlighet med bilaga I till kommissionens genomförandeförordning (EU) 2024/482 ([2]), såvida det inte är vederbörligen motiverat för certifieringsorganet att krypteringsapplikationens säkerhetsegenskaper gör det möjligt att använda en lägre bedömningsnivå samtidigt som samma övergripande tillitsnivå hög bibehålls i enlighet med genomförandeförordning (EU) 2015/1502.

([1]) Kommissionens genomförandeförordning (EU) 2015/1502 av den 8 september 2015 om fastställande av tekniska minimispecifikationer och förfaranden för tillitsnivåer för medel för elektronisk identifiering i enlighet med artikel 8.3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (EUT L 235, 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([2]) Kommissionens genomförandeförordning (EU) 2024/482 av den 31 januari 2024 om fastställande av tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) 2019/881 vad gäller antagande av den europeiska Common Criteria-baserade ordningen för cybersäkerhetscertifiering (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(4) I dokumentationen för varje specifik arkitektur ska de nationella certifieringsordningarna dessutom formulera antaganden för denna utvärdering av krypteringshårdvaran enligt vilka motståndskraft mot angripare med hög angreppspotential i enlighet med genomförandeförordning (EU) 2015/1502 kan tillhandahållas och ange vilken utvärderingsverksamhet som ska användas för att bekräfta dessa antaganden och för att efter utfärdandet av intyget bekräfta att antagandena fortfarande är verifierade. De nationella ordningarna ska också kräva att de som ansökt om certifiering förfinar dessa antaganden för deras specifika genomförande och beskriver de åtgärder som vidtagits för att garantera att antagandena kontrolleras under hela certifieringscykeln.

(5) I samtliga fall ska de nationella certifieringsordningarna omfatta utvärderingsverksamhet för att, genom en analys av tillitsinformationen, till exempel säkerhetsmålet för EUCC-certifikat, kontrollera att den tillitsinformation som finns tillgänglig för krypteringshårdvaran är lämplig för plånbokslösningen, bland annat

a) kontrollera att utvärderingens omfattning är lämplig, vilket för EUCC-certifikat till exempel innebär kontroll av att säkerhetsmålet påstås överensstämma med en av de skyddsprofiler som rekommenderas i EUCC,

b) kontrollera att antagandena om driftsmiljön är förenliga med plånbokslösningen, vilket för EUCC-certifikat till exempel innebär att dessa antaganden återfinns i säkerhetsmålet,

c) kontrollera att rekommendationerna i användarvägledningen eller användardokumentationen är förenliga med villkoren för hur krypteringshårdvaran ska användas i plånbokslösningen,

d) kontrollera att de antaganden om krypteringshårdvaror som gjorts i den nationella certifieringsordningen verifieras och omfattas av tillitsinformationen.

(6) I de fall där vissa av kontrollerna inte är helt entydiga ska de nationella certifieringsordningarna kräva att certifieringsorganen anger kompensationskrav för krypteringsapplikationen på grundval av krypteringshårdvaran, som ska ingå i utvärderingen av krypteringsapplikationen. Om detta inte är möjligt ska de nationella certifieringsordningarna betrakta krypteringshårdvaran som olämplig, vilket innebär att ett intyg om överensstämmelse inte ska utfärdas för plånbokslösningen.

3. **Utvärdering av krypteringsapplikationen**

(1) Nationella certifieringsordningar ska kräva att en krypteringsapplikation, som ingår i en plånbokslösning, utvärderas utifrån kraven på minst tillitsnivå hög enligt genomförandeförordning (EU) 2015/1502.

(2) Denna utvärdering ska omfatta en sårbarhetsbedömning enligt EN ISO/IEC 15408–3:2022 på AVA_VAN.5-nivå, i enlighet med bilaga I till genomförandeförordning (EU) 2024/482, såvida det inte är vederbörligen motiverat för certifieringsorganet att krypteringsapplikationens säkerhetsegenskaper gör det möjligt att använda en lägre bedömningsnivå samtidigt som samma övergripande tillitsnivå hög bibehålls i enlighet med genomförandeförordning (EU) 2015/1502.

(3) När krypteringsapplikationen inte tillhandahålls av plånbokstillhandahållaren ska de nationella certifieringsordningarna dessutom formulera antaganden för denna utvärdering av krypteringsapplikationen enligt vilka motståndskraft mot angripare med hög angreppspotential i enlighet med genomförandeförordning (EU) 2015/1502 kan tillhandahållas och specificera den utvärderingsverksamhet som ska bekräfta dessa antaganden och efter utfärdandet av intyget bekräfta att antagandena fortfarande är verifierade. De nationella ordningarna ska också kräva att de som ansökt om certifiering förfinar dessa antaganden för deras specifika genomförande och beskriver de åtgärder som vidtagits för att garantera att antagandena verifieras under hela certifieringscykeln.

(4) I samtliga fall ska de nationella certifieringsordningarna omfatta utvärderingsverksamhet för att, genom en analys av tillitsinformationen, till exempel säkerhetsmålet för EUCC-certifikat, kontrollera att den tillitsinformation som finns tillgänglig för krypteringsapplikationen är lämplig för plånbokslösningen, bland annat

a) kontrollera att utvärderingens omfattning är lämplig, vilket för EUCC-certifikat till exempel innebär kontroll av att säkerhetsmålet påstås överensstämma med en av de skyddsprofiler som rekommenderas i EUCC,

b) kontrollera att antagandena om driftsmiljön är förenliga med plånbokslösningen, vilket för EUCC-certifikat till exempel innebär att dessa antaganden återfinns i säkerhetsmålet,

c) kontrollera att rekommendationerna i användarvägledningen eller användardokumentationen är förenliga med villkoren för hur krypteringsapplikationen ska användas i plånbokslösningen,

d) kontrollera att de antaganden om krypteringsapplikationer som gjorts i den nationella certifieringsordningen verifieras och omfattas av tillitsinformationen.

(5) De nationella certifieringsordningarna ska kräva att utvärderingen av krypteringsapplikationen omfattar alla säkerhetskontroller som genomförs av denna krypteringsapplikation.

4. **Utvärdering av slutanvändarenheten**

Eftersom riskregistret enligt bilaga I till denna förordning identifierar risker som är direkt kopplade till slutanvändarenhetens säkerhet, ska de nationella certifieringsordningarna ange säkerhetskrav för slutanvändarenheter. Eftersom dessa enheter tillhandahålls av slutanvändaren och inte av plånbokstillhandahållaren ska dessa krav dock omfattas av antaganden.

För varje antagande ska plånbokslösningen innehålla en mekanism för att för varje plånboksenhet kontrollera att den underliggande slutanvändarenheten uppfyller antagandet. Sådana mekanismer ska betraktas som säkerhetskontroller och omfattas av utvärderingsverksamhet för att visa både deras lämplighet och effektivitet på lämplig tillitsnivå.

Två exempel anges nedan:

a) En slutanvändarenhet kan innehålla certifierad krypteringshårdvara, som måste visas. I regel görs detta med hjälp av en kryptografisk mekanism för att kontrollera att det i den certifierade krypteringshårdvaran finns en kryptografisk hemlighet som endast finns tillgänglig i den certifierade krypteringshårdvaran. I detta fall bör denna kryptografiska hemlighet betraktas som en kritisk tillgång och omfattas av certifieringen av krypteringshårdvaran och/eller krypteringsapplikationen.

b) Ett typiskt krav för slutanvändarenheter kan vara att enheterna måste ta emot säkerhetsuppdateringar. Eftersom detta krav avser plånboksinstansen behöver den mekanism som används för att kontrollera tillgången till säkerhetsuppdateringar endast omfattas av utvärderingsverksamhet på en tillitsnivå som är lämplig för plånboksinstansen, särskilt eftersom den sannolikt är integrerad i plånboksinstansen.

5. **Utvärdering av plånboksinstansen**

(1) Vid utvärderingen av plånboksinstansen ska hänsyn tas till följande två huvudutmaningar:

a) Plånboksinstansen förekommer sannolikt i en rad varianter av samma basapplikation, där varje variant är specialiserad för en specifik kategori slutanvändarenheter.

b) Plånboksinstansens olika varianter behöver sannolikt uppdateras ofta för att följa utvecklingen av den underliggande säkerhetsplattformen, till exempel när sårbarheter identifieras som kräver ändringar av applikationer.

(2) Vid utvärderingen av plånboksinstansen ska hänsyn tas till dessa specifika utmaningar. En av de omedelbara konsekvenserna är att Common Criteria-ramen kanske inte alltid är lämplig. Därför ska alternativa utvärderingsmetoder övervägas vid behov. De nationella certifieringsordningarna ska beakta användningen av metoden i EN 17640:2018 för följande:

a) Som en del av själva ordningen.

b) Genom nationella ordningar som bygger på metoden.

c) Genom nationella ordningar som bygger på liknande principer men som skapats före utvecklingen av metoden i EN 17640:2018.

(3) Eftersom mervärdet av att göra en fullständig särskild utvärdering av varje variant kan vara begränsat ska de nationella certifieringsordningarna dessutom överväga att ange kriterier som gör det möjligt att genomföra stickprov, för att undvika att identiska utvärderingsverksamheter upprepas och för att fokusera på verksamheter som är specifika för en viss variant. De nationella certifieringsordningarna ska kräva att alla certifieringsorgan motiverar sin användning av urval.

(4) De nationella certifieringsordningarna ska inkludera uppdateringar av plånboksinstansen i den övergripande förändringshanteringsprocess som anges för plånbokslösningen. De ska också fastställa regler för de förfaranden som plånbokstillhandahållaren ska tillämpa för varje uppdatering (t.ex. analys av ändringarnas inverkan på säkerhetskontrollerna) och för den utvärdering som certifieringsorganet ska göra av uppdateringar enligt angivna villkor (t.ex. utvärdering av en ändrad säkerhetskontrolls driftseffektivitet). Förändringshanteringsprocessen är en av de processer vars driftseffektivitet årligen måste kontrolleras i enlighet med artikel 18.3.

6. **Utvärdering av de tjänster och processer som används för tillhandahållande och drift av plånbokslösningen**

(1) För utvärdering av tjänster och processer som har betydelse för tillhandahållandet och driften av plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls ska utvärderingsgruppen samla in bevis genom att bedriva utvärderingsverksamhet som kan omfatta revision, inspektion, verifiering och validering.

(2) Certifieringsorganet ska bekräfta att bevisen är tillräckliga och lämpliga för att ge tillräckliga garantier för att tjänsterna och processerna uppfyller certifieringskraven, genom att bekräfta följande:

a) Att den information som presenteras i beskrivningen av processerna och tjänsterna är korrekt.

b) Att utformningen och kontrollerna av processerna och tjänsterna är lämpliga för att uppfylla utvärderingskriterierna.

c) Att genomförandet av dessa kontroller under en angiven period före utvärderingen är driftseffektiva.

(3) Korrektheten i beskrivningen och driftseffektiviteten i genomförandet av kontroller kan betraktas som verifieringsmål, i den mening som avses i ISO/IEC 17000:2020, för motsvarande påståenden av plånbokstillhandahållaren (dvs. bekräftelse av rimligheten i redan inträffade händelser eller redan uppnådda resultat), medan lämpligheten i utformningen och kontrollerna av tjänsterna och processerna för att uppfylla utvärderingskriterierna kan betraktas som ett valideringsmål, i den mening som avses i ISO/IEC 17000:2020, för motsvarande påstående av plånbokstillhandahållaren (dvs. bekräftelse av rimligheten i en avsedd framtida användning eller ett prognostiserat utfall).

(4) Med tanke på att en plånbokslösning inte får användas innan den är certifierad kan driftseffektiviteten inte bekräftas på grundval av lösningens faktiska drift. Denna ska därför bekräftas med hjälp av bevis som samlats in under tester eller pilotförsök.

(5) Nationella certifieringsordningar kanske redan finns för specifika tjänster och processer, till exempel för anslutning av användare. Användningen av sådana ordningar ska i tillämpliga fall beaktas av de nationella certifieringsordningarna.

7. **Utvärdering av de IKT-tjänster som används för tillhandahållande och drift av plånbokslösningen**

(1) Vissa plånboksarkitekturer kan förlita sig på särskilda IKT-tjänster, inbegripet molntjänster för tillhandahållande och drift av en plånbokslösning, och dessa tjänster kan innehålla känsliga uppgifter och känslig verksamhet. I sådana fall ska de nationella certifieringsordningarna ange säkerhetskrav för dessa IKT-tjänster.

(2) Det finns redan många certifieringsordningar för IKT-tjänster, molntjänster och andra källor till tillitsinformation, bland annat de som förtecknas i bilaga II. De nationella certifieringsordningarna ska, i förekommande och tillämpliga fall, förlita sig på dessa befintliga mekanismer genom en av följande mekanismer:

a) Föreskriva användningen av en specifik ordning eller ett urval av ordningar genom att ange på vilka villkor IKT-tjänster eller molntjänster ska bedömas med hjälp av dessa ordningar.

b) Överlåta valet av bedömning till plånbokstillhandahållaren och använda beroendeanalysen för att analysera lämpligheten hos den tillitsinformation som erhålls genom dessa bedömningar.

(3) I båda fallen ska de nationella certifieringsordningarna ange vilken ytterligare utvärderingsverksamhet som behövs för att analysera eller komplettera den information som erhålls genom dessa ordningar.

BILAGA V

FÖRTECKNING ÖVER ALLMÄNT TILLGÄNGLIG INFORMATION OM PLÅNBÖCKER

1. Den information som ska offentliggöras enligt artikel 8.5 ska omfatta åtminstone följande:

   a) Eventuella begränsningar av användningen av en plånbokslösning.

   b) Vägledning och rekommendationer från plånbokstillhandahållaren för att hjälpa slutanvändare med säker konfigurering, installation, införande, drift och underhåll av plånböcker.

   c) Uppgift om tidsperiod under vilken säkerhetsstöd kommer att erbjudas slutanvändare, särskilt vad gäller tillgång till cybersäkerhetsrelaterade uppdateringar.

   d) Kontaktuppgifter för tillverkaren eller tillhandahållaren och uppgift om metoder som accepteras för mottagande av sårbarhetsinformation från slutanvändare och säkerhetsforskare.

   e) Hänvisning till förteckningar online över offentliggjorda sårbarheter kopplade till plånböcker och relevant cybersäkerhetsrådgivning.

2. Den information som avses i punkt 1 ska göras tillgänglig på ett tydligt, heltäckande och lättillgängligt sätt, på en allmänt tillgänglig plats, för varje person som vill använda en plånbokslösning.

BILAGA VI

METOD FÖR BEDÖMNING AV HURUVIDA TILLITSINFORMATIONEN ÄR GODTAGBAR

1. **Bedömning av tillgången till tillitsdokumentation**

Utvärderarna ska förteckna den tillitsdokumentation som finns tillgänglig för varje relevant komponent i plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls. Därefter ska utvärderarna bedöma varje tillitsdokumentations övergripande betydelse för beroendegranskningen.

Följande aspekter ska beaktas i analysen:

(1) Om själva tillitsdokumentationen:

a) Typen av tillitsdokumentation, med alla nödvändiga uppgifter

(exempel på sådana dokument är intyg om överensstämmelse enligt EN ISO/IEC 27001:2022 eller typ 1 eller typ 2 för ISAE-rapporter).

b) Den period som omfattas eller giltighetstiden

(denna period kan kompletteras med en mellanliggande rapport (ett dokument som omfattar en tidsperiod mellan slutdatumet för rapporteringsperioden för den aktuella ISAE-rapporten och offentliggörandet av en ny ISAE-rapport) eller liknande redogörelse).

c) Den tillämpliga ramen (t.ex. befintlig standard).

d) Huruvida tillitsdokumentationen innehåller en kartläggning av ordningens krav.

(2) Om den yrkesmässiga kompetensen och opartiskheten hos utfärdaren av tillitsrapporten:

a) Certifieringsorganets namn och, i förekommande fall, huvudutvärderarens namn.

b) Bevis på certifieringsorganets och utvärderarens kompetens (t.ex. ackreditering, personlig certifiering osv.).

c) Bevis på certifieringsorganets och utvärderarens opartiskhet (t.ex. ackreditering osv.).

2. **Bedömning av säkerhet i samband med enskilda krav**

Utvärderarna ska kontrollera att den tillitsdokumentation som finns tillgänglig för plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls är tillräcklig för att fastställa att plånbokslösningen uppfyller förväntningarna i förhållande till certifieringsordningens enskilda krav.

Denna bedömning ska utföras för varje relevant komponent i plånbokslösningen och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls, genom att formulera ett antagande om plånbokslösningens säkerhetskontroller.

För varje sådant antagande ska utvärderingsgruppen avgöra om den säkerhet som den tillgängliga tillitsdokumentationen ger är tillräcklig eller inte.

Avgörandet om att säkerheten är tillräcklig ska grundas på följande:

(1) Den information som krävs finns tillgänglig, med den förväntade tillitsnivån, i tillitsdokumentationen.

(2) Den information som finns tillgänglig i tillitsdokumentationen tillgodoser inte hela kravet, men ytterligare kontroller eller kompenserande kontroller (dvs. interna kontroller som minskar risken för befintliga eller potentiella kontrollbrister) som genomförs i plånbokslösningen eller i det system för elektronisk identifiering inom ramen för vilket den tillhandahålls gör det möjligt för utvärderarna att fastställa att informationen är tillräcklig.

(3) Den information som finns tillgänglig i tillitsdokumentationen ger inte den förväntade tillitsnivån, men de kontroller som genomförs för att bedöma och övervaka plånbokstillhandahållaren gör det möjligt för utvärderarna att fastställa att informationen är tillräcklig.

(4) Om det i tillitsdokumentationen nämns att det finns avvikelser i utformningen eller genomförandet av de kontroller som används för att uppfylla ett antagande ska de korrigerande åtgärder som föreslås och genomförs av plånbokstillhandahållaren och granskas av dess utvärderare vara tillräckliga för att garantera att antagandet faktiskt uppfylls.

BILAGA VII

INNEHÅLLET I INTYGET OM ÖVERENSSTÄMMELSE

1. En unik identifieringskod som tilldelats av det certifieringsorgan som utfärdar intyget om överensstämmelse.

2. Information om den certifierade plånbokslösningen och de system för elektronisk identifiering inom ramen för vilka den tillhandahålls och om innehavaren av intyget om överensstämmelse, inbegripet följande:
   a) Plånbokslösningens namn.
   b) Namn på de system för elektronisk identifiering inom ramen för vilka plånbokslösningen tillhandahålls.
   c) Vilken version av plånbokslösningen som utvärderades.
   d) Namn, adress och kontaktuppgifter till innehavaren av intyget om överensstämmelse.
   e) Länk till webbplatsen för innehavaren av intyget om överensstämmelse som innehåller den information som ska offentliggöras.

3. Information om utvärderingen och certifieringen av plånbokslösningen och de system för elektronisk identifiering inom ramen för vilka den tillhandahålls, inbegripet följande:
   a) Namn, adress och kontaktuppgifter till det certifieringsorgan som utfärdade intyget om överensstämmelse.
   b) Om annat än certifieringsorganet, namnet på det organ för bedömning av överensstämmelse som gjorde utvärderingen, tillsammans med information om dess ackreditering.
   c) Systemägarens namn.
   d) Hänvisningar till förordning (EU) nr 910/2014 och till denna förordning.
   e) En hänvisning till den certifieringsrapport som är förknippad med intyget om överensstämmelse.
   f) En hänvisning till den bedömningsrapport för certifiering som är förknippad med intyget om överensstämmelse.
   g) En hänvisning till de standarder som används för utvärderingen, inklusive vilken version av dessa.
   h) Datum för utfärdande av intyget om överensstämmelse.
   i) Giltighetstiden för intyget om överensstämmelse.

BILAGA VIII

INNEHÅLLET I DEN OFFENTLIGA CERTIFIERINGSRAPPORTEN OCH RAPPORTEN OM CERTIFIERINGSBEDÖMNINGEN

1. Den offentliga certifieringsrapporten ska innehålla minst följande aspekter:

   a) Sammanfattning.

   b) Identifiering av den plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls.

   c) En beskrivning av den plånbokslösning och det system för elektronisk identifiering inom ramen för vilket den tillhandahålls.

   d) Den säkerhetsinformation som ska göras allmänt tillgänglig enligt beskrivningen i bilaga V eller en hänvisning till denna information.

   e) En sammanfattning av den preliminära revisions- och valideringsplanen.

   f) En sammanfattning av granskningen och beslutet om certifiering.

2. Rapporten om certifieringsbedömning ska åtminstone innehålla följande:

   a) En beskrivning av plånbokslösningens utformning, identifieringssystemet och anslutningsprocessen, tillsammans med riskbedömningen och den särskilda valideringsplanen.

   b) En beskrivning av hur plånbokslösningen uppfyller kraven på tillitsnivå hög och hur detta visas genom resultaten av den certifieringsbedömning av plånbokslösningen som utförts i enlighet med denna förordning.

   c) En beskrivning av resultatet av bedömningen av plånbokslösningens överensstämmelse och av det system för elektronisk identifiering inom ramen för vilket tillhörande plånboksenheter tillhandahålls, särskilt överensstämmelsen med följande:

      — De krav som anges i artikel 5a.4, 5a.5 och 5a.8 i förordning (EU) nr 910/2014.

      — Det krav på logisk avskildhet som anges i artikel 5a.14 i förordning (EU) nr 910/2014.

      — I tillämpliga fall, de standarder och tekniska specifikationer som avses i artikel 5a.24 i förordning (EU) nr 910/2014, med en beskrivning av hur dessa krav förhåller sig till motsvarande normativa krav som anges i nationella certifieringsordningar.

   d) En sammanfattning av resultatet av utförandet av valideringsplanen, inklusive alla identifierade avvikelser.

BILAGA IX

TIDSPLAN FÖR OBLIGATORISKA KONTROLLUTVÄRDERINGAR

1. I artikel 18 anges kraven för certifieringscykeln, särskilt genomförandet av regelbundna utvärderingar. Dessa utvärderingar ska åtminstone inbegripa följande:

   a) En fullständig utvärdering av föremålet för bedömningen av överensstämmelse vid den inledande utvärderingen och vid varje omcertifieringsutvärdering, inklusive en uppdateringsfunktion för alla produktkomponenter.

   b) En sårbarhetsbedömning vid den inledande utvärderingen och vid varje omcertifieringsutvärdering, och minst vartannat år vid kontrollutvärderingar, som åtminstone omfattar ändringarna av föremålet för bedömningen av överensstämmelse och ändringarna i hotmiljön sedan den senaste sårbarhetsbedömningen.

   c) Ytterligare utvärderingar, som till exempel penetrationstestning, i händelse av en ökad risknivå eller uppkomsten av nya hot.

   d) En utvärdering av underhållsprocessernas driftseffektivitet minst varje år vid kontroll- och omcertifieringsutvärderingar, som åtminstone omfattar processer för versionskontroll, uppdatering och sårbarhetshantering.

   e) Efter en framgångsrik granskning och beslut om certifiering, utfärdande av ett intyg om överensstämmelse efter den inledande utvärderingen och efter varje omcertifieringsutvärdering.

2. En referenstidsplan anges i tabell 1 baserad på en fyraårscykel, där

   a) år 1 börjar när intyget om överensstämmelse utfärdas för första gången, och

   b) all utvärderingsverksamhet ska genomföras inom tolv månader från det föregående årets utvärdering.

3. Tidsplanen i tabell 1 är en rekommendation för att säkerställa att omcertifieringen sker i rätt tid och för att undvika störningar i tillhandahållandet av plånbokslösningen. Andra tidsplaner kan vara möjliga så länge intyget om överensstämmelse är giltigt i högst fem år i enlighet med artikel 5c.4 i förordning (EU) nr 910/2014.

4. Utöver de regelbundna utvärderingarna kan en särskild utvärdering utlösas på begäran av certifieringsorganet eller innehavaren av intyget om överensstämmelse, efter en väsentlig ändring av certifieringsobjektet eller hotmiljön.

5. Alla utvärderingar, inbegripet kontrollutvärderingar och särskilda utvärderingar, kan leda till att ett nytt intyg om överensstämmelse utfärdas, särskilt vid väsentliga ändringar av certifieringsobjektet, men med samma sista giltighetsdag som det ursprungliga intyget om överensstämmelse.

Tabell 1

En fullständig fyraårig utvärderingscykel

Tid	Utvärderingstyp	Verksamhet
År 0	Inledande	— Fullständig utvärdering av certifieringsobjektet, inklusive sårbarhetsbedömning — Inklusive en funktion för att utföra uppdateringar av varje programvarukomponent — Utvärdering av underhållsprocesserna, med undantag för deras driftseffektivitet — Utfärdande av intyg om överensstämmelse och början på fyraårscykeln
År 1	Övervakning	— Utvärdering av underhållsprocessernas driftseffektivitet — Åtminstone versionskontroll, uppdatering, sårbarhetshantering — Utvärdering av ändringar som påverkar produktens säkerhet

Tid	Utvärderingstyp	Verksamhet
År 2	Övervakning	— Sårbarhetsbedömning av hela lösningen — Utvärdering av underhållsprocessernas driftseffektivitet — Åtminstone versionskontroll, uppdatering, sårbarhetshantering — Utvärdering av ändringar som påverkar produktens säkerhet
År 3	Övervakning	— Utvärdering av underhållsprocessernas driftseffektivitet — Åtminstone versionskontroll, uppdatering, sårbarhetshantering — Utvärdering av ändringar som påverkar produktens säkerhet
År 4	Omcertifiering	(1) Fullständig utvärdering av certifieringsobjektet, inklusive sårbarhetsbedömning (2) Förenklad utvärdering av funktioner/processer som inte har ändrats (3) Inklusive en funktion för att utföra uppdateringar av varje programvarukomponent (4) Utvärdering av underhållsprocesserna, inklusive deras driftseffektivitet (5) Utfärdande av ett nytt intyg om överensstämmelse