Europeiska unionens
officiella tidning

SV
L-serien

2024/2979

4.12.2024

KOMMISSIONENS GENOMFÖRANDEFÖRORDNING (EU) 2024/2979

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

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 5a.23, och

av följande skäl:

(1) Det europeiska ramverket för digital identitet, som inrättades genom förordning (EU) nr 910/2014, är en avgörande komponent i inrättandet av ett säkert och interoperabelt ekosystem för digital identitet i hela unionen. EU:s digitala identitetsplånböcker (*plånböckerna*) utgör hörnstenen i ramverket som syftar till att underlätta för fysiska och juridiska personer att få tillgång till tjänster i medlemsstaterna, samtidigt som skyddet av personuppgifter och integritet säkerställs.

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

(3) Enligt artikel 5a.23 i förordning (EU) nr 910/2014 ska kommissionen vid behov fastställa relevanta specifikationer och förfaranden. Detta uppnås genom fyra genomförandeförordningar, som behandlar protokoll och gränssnitt: kommissionens genomförandeförordning (EU) 2024/2982 ([4]), integritet och centrala funktioner: kommissionens genomförandeförordning (EU) 2024/2979 ([5]), personidentifieringsuppgifter och elektroniska attributsintyg: kommissionens genomförandeförordning (EU) 2024/2977 ([6]) samt anmälningar till kommissionen: kommissionens genomförandeförordning (EU) 2024/2980 ([7]). I denna förordning fastställs de relevanta kraven för personidentifieringsuppgifter och elektroniska attributsintyg som ska utfärdas för EU:s digitala identitetsplånböcker.

([1]) EUT L 257, 28.8.2014, s. 73, ELI: https://eur-lex.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: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=sv).

([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]) 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).

([5]) 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, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) 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).

([7]) Kommissionens genomförandeförordning (EU) 2024/2980 av den 28 november 2024 om tillämpningsföreskrifter för Europaparlamentets och rådets förordning (EU) nr 910/2014 vad gäller anmälningar till kommissionen avseende ekosystemet för EU:s digitala identitetsplånböcker (EUT L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) 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 ([8]), särskilt arkitekturen och referensramen. I enlighet med skäl 75 i Europaparlamentets och rådets förordning (EU) 2024/1183 ([9]) 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.

(5) För att säkerställa exakt kommunikation, teknisk differentiering och tydlig ansvarsfördelning är det nödvändigt att skilja mellan olika komponenter och konfigureringar av plånböcker. En plånbokslösning bör förstås som det fullständiga system som tillhandahålls av en tillhandahållare av plånböcker och som är nödvändigt för att driva en plånbok. Det bör omfatta programvaru- och hårdvarukomponenter samt de tjänster, inställningar och konfigureringar som behövs för att säkerställa att plånboken fungerar korrekt. En plånbokslösning kan finnas på användarens enheter och miljöer och på tillhandahållarens backend-struktur. En plånboksenhet bör förstås som en särskild konfigurering av plånbokslösningen för en enskild användare. Den bör omfatta den applikation som installerats på en plånboksanvändares enhet eller miljö som plånboksanvändaren interagerar direkt med (plånboksinstansen) och de säkerhetsdetaljer som krävs för att skydda användarnas uppgifter och transaktioner. Dessa säkerhetsfunktioner bör omfatta särskild programvara eller hårdvara för att kryptera och skydda känslig information. En plånboksinstans bör ingå i plånboksenheten och göra det möjligt för plånboksanvändaren att få tillgång till plånbokens funktioner.

(6) Krypteringsapplikationer som separata specialiserade komponenter inom en plånboksenhet är nödvändiga inte bara för att skydda kritiska tillgångar, såsom privata krypteringsnycklar, utan även för att tillhandahålla viktiga funktioner, såsom presentation av elektroniska attributsintyg. Användningen av gemensamma tekniska specifikationer kan underlätta plånbokstillhandahållarnas tillgång till inbyggda säkerhetskomponenter. Krypteringsapplikationer kan tillhandahållas på olika sätt och till olika typer av krypteringshårdvaror. Om krypteringsapplikationer tillhandahålls av plånbokstillhandahållare i form av Java Card-miniprogram till inbyggda säkerhetskomponenter, bör plånbokstillhandahållarna följa de standarder som förtecknas i bilaga I eller motsvarande tekniska specifikationer.

(7) Plånboksenheter ska göra det möjligt för tillhandahållare av personidentifieringsuppgifter eller elektroniska attributsintyg att kontrollera att de utfärdar dessa uppgifter eller intyg till verkliga plånboksenheter tillhörande plånboksanvändare.

(8) För att säkerställa ett inbyggt dataskydd och dataskydd som standard bör plånböckerna förses med den senaste tillgängliga integritetsfrämjande tekniken. Dessa funktioner bör göra det möjligt att använda plånböcker utan att plånboksanvändaren kan spåras mellan olika förlitande parter, om detta är tillämpligt i användningsscenariot. Plånbokstillhandahållare bör till exempel överväga de senaste integritetsbegränsande åtgärderna för plånboksenhetsintyg, till exempel tillfälliga plånboksenhetsintyg eller grupputfärdande. Dessutom bör inbyggda policyer för utlämnande varna plånboksanvändarna för olämpligt eller olagligt utlämnande av attribut från elektroniska attributsintyg.

(9) Plånboksenhetsintygen bör göra det möjligt för förlitande parter som begär attribut från plånboksenheter att kontrollera giltigheten för den plånboksenhet som de kommunicerar med, eftersom plånboksenhetsintyg ska återkallas när en plånboksenhet inte längre anses vara giltig. Informationen om plånboksenheternas giltighet bör göras tillgänglig på ett interoperabelt sätt för att säkerställa att den kan användas av alla förlitande parter. I fall där plånboksanvändare förlorat sina plånboksenheter eller inte längre har kontroll över dem bör plånbokstillhandahållarna dessutom göra det möjligt för plånboksanvändare att begära att deras plånboksenhet återkallas. För att säkerställa integritet och olänkbarhet bör medlemsstaterna använda integritetsbevarande teknik även för plånboksenhetsintyg. Detta kan inbegripa användning av flera plånboksenhetsintyg för olika ändamål, där endast den minimalt relevanta information om plånboken som krävs för en transaktion lämnas ut, eller att begränsa livslängden för ett plånboksenhetsintyg som ett alternativ till att använda identifieringskoder för återkallelse.

([8]) EUT L 210, 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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: https://eur-lex.europa.eu/eli/reg/2024/1183/oj).

(10) För att säkerställa att alla plånböcker har tekniska möjligheter att ta emot och presentera personidentifieringsuppgifter och elektroniska attributsintyg i gränsöverskridande scenarier utan att detta försämrar interoperabiliteten bör plånböckerna stödja förutbestämda typer av dataformat och selektivt utlämnande. Såsom fastställs i förordning (EU) nr 910/2014 är selektivt utlämnande ett begrepp som ger dataägaren rätt att endast lämna ut vissa delar av en större datamängd, så att den mottagande enheten endast kan inhämta information som är nödvändig för tillhandahållandet av en tjänst som begärs av en användare. Eftersom plånböckerna ska göra det möjligt för användaren att selektivt utlämna attribut bör de standarder som förtecknas i bilaga II genomföras på ett sätt som möjliggör denna funktion i plånböckerna. Plånböcker kan dessutom stödja andra format och funktioner för att underlätta särskilda användningsfall.

(11) Loggning av transaktioner är ett viktigt verktyg för att skapa transparens genom att ge plånboksanvändaren en översikt över transaktionerna. Dessutom bör loggar användas för att göra det möjligt att, på begäran av plånboksanvändaren, snabbt och enkelt utbyta viss information med de behöriga tillsynsmyndigheter som inrättats i enlighet med artikel 51 i förordning (EU) 2016/679, om förlitande parter uppträder misstänkt.

(12) För att en plånboksanvändare ska kunna skriva under elektroniskt bör ett kvalificerat certifikat, som är bundet till en kvalificerad anordning för skapande av elektroniska underskrifter, utfärdas till plånboksanvändaren. Plånboksanvändaren bör ha tillgång till en applikation för skapande av underskrifter. Utfärdandet av kvalificerade certifikat är en tjänst som tillhandahålls av kvalificerade tillhandahållare av betrodda tjänster, men plånbokstillhandahållare eller andra enheter bör kunna tillhandahålla övriga komponenter. Kvalificerade anordningar för skapande av elektroniska underskrifter kan till exempel förvaltas av kvalificerade tillhandahållare av betrodda tjänster som en tjänst eller kan vara lokala i förhållande till plånboksanvändarens enhet, till exempel som ett smartkort. På samma sätt kan applikationer för skapande av underskrifter integreras i plånboksinstansen, vara en separat app i plånboksanvändarens enhet eller tillhandahållas på distans.

(13) Föremål för dataexport och dataportabilitet kan logga personidentifieringsuppgifter och elektroniska attributsintyg som har utfärdats till en viss plånboksenhet. Dessa föremål gör det möjligt för plånboksanvändare att hämta relevanta uppgifter från sin plånboksenhet för att stärka sin rätt till dataportabilitet. Plånbokstillhandahållare uppmuntras att använda samma tekniska lösningar för att även genomföra säkerhetskopierings- och återställningsprocesser för plånboksenheter, vilket gör det möjligt att återställa förlorade plånboksenheter eller överföra information från en plånbokstillhandahållare till en annan, när så är lämpligt och i den mån detta kan göras utan att rätten till dataskydd och säkerheten i ekosystemet för digital identitet försämras.

(14) Genereringen av pseudonymer som är specifika för förlitande parter bör göra det möjligt för plånboksanvändare att autentisera sig utan att förse förlitande parter med onödig information. I enlighet med förordning (EU) nr 910/2014 ska plånboksanvändare inte hindras från att få tillgång till tjänster under en pseudonym, om det inte finns något rättsligt krav på juridisk identitet för autentisering. Plånböckerna ska därför innehålla en funktion för att generera pseudonymer som användaren väljer och hanterar, för autentisering för att få tillgång till onlinetjänster. Genomförandet av specifikationerna i bilaga V bör möjliggöra dessa funktioner i enlighet med detta. Förlitande parter får vidare inte begära att användarna tillhandahåller några andra uppgifter än de som anges för plånböckernas avsedda användning i registret över förlitande parter. Plånboksanvändare bör ha möjlighet att när som helst kontrollera förlitande parters registreringsuppgifter.

(15) Enligt förordning (EU) 2024/1183 får medlemsstaterna inte direkt eller indirekt begränsa tillgången till offentliga eller privata tjänster för fysiska eller juridiska personer som väljer att inte använda plånböcker och ska tillhandahålla lämpliga alternativa lösningar.

(16) Samråd med Europeiska datatillsynsmannen har skett i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([10]) och avgav ett yttrande den 30 september 2024.

([10]) 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).

(17) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från den kommitté som avses i artikel 48 i förordning (EU) nr 910/2014.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll och tillämpningsområde

I denna förordning fastställs regler för plånböckernas integritet och centrala funktioner, som ska uppdateras regelbundet för att hållas i linje med utvecklingen av teknik och standarder och med det arbete som utförs på grundval av rekommendation (EU) 2021/946, särskilt arkitekturen och referensramen.

Artikel 2

Definitioner

I denna förordning gäller följande definitioner:

1. *krypteringsapplikation*: en applikation som hanterar kritiska tillgångar genom att vara kopplad till och använda de kryptografiska och icke-kryptografiska funktioner som tillhandahålls av krypterings hårdvaran.

2. *plånboksenhet*: en unik konfigurering av en plånbokslösning som omfattar plånboksinstanser, krypteringsapplikationer och krypteringshårdvaror som en plånbokstillhandahållare tillhandahåller en enskild plånboksanvändare.

3. *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.

4. *tillhandahållare av personidentifieringsuppgifter*: en fysisk eller juridisk person som ansvarar för att utfärda och återkalla personidentifieringsuppgifter och säkerställa att en användares personidentifieringsuppgifter är kryptografiskt bundna till en plånboksenhet.

5. *plånboksanvändare*: en användare som kontrollerar plånboksenheten.

6. *förlitande part*: en förlitande part som avser att förlita sig på plånboksenheter för att genom digital interaktion tillhandahålla offentliga eller privata tjänster.

7. *plånbokstillhandahållare*: en fysisk eller juridisk person som tillhandahåller plånbokslösningar.

8. *plånboksenhetsintyg*: ett dataobjekt som beskriver plånboksenhetens komponenter eller möjliggör autentisering och validering av dessa komponenter.

9. *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.

10. *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.

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

12. *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.

13. *krypteringsoperation*: en kryptografisk mekanism som är nödvändig för autentisering av plånboksanvändaren och utfärdande eller presentation av personidentifieringsuppgifter eller elektroniska attributsintyg.

14. *förlitandepartcertifikat*: ett certifikat för elektroniska stämplar eller underskrifter som autentiserar och validerar den förlitande parten och som utfärdats av en tillhandahållare av förlitandepartcertifikat.

15. *tillhandahållare av förlitandepartcertifikat*: en fysisk eller juridisk person som bemyndigats av en medlemsstat att utfärda förlitandepartcertifikat till förlitande parter som är registrerade i den medlemsstaten.

KAPITEL II

EU:s DIGITALA IDENTITETSPLÅNBÖCKERS INTEGRITET

Artikel 3

Plånboksenhetens integritet

1. Plånboksenheter ska inte utföra någon av de funktioner som anges i artikel 5a.4 i förordning (EU) nr 910/2014, utom autentisering av plånboksanvändare för åtkomst till plånboksenheten, förrän plånboksenheten har autentiserat plånboksanvändaren.

2. Plånbokstillhandahållare ska för varje plånboksenhet underteckna eller stämpla minst ett plånboksenhetsintyg som uppfyller kraven i artikel 6. Det certifikat som används för att underteckna eller stämpla plånboksenhetsintyget ska utfärdas enligt ett certifikat som anges i den förteckning över tillhandahållare av betrodda tjänster som avses i genomförandeförordning (EU) 2024/2980.

Artikel 4

Plånboksinstanser

1. Plånboksinstanser ska använda minst en krypteringshårdvara för att hantera kritiska tillgångar.

2. Plånbokstillhandahållare ska säkerställa integritet, autenticitet och konfidentialitet i kommunikationen mellan plånboksinstanser och krypteringsapplikationer.

3. Om kritiska tillgångar är förknippade med utförande av elektronisk identifiering på tillitsnivå hög ska krypteringsoperationer eller andra operationer för behandling av kritiska tillgångar utföras i enlighet med de krav som ställs på egenskaper och utformning när det gäller medel för elektronisk identifiering på tillitsnivå hög, i enlighet med kommissionens genomförandeförordning (EU) 2015/1502 ([11]).

Artikel 5

Krypteringsapplikationer

1. Plånbokstillhandahållare ska säkerställa att krypteringsapplikationer

a) utför krypteringsoperationer som omfattar andra kritiska tillgångar än de som krävs för att plånboksenheten ska autentisera plånboksanvändaren. endast i de fall då dessa applikationer har autentiserat plånboksanvändarna,

([11]) 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).

b) som autentiserar plånboksanvändare i samband med utförandet av elektronisk identifiering på tillitsnivå hög, autentiserar plånboksanvändare i enlighet med de krav som ställs på egenskaper och utformning när det gäller medel för elektronisk identifiering på tillitsnivå hög, i enlighet med genomförandeförordning (EU) 2015/1502,

c) kan generera nya krypteringsnycklar på ett säkert sätt,

d) kan utföra säker radering av kritiska tillgångar,

e) kan generera bevis på innehav av privata nycklar,

f) skyddar de privata nycklar som genereras av dessa krypteringsapplikationer så länge nycklarna finns,

g) uppfyller de krav som ställs på egenskaper och utformning när det gäller medel för elektronisk identifiering på tillitsnivå hög, i enlighet med genomförandeförordning (EU) 2015/1502,

h) är de enda komponenter som kan utföra krypteringsoperationer och andra operationer med kritiska tillgångar i samband med elektronisk identifiering på tillitsnivå hög.

2. Om plånbokstillhandahållare beslutar att tillhandahålla en säker krypteringsapplikation till en inbyggd säkerhetskomponent, ska dessa plånbokstillhandahållare basera sin tekniska lösning på de tekniska specifikationer som förtecknas i bilaga I eller på andra likvärdiga tekniska specifikationer.

Artikel 6

Plånboksenhetens äkthet och giltighet

1. Plånbokstillhandahållare ska säkerställa att varje plånboksenhet innehåller plånboksenhetsintyg.

2. Plånbokstillhandahållare ska säkerställa att de plånboksenhetsintyg som avses i punkt 1 innehåller öppna nycklar och att motsvarande privata nycklar skyddas av en krypteringshårdvara.

3. Plånbokstillhandahållare ska

a) informera plånboksanvändarna om deras rättigheter och skyldigheter i förhållande till deras plånboksenhet,

b) tillhandahålla mekanismer, oberoende av plånboksenheterna, för säker identifiering och autentisering av plånboksanvändare,

c) säkerställa att plånboksanvändare har rätt att begära att deras plånboksenhetsintyg återkallas med hjälp av de autentiseringsmekanismer som avses i led b.

Artikel 7

Återkallelse av plånboksenhetsintyg

1. Plånbokstillhandahållare ska vara de enda enheter som kan återkalla plånboksenhetsintyg för plånboksenheter som de har tillhandahållit.

2. Plånbokstillhandahållare ska fastställa en allmänt tillgänglig policy som innehåller villkoren och tidsramen för återkallelsen av plånboksenhetsintyg.

3. Om plånbokstillhandahållare har återkallat plånboksenhetsintyg ska de informera berörda plånboksanvändare inom 24 timmar efter återkallelsen av deras plånboksenheter, bland annat om skälet för återkallelsen och konsekvenserna för plånboksanvändaren. Denna information ska tillhandahållas på ett koncist och lättillgängligt sätt samt på ett klart och tydligt språk.

4. Om plånbokstillhandahållare har återkallat plånboksenhetsintyg ska de på ett integritetsbevarande sätt offentliggöra plånboksenhetsintygets giltighet och beskriva var i plånboksenhetsintyget denna information finns.

KAPITEL III

EU:s DIGITALA IDENTITETSPLÅNBÖCKERS CENTRALA FUNKTIONER OCH INSLAG

Artikel 8

Format för personidentifieringsuppgifter och elektroniska attributsintyg

Plånbokstillhandahållare ska säkerställa att plånbokslösningar stöder användningen av personidentifieringsuppgifter och elektroniska attributsintyg som utfärdats i enlighet med förteckningen över standarder i bilaga II.

Artikel 9

Transaktionsloggar

1. Oavsett om en transaktion har fullbordats eller inte ska plånboksinstanserna logga alla transaktioner med förlitande parter och andra plånboksenheter, inbegripet elektroniska underskrifter och stämplar.

2. Den loggade informationen ska åtminstone innehålla

a) tid och datum för transaktionen,

b) namn, kontaktuppgifter och den unika identifieringskoden för den berörda förlitande parten och den medlemsstat där den förlitande parten är etablerad, eller, när det gäller andra plånboksenheter, relevant information från plånboksenhetsintyget,

c) den typ av uppgifter som begärts och presenterats i transaktionen,

d) skälet till eventuella ofullbordade transaktioner.

3. Plånbokstillhandahållare ska säkerställa den loggade informationens integritet, autenticitet och konfidentialitet.

4. Plånboksinstanser ska logga rapporter som plånboksanvändare skickar till dataskyddsmyndigheterna via deras plånboksenhet.

5. De loggar som avses i punkterna 1 och 2 ska, om det är nödvändigt för tillhandahållandet av plånbokstjänster, vara tillgängliga för plånbokstillhandahållaren på grundval av plånboksanvändarens uttryckliga förhandsgodkännande.

6. De loggar som avses i punkterna 1 och 2 ska förbli tillgängliga så länge som krävs enligt unionsrätten eller nationell rätt.

7. Plånbokstillhandahållare ska göra det möjligt för plånboksanvändare att exportera den loggade information som avses i punkt 2.

Artikel 10

Inbyggt utlämnande

1. Plånbokstillhandahållare ska säkerställa att elektroniska attributsintyg med gemensamma inbyggda policyer för utlämnande enligt bilaga III kan behandlas av de plånboksenheter som de tillhandahåller.

2. Plånboksinstanser ska kunna behandla och presentera sådana inbyggda policyer för utlämnande som avses i punkt 1 i samband med uppgifter som mottagits från den begärande förlitande parten.

3. Plånboksinstanser ska kontrollera om den förlitande parten uppfyller kraven i den inbyggda policyn för utlämnande och informera plånboksanvändaren om resultatet.

Artikel 11

Kvalificerade elektroniska underskrifter och stämplar

1. Plånbokstillhandahållare ska säkerställa att plånboksanvändare kan få kvalificerade certifikat för kvalificerade elektroniska underskrifter eller stämplar som är kopplade till kvalificerade anordningar för skapande av underskrifter eller stämplar som är antingen lokala, externa eller på distans i förhållande till plånboksinstanserna.

2. Plånbokstillhandahållare ska säkerställa att plånbokslösningar på ett säkert sätt kan samverka med någon av följande typer av kvalificerade anordningar för skapande av underskrifter eller stämplar: lokala, externa eller på distans förvaltade kvalificerade anordningar för skapande av underskrifter eller stämplar i syfte att använda de kvalificerade certifikat som avses i punkt 1.

3. Plånbokstillhandahållare ska säkerställa att plånboksanvändare som är fysiska personer, åtminstone för icke-yrkesmässiga ändamål, har kostnadsfri tillgång till applikationer för skapande av underskrifter som gör det möjligt att skapa kostnadsfria kvalificerade elektroniska underskrifter med hjälp av de certifikat som avses i punkt 1.

Artikel 12

Applikationer för skapande av underskrifter

1. De applikationer för skapande av underskrifter som plånboksenheterna använder kan tillhandahållas antingen av plånbokstillhandahållare, av tillhandahållare av betrodda tjänster eller av förlitande parter.

2. Applikationer för skapande av underskrifter ska ha följande funktioner:

a) Underteckna eller stämpla uppgifter som tillhandahålls plånboksanvändare.

b) Underteckna eller stämpla uppgifter som tillhandahålls av förlitande parter.

c) Skapa underskrifter eller stämplar i enlighet med åtminstone de obligatoriska format som avses i bilaga IV.

d) Informera plånboksanvändarna om resultatet av processen för skapande av underskrifter eller stämplar.

3. Applikationer för skapande av underskrifter kan antingen vara integrerade i eller externa i förhållande till plånboksinstanserna. Om applikationer för skapande av underskrifter är beroende av kvalificerade anordningar för skapande av underskrifter på distans och om de är integrerade i plånboksinstanserna ska de stödja det gränssnitt för tillämpningsprogram som avses i bilaga IV.

Artikel 13

Dataexport och dataportabilitet

Plånboksenheter ska, när det är tekniskt möjligt och med undantag för kritiska tillgångar, stödja säker export och portabilitet av plånboksanvändarens personuppgifter, så att plånboksanvändaren kan övergå till en plånboksenhet med en annan plånbokslösning på ett sätt som säkerställer tillitsnivå hög, i enlighet med genomförandeförordning (EU) 2015/1502.

Artikel 14

Pseudonymer

1. Plånboksenheter ska stödja genereringen av pseudonymer för plånboksanvändare i enlighet med de tekniska specifikationer som anges i bilaga V.

2. Plånboksenheter ska, på begäran av en förlitande part, stödja genereringen av en pseudonym som är specifik och unik för den förlitande parten och tillhandahålla den förlitande parten denna pseudonym ensam eller i kombination med eventuella personidentifieringsuppgifter eller elektroniska attributsintyg som begärs av den förlitande parten.

KAPITEL IV

SLUTBESTÄMMELSER

Artikel 15

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

FÖRTECKNING ÖVER STANDARDER SOM AVSES I ARTIKEL 5

— SAM.01 Secured Applications for Mobile – Requirements for supporting 3rd party Applets on eSIM and eSE via SAM. v1.1 2023, GSMA.

— GPC_GUI_ 217 GlobalPlatform SAM Configuration Technical specification for implementation of SAM v1.0 2024-04.

— GPC_SPE_0 34 GlobalPlatform Card Specification Technical specification for smart cards v2.3.1 2018-03.

— GPC_SPE_0 07 GlobalPlatform Amendment A Confidential Card Content Management v1.2 2019-07.

— GPC_SPE_0 13 GlobalPlatform Amendment D Secure Channel Protocol 03 v1.2 2020-04.

— GPC_SPE_0 93 GlobalPlatform Amendment F Secure Channel Protocol 11 v1.4 2024-03.

— GPD_SPE_0 75 Open Mobile API Specification OMAPI API for mobile apps to access secure elements on user devices. v3.3 2018-08, GlobalPlatform.

BILAGA II

FÖRTECKNING ÖVER STANDARDER SOM AVSES I ARTIKEL 8

— ISO/IEC 18013-5:2021.

— *Verifiable Credentials Data Model 1.1* (datamodell för verifierbara behörighetsuppgifter), W3C-rekommendation, 3 mars 2022.

BILAGA III

FÖRTECKNING ÖVER GEMENSAMMA INBYGGDA POLICYER FÖR UTLÄMNANDE SOM AVSES I ARTIKEL 10

1. *Ingen policy* anger att ingen policy gäller för de elektroniska attributsintygen.
2. Policyn *Endast för behöriga förlitande parter* anger att plånboksanvändare endast får lämna ut elektroniska attributsintyg till autentiserade förlitande parter som uttryckligen anges i policyerna för utlämnande.
3. *Specifikt tillitsankare* anger att plånboksanvändare endast bör lämna ut det specifika elektroniska attributsintyget till autentiserade förlitande parter med förlitandepartcertifikat som härrör från ett specifikt ankare (eller en förteckning över specifika ankare) eller ett eller flera mellanliggande certifikat.

BILAGA IV

FORMAT FÖR UNDERSKRIFT OCH STÄMPEL SOM AVSES I ARTIKEL 12

1. Format för obligatorisk underskrift eller stämpel:

   a) Avancerad elektronisk underskrift för PDF (*PDF Advanced Electronic Signature*, PAdES) enligt Etsi EN 319 142-1 V1.1.1 (2016-04). Elektroniska underskrifter och infrastrukturer (*Electronic Signatures and Infrastructures*, ESI). PAdES digitala underskrifter. Del 1: Byggstenar och PAdES-basunderskrifter (*Building blocks and PAdES baseline signatures*).

2. Förteckning över valfria format för underskrift eller stämpel:

   a) XAdES enligt Etsi EN 319 132-1 V1.2.1 (2022-02) elektroniska underskrifter och infrastrukturer (*Electronic Signatures and Infrastructures*, ESI). XAdES digitala underskrifter. Del 1: Byggstenar och XAdES-basunderskrifter (*Building blocks and XAdES baseline signatures*, XAdES) för underskrift av XML-format.

   b) JAdES enligt Etsi TS 119 182-1 V1.2.1 (2024-07) elektroniska underskrifter och infrastrukturer (ESI). JAdES digitala underskrifter. Del 1: Byggstenar och JAdES-basunderskrifter (*Building blocks and JAdES baseline signatures)* för underskrift av JSON-format.

   c) CAdES (*CMS Advanced Electronic Signature*, avancerad elektronisk underskrift för CMS) enligt Etsi EN 319 122-1 V1.3.1 (2023-06) elektroniska underskrifter och infrastrukturer (ESI). CAdES digitala underskrifter. Del 1: Byggstenar och CAdES-basunderskrifter (*Building blocks and CAdES baseline signatures*) för underskrift av CMS-format.

   d) ASiC (*Associated Signature Container*, behållare för tillhörande underskrifter) enligt Etsi EN 319 162-1 V1.1.1 (2016-04) elektroniska underskrifter och infrastrukturer (ESI). Behållare för tillhörande underskrifter (ASiC). Del 1: Byggstenar och ASiC-basbehållare (*Building blocks and ASiC baseline containers*) och Etsi EN 319 162-2 V1.1.1 (2016-04) elektroniska underskrifter och infrastrukturer (ESI). Behållare för tillhörande underskrifter (ASiC). Del 2: Ytterligare ASiC-behållare (*Additional ASiC containers*) för underskrift av behållare.

3. Gränssnitt för tillämpningsprogram:

   — Specifikation för *Cloud Signature Consortium* (CSC) v2.0 (20 april 2023).

BILAGA V

TEKNISKA SPECIFIKATIONER FÖR GENERERING AV PSEUDONYMER ENLIGT ARTIKEL 14

Tekniska specifikationer:

— WebAuthn – W3C:s rekommendation, 8 april 2021, nivå 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.