2024/2979

4.12.2024

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2024/2979

af 28. november 2024

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår integriteten af og de centrale funktioner i europæiske digitale identitetstegnebøger

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF ([1]), særlig artikel 5a, stk. 23, og

ud fra følgende betragtninger:

(1) Den europæiske ramme for digital identitet, der blev oprettet ved forordning (EU) nr. 910/2014, er et afgørende element i etableringen af et sikkert og interoperabelt økosystem for digital identitet i hele Unionen. Med de europæiske digitale identitetstegnebøger (»tegnebøger«) som hjørnesten har rammen til formål at lette adgangen til tjenester på tværs af medlemsstaterne for fysiske og juridiske personer og samtidig sikre beskyttelsen af personoplysninger og privatlivets fred.

(2) Europa-Parlamentets og Rådets forordning (EU) 2016/679 ([2]) og, hvor det er relevant, Europa-Parlamentets og Rådets direktiv 2002/58/EF ([3]) finder anvendelse på alle behandlingsaktiviteter vedrørende personoplysninger i henhold til denne forordning.

(3) I henhold til artikel 5a, stk. 23, i forordning (EU) nr. 910/2014 skal Kommissionen om nødvendigt fastsætte de relevante specifikationer og procedurer. Dette opnås ved hjælp af fire gennemførelsesforordninger, der omhandler protokoller og grænseflader Kommissionens gennemførelsesforordning (EU) 2024/2982 ([4]), integritet og centrale funktioner: Kommissionens gennemførelsesforordning (EU) 2024/2979 ([5]), personidentifikationsdata og elektronisk attestering af attributter: Kommissionens gennemførelsesforordning (EU) 2024/2977 ([6]) og anmeldelser til Kommissionen Kommissionens gennemførelsesforordning (EU) 2024/2980 ([7]). Ved denne forordning fastsættes de relevante krav for så vidt angår integriteten af og de centrale funktioner i europæiske digitale identitetstegnebøger.

([1]) EUT L 257 af 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([4]) Kommissionens gennemførelsesforordning (EU) 2024/2982 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår protokoller og grænseflader, der skal understøttes af den europæiske ramme for digital identitet (EUT L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Kommissionens gennemførelsesforordning (EU) 2024/2979 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår integriteten af og de centrale funktioner i europæiske digitale identitetstegnebøger (EUT L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Kommissionens gennemførelsesforordning (EU) 2024/2977 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår personidentifikationsdata og elektronisk attestering af attributter udstedt til europæiske digitale identitetstegnebøger (EUT L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Kommissionens gennemførelsesforordning (EU) 2024/2980 af 28. november 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår anmeldelser til Kommissionen vedrørende økosystemet for europæiske digitale identitetstegnebøger (EUT L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Kommissionen vurderer regelmæssigt nye teknologier, praksisser, standarder eller tekniske specifikationer. For at sikre den højeste grad af harmonisering mellem medlemsstaterne med hensyn til udvikling og certificering af tegnebøgerne er de tekniske specifikationer, der er fastsat i denne gennemførelsesforordning, baseret på det arbejde, der er udført på grundlag af Kommissionens henstilling (EU) 2021/946 af 3. juni 2021 om en fælles EU-værktøjskasse for en koordineret tilgang til en ramme for en europæisk digital identitet ([8]) og navnlig den tekniske struktur og referencerammen. I overensstemmelse med betragtning 75 til Europa-Parlamentets og Rådet forordning (EU) 2024/1183 ([9]) bør Kommissionen revidere og ajourføre denne gennemførelsesforordning, hvis det er nødvendigt, for at sikre dens overensstemmelse med den globale udvikling, den tekniske struktur og referencerammen og for at følge bedste praksis på det indre marked.

(5) For at sikre præcis kommunikation, teknisk differentiering og en klar ansvarsfordeling er det nødvendigt at skelne mellem forskellige komponenter i og konfigurationer af tegnebøger. En tegnebogsløsning bør forstås som det komplette system, som en tegnebogsudbyder stiller til rådighed, og som er nødvendigt for at bruge en tegnebog. Dette bør omfatte de software- og hardwarekomponenter samt tjenester, indstillinger og konfigurationer, der er nødvendige for, at tegnebogen fungerer korrekt. En tegnebogsløsning kan placeres på brugernes enheder og miljøer og udbyderens backendstruktur. En tegnebogsenhed bør forstås som en specifik opsætning af tegnebogsløsningen for en individuel bruger. Dette bør omfatte den applikation, der er installeret på tegnebogsbrugerens enhed eller miljø, som tegnebogsbrugeren interagerer direkte med (»tegnebogsforekomsten«), og de sikkerhedsfunktioner, der er nødvendige for at beskytte brugerens oplysninger og transaktioner. Disse sikkerhedsfunktioner bør omfatte særlig software eller hardware til kryptering og beskyttelse af følsomme oplysninger. En tegnebogsforekomst bør være en del af tegnebogsenheden og give tegnebogsbrugeren adgang til deres tegnebogs funktioner.

(6) Sikre kryptografiske tegnebogsapplikationer som særskilte specialiserede komponenter i en tegnebogsenhed er ikke kun nødvendige for at beskytte kritiske aktiver såsom private kryptografiske nøgler, men også for at tilvejebringe vigtige funktioner, som f.eks. fremlæggelse af elektroniske attesteringer af attributter. Anvendelsen af fælles tekniske specifikationer kan gøre det lettere for tegnebogsudbydere at få adgang til indlejrede sikre elementer. Sikre kryptografiske tegnebogsapplikationer kan leveres på forskellige måder og til forskellige slags sikre kryptografiske tegnebogsanordninger. Hvis tegnebogsudbydere leverer brugerdefinerede sikre kryptografiske tegnebogsapplikationer som Java Card-applets til indlejrede sikre elementer, bør tegnebogsudbyderne følge de standarder, der er anført i bilag I, eller tilsvarende tekniske specifikationer.

(7) Tegnebogsenheder skal gøre det muligt for udbydere af personidentifikationsdata eller elektroniske attesteringer af attributter at verificere, at de udsteder disse data eller attesteringer til ægte tegnebogsenheder hos en tegnebogsbruger.

(8) For at sikre databeskyttelse gennem design og gennem standardindstillinger bør tegnebøgerne udstyres med de mest avancerede teknikker til beskyttelse af privatlivets fred. Disse funktioner bør give mulighed for, at tegnebøger kan bruges, uden at tegnebogsbrugeren kan spores på tværs af forskellige tegnebogsmodtagere, hvis det er relevant i brugsscenariet. Tegnebogsudbydere bør f.eks. overveje avancerede afbødningsforanstaltninger til beskyttelse af privatlivets fred i forbindelse med attesteringer af tegnebogsenheder, f.eks. anvendelse af efemere attesteringer af tegnebogsenheder eller batchudsendelse. Desuden bør indlejrede offentliggørelsespolitikker advare tegnebogsbrugerne mod uhensigtsmæssig eller ulovlig videregivelse af attributter fra elektroniske attesteringer af attributter.

(9) Attesteringer af tegnebogsenheder bør gøre det muligt for tegnebogsmodtagere, der anmoder om attributter fra tegnebogsenheder, at verificere gyldighedsstatus for den tegnebogsenhed, som de kommunikerer med, da attesteringer af tegnebogsenheder skal tilbagekaldes, når en tegnebogsenhed ikke længere anses for gyldig. Oplysningerne om tegnebogsenhedernes gyldighedsstatus bør stilles til rådighed på en interoperabel måde for at sikre, at de kan anvendes af alle tegnebogsmodtagere. I tilfælde, hvor tegnebogsbrugere har mistet deres tegnebogsenheder eller ikke længere har kontrol over dem, bør tegnebogsudbyderne desuden gøre det muligt for tegnebogsbrugerne at anmode om tilbagekaldelse af deres tegnebogsenheder. For at sikre privatlivets fred og uforbindelighed bør medlemsstaterne anvende teknikker til opretholdelse af privatlivets fred i forbindelse med attestering af tegnebogsenheder. Dette kan omfatte anvendelse af flere attesteringer af tegnebogsenheder til forskellige formål, offentliggøre af kun de relevante oplysninger om tegnebogen, der er absolut nødvendige for en transaktion, eller begrænsning af tegnebogsenhedsattesteringens levetid som et alternativ til anvendelsen af tilbagekaldelsesidentifikatorer.

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

([9]) Europa-Parlamentets og Rådets forordning (EU) 2024/1183 af 11. april 2024 om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af den europæiske ramme for digital identitet (EUT L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(10) For at sikre, at alle tegnebøger teknisk er i stand til at modtage og fremlægge personidentifikationsdata og elektroniske attesteringer af attributter i grænseoverskridende scenarier, uden at interoperabiliteten forringes, bør tegnebøgerne understøtte forudbestemte typer dataformater og selektiv videregivelse. Som fastsat i forordning (EU) nr. 910/2014 er selektiv videregivelse et begreb, der giver ejeren af data mulighed for kun at videregive visse dele af et større datasæt, så den modtagende enhed kun modtager de oplysninger, som er nødvendige for leveringen af en tjeneste, som en bruger har anmodet om. Da tegnebøgerne skal sætte brugeren i stand til selektivt at videregive attributter, bør de standarder, der er anført i bilag II, gennemføres på en måde, der muliggør en sådan funktion af tegnebøgerne. Tegnebøgerne kan desuden understøtte andre formater og funktioner for at lette specifikke brugstilfælde.

(11) Logning af transaktioner er et vigtigt redskab til at skabe gennemsigtighed, idet det giver tegnebogsbrugeren et overblik over transaktionerne. Logfiler bør endvidere anvendes til at muliggøre hurtig og nem deling af visse oplysninger på tegnebogsbrugerens anmodning med de kompetente tilsynsmyndigheder, der er oprettet i henhold til artikel 51 i forordning (EU) 2016/679, i tilfælde af mistænkelig adfærd hos tegnebogsmodtagere.

(12) For at en tegnebogsbruger kan underskrive elektronisk, bør der udstedes et kvalificeret certifikat, som er bundet til en kvalificeret elektronisk signaturgenereringsenhed, til tegnebogsbrugeren. Tegnebogsbrugeren bør have adgang til en applikation til signaturgenerering. Selv om udstedelsen af kvalificerede certifikater er en tjeneste, der udbydes af kvalificerede tillidstjenesteudbydere, bør tegnebogsudbydere eller andre enheder kunne levere de øvrige komponenter. Kvalificerede elektroniske signaturgenereringssystemer kan f.eks. forvaltes af kvalificerede tillidstjenesteudbydere som en tjeneste, eller de kan være lokale i forhold til tegnebogsbrugerens enhed, f.eks. som et smartcard. Tilsvarende kan signaturgenereringsapplikationer integreres i tegnebogsforekomsten, være en separat app på tegnebogsbrugerens enhed eller leveres eksternt.

(13) Dataeksport- og dataportabilitetsobjekter kan logge personidentifikationsdata og elektroniske attesteringer af attributter, der er udstedt til en bestemt tegnebogsenhed. Disse objekter giver tegnebogsbrugere mulighed for at udtrække de relevante data fra deres tegnebogsenhed for at styrke deres ret til dataportabilitet. Tegnebogsudbydere opfordres til at anvende de samme tekniske løsninger til også at gennemføre backup- og gendannelsesprocesser for tegnebogsenheder, så det bliver muligt at gendanne tabte tegnebogsenheder eller overføre oplysninger fra én tegnebogsudbyder til en anden, hvis det er relevant, og for så vidt som dette kan gøres uden at forringe retten til databeskyttelse og sikkerheden i økosystemet for digital identitet.

(14) Genereringen af pseudonymer, der er specifikke for tegnebogsmodtagere, bør gøre det muligt for tegnebogsbrugere at autentificere sig selv uden at give tegnebogsmodtagerne unødvendige oplysninger. Som fastsat i forordning (EU) nr. 910/2014 må tegnebogsbrugere ikke hindres i at få adgang til tjenester under et pseudonym, hvis der ikke er noget retligt krav om juridisk identitet for autentifikation. Tegnebøgerne skal derfor have en funktion til generering af brugervalgte og -forvaltede pseudonymer, der kan autentificeres, når onlinetjenester tilgås. Gennemførelsen af specifikationerne i bilag V bør derfor muliggøre sådanne funktioner. Desuden må tegnebogsmodtagere ikke anmode brugerne om at fremlægge andre data end dem, der er angivet for den påtænkte tegnebogsanvendelse i tegnebogsmodtagerens register. Tegnebogsbrugere bør have mulighed for at verificere tegnebogsmodtagernes registreringsdata på et hvilket som helst tidspunkt.

(15) Som fastsat i forordning (EU) 2024/1183 må medlemsstaterne ikke direkte eller indirekte begrænse adgangen til offentlige eller private tjenester for fysiske eller juridiske personer, som vælger ikke at anvende tegnebøger, og de skal stille passende alternative løsninger til rådighed.

(16) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([10]) og afgav udtalelse den 30. september 2024.

([10]) Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23. oktober 2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse 1247/2002/EF (EUT L 295 af 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(17) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nævnt i artikel 48 i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

Ved denne forordning fastsættes der regler for tegnebøgernes integritet og centrale funktioner, der skal ajourføres regelmæssigt, så de er i overensstemmelse med den teknologiske udvikling og udviklingen af standarder og med det arbejde, der udføres på grundlag af henstilling (EU) 2021/946, navnlig den tekniske struktur og referencerammen.

Artikel 2

Definitioner

I denne forordning forstås ved:

(1) »sikker kryptografisk tegnebogsapplikation«: en applikation, der forvalter kritiske aktiver ved at være knyttet til og anvende de kryptografiske og ikkekryptografiske funktioner, der leveres af en sikker kryptografisk tegnebogsanordning

(2) »tegnebogsenhed«: en unik konfiguration af en tegnebogsløsning, der omfatter forekomster af tegnebøger, sikre kryptografiske tegnebogsapplikationer og sikre kryptografiske tegnebogsanordninger, som en tegnebogsudbyder stiller til rådighed for en individuel tegnebogsbruger

(3) »kritiske aktiver«: aktiver i eller i forbindelse med en tegnebogsenhed af så ekstraordinær betydning, at det i alvorlig grad vil svække muligheden for at have tillid til tegnebogsenheden, hvis deres tilgængelighed, fortrolighed eller integritet kompromitteres

(4) »udbyder af personidentifikationsdata«: en fysisk eller juridisk person, der er ansvarlig for at udstede og tilbagekalde personidentifikationsdata og sikre, at en brugers personidentifikationsdata er kryptografisk bundet til en tegnebogsenhed

(5) »tegnebogsbruger«: en bruger, der har kontrol over tegnebogsenheden

(6) »tegnebogsmodtager«: en modtagerpart, der har til hensigt at benytte tegnebogsenheder til levering af offentlige eller private tjenester ved hjælp af digital interaktion

(7) »tegnebogsudbyder«: en fysisk eller juridisk person, der leverer tegnebogsløsninger

(8) »attestering af tegnebogsenhed« og »tegnebogsattestering«: et dataobjekt, der beskriver tegnebogsenhedens komponenter eller gør det muligt at autentificere og validere disse komponenter

(9) »indlejret offentliggørelsespolitik«: et sæt regler, der er indlejret i en elektronisk attestering af attributter fra udbyderen, der angiver de betingelser, som en tegnebogsmodtager skal opfylde for at få adgang til den elektroniske attestering af attributter

(10) »tegnebogsforekomst«: den applikation, der er installeret og konfigureret på en tegnebogsbrugers enhed eller miljø, som er en del af en tegnebogsenhed, og som tegnebogsbrugeren bruger til at interagere med tegnebogsenheden

(11) »tegnebogsløsning«: en kombination af software, hardware, tjenester, indstillinger og konfigurationer, herunder tegnebogsforekomster, en eller flere sikre kryptografiske tegnebogsapplikationer og en eller flere sikre kryptografiske tegnebogsanordninger

(12) »sikker kryptografisk tegnebogsanordning«: en anordning, der er sikret mod manipulation, og som tilvejebringer et miljø, der er knyttet til og anvendes af den sikre kryptografiske tegnebogsapplikation til at beskytte kritiske aktiver og tilvejebringe kryptografiske funktioner til sikker udførelse af kritiske operationer

(13) »kryptografisk tegnebogsoperation«: en kryptografisk mekanisme, der er nødvendig i forbindelse med autentifikation af tegnebogsbrugeren og udstedelse eller fremlæggelse af personidentifikationsdata eller elektroniske attesteringer af attributter

(14) »adgangscertifikat for tegnebogsmodtager«: et certifikat for elektroniske segl eller signaturer, der autentificerer og validerer tegnebogsmodtageren, og som er udstedt af en udbyder af adgangscertifikater for tegnebogsmodtagere

(15) »udbyder af adgangscertifikater for tegnebogsmodtagere«: en fysisk eller juridisk person, der er bemyndiget af en medlemsstat til at udstede adgangscertifikater for tegnebogsmodtagere, der er registreret i den pågældende medlemsstat.

KAPITEL II

EUROPÆISKE DIGITALE IDENTITETSTEGNEBØGERS INTEGRITET

Artikel 3

Tegnebogsenhedens integritet

1. Tegnebogsenheder må ikke udføre nogen af de funktioner, der er anført i artikel 5a, stk. 4, i forordning (EU) nr. 910/2014, undtagen tegnebogsbrugerautentifikation med henblik på adgang til tegnebogsenheden, før tegnebogsenheden har autentificeret tegnebogsbrugeren.

2. Tegnebogsudbydere underskriver eller forsegler for hver tegnebogsenhed mindst én attestering af tegnebogsenheden, der opfylder kravene i artikel 6. Det certifikat, der anvendes til at underskrive eller forsegle tegnebogsenhedsattesteringen, udstedes i henhold til et certifikat, der er opført på den positivliste, der er omhandlet i gennemførelsesforordning (EU) 2024/2980.

Artikel 4

Tegnebogsforekomster

1. Tegnebogsforekomster skal anvende mindst én sikker kryptografisk tegnebogsanordning til at forvalte kritiske aktiver.

2. Tegnebogsudbydere sikrer integritet, autenticitet og fortrolighed i kommunikationen mellem tegnebogsforekomster og sikre kryptografiske tegnebogsapplikationer.

3. Hvis kritiske aktiver vedrører udførelse af elektronisk identifikation på sikringsniveauet »høj«, skal kryptografiske tegnebogsoperationer eller andre operationer til behandling af kritiske aktiver udføres i overensstemmelse med kravene til de elektroniske identifikationsmidlers karakteristika og udformning på sikringsniveauet »høj« som omhandlet i Kommissionens gennemførelsesforordning (EU) 2015/1502 ([11]).

Artikel 5

Sikre kryptografiske tegnebogsapplikationer

1. Tegnebogsudbydere sørger for, at sikre kryptografiske tegnebogsapplikationer:

a) kun udfører kryptografiske tegnebogsoperationer, der involverer andre kritiske aktiver end dem, der er nødvendige for, at tegnebogsenheden kan autentificere tegnebogsbrugeren, i tilfælde, hvor disse applikationer har godkendt tegnebogsbrugere

([11]) Kommissionens gennemførelsesforordning (EU) 2015/1502 af 8. september 2015 om fastlæggelse af tekniske minimumsspecifikationer og procedurer for fastsættelse af sikringsniveauer for elektroniske identifikationsmidler i henhold til artikel 8, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (EUT L 235 af 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

b) ved autentifikation af tegnebogsbrugere i forbindelse med udførelse af elektronisk identifikation på sikringsniveauet »høj« autentificerer tegnebogsbrugerne i overensstemmelse med kravene til elektroniske identifikationsmidlers karakteristika og udformning på sikringsniveauet »høj« som omhandlet i gennemførelsesforordning (EU) 2015/1502

c) kan generere nye kryptografiske nøgler på en sikker måde

d) kan foretage sikker sletning af kritiske aktiver

e) kan generere et bevis for besiddelse af private nøgler

f) beskytter de private nøgler, der genereres af disse sikre kryptografiske tegnebogsapplikationer til tegnebøger, så længe nøglerne eksisterer

g) opfylder kravene til elektroniske identifikationsmidlers karakteristika og udformning på sikringsniveauet »høj« som omhandlet i gennemførelsesforordning (EU) 2015/1502

h) er de eneste komponenter, der kan udføre kryptografiske tegnebogsoperationer og enhver anden operation med kritiske aktiver i forbindelse med udførelse af elektronisk identifikation på sikringsniveauet »høj«.

2. Hvis tegnebogsudbydere beslutter at levere en sikker kryptografisk tegnebogsapplikation til et indlejret sikkert element, baserer tegnebogsudbyderne deres tekniske løsning på de tekniske specifikationer, der er anført i bilag I, eller på andre tilsvarende tekniske specifikationer.

Artikel 6

Tegnebogsenhedens ægthed og gyldighed

1. Tegnebogsudbydere sikrer, at hver tegnebogsenhed indeholder attesteringer af tegnebogsenheder.

2. Tegnebogsudbydere sikrer, at de attesteringer af tegnebogsenheder, der er omhandlet i stk. 1, indeholder offentlige nøgler, og at de tilsvarende private nøgler er beskyttet af en sikker kryptografisk tegnebogsanordning.

3. Tegnebogsudbydere skal:

a) informere tegnebogsbrugere om deres rettigheder og forpligtelser i forbindelse med deres tegnebogsenhed

b) sørge for mekanismer, der er uafhængige af tegnebogsenheder, til sikker identifikation og autentifikation af tegnebogsbrugere

c) sikre, at tegnebogsbrugere har ret til at anmode om tilbagekaldelse af deres attesteringer af tegnebogsenheder ved hjælp af de autentifikationsmekanismer, der er omhandlet i litra (b).

Artikel 7

Tilbagekaldelse af attesteringer af tegnebogsenheder

1. Tegnebogsudbydere skal være de eneste enheder, der kan tilbagekalde attesteringer af tegnebogsenheder for tegnebogsenheder, som de har leveret.

2. Tegnebogsudbydere fastsætter en offentligt tilgængelig politik med angivelse af betingelserne og tidsrammen for tilbagekaldelse af attesteringer af tegnebogsenheder.

3. Hvis tegnebogsudbydere har tilbagekaldt attesteringer af tegnebogsenheder, skal de underrette de berørte tegnebogsbrugere senest 24 timer efter tilbagekaldelsen af deres tegnebogsenheder og angive årsagen til tilbagekaldelsen og konsekvenserne for tegnebogsbrugeren. Disse oplysninger skal gives på en måde, der er kortfattet, let tilgængelig og i et klart og enkelt sprog.

4. Hvis tegnebogsudbydere har tilbagekaldt attesteringer af tegnebogsenheder, skal de offentliggøre gyldighedsstatus for attesteringen af tegnebogsenheden på en måde, der beskytter privatlivets fred, og beskrive placeringen af disse oplysninger i attesteringen af tegnebogsenheden.

KAPITEL III

CENTRALE FUNKTIONER I OG EGENSKABER VED EUROPÆISKE DIGITALE IDENTITETSTEGNEBØGER

Artikel 8

Formater for personidentifikationsdata og elektroniske attesteringer af attributter

Tegnebogsudbydere sikrer, at tegnebogsløsninger understøtter brugen af personidentifikationsdata og elektroniske attesteringer af attributter, der er udstedt i overensstemmelse med listen over standarder i bilag II.

Artikel 9

Transaktionslogfiler

1. Uanset om en transaktion gennemføres korrekt eller ej, skal tegnebogsforekomster logge alle transaktioner med tegnebogsmodtagere og andre tegnebogsenheder, herunder elektroniske signaturer og segl.

2. De loggede oplysninger skal mindst indeholde:

a) tid og dato for transaktionen

b) navn, kontaktoplysninger og den entydige identifikator for den tilsvarende tegnebogsmodtager og den medlemsstat, hvor den pågældende tegnebogsmodtager er etableret, eller, hvis der er tale om andre tegnebogsenheder, relevante oplysninger fra attesteringen af tegnebogsenheder

c) den eller de typer data, der anmodes om og fremlægges i transaktionen

d) i tilfælde af ikkegennemførte transaktioner, årsagen til den manglende gennemførelse.

3. Tegnebogsudbydere sikrer integriteten, autenticiteten og fortroligheden af de loggede oplysninger.

4. Tegnebogsforekomster skal logge rapporter, som tegnebogsbrugeren har sendt til databeskyttelsesmyndighederne via deres tegnebogsenhed.

5. De logfiler, der er omhandlet i stk. 1 og 2, skal være tilgængelige for tegnebogsudbyderen, hvis det er nødvendigt for leveringen af tegnebogstjenester, på grundlag af tegnebogsbrugerens udtrykkelige forudgående samtykke.

6. De logfiler, der er omhandlet i stk. 1 og 2, skal være tilgængelige, så længe de kræves i henhold til EU-retten eller national ret.

7. Tegnebogsudbydere skal give tegnebogsbrugere mulighed for at eksportere de loggede oplysninger, der er omhandlet i stk. 2.

Artikel 10

Indlejret offentliggørelse

1. Tegnebogsudbydere sikrer, at elektroniske attesteringer af attributter med fælles indlejrede offentliggørelsespolitikker omhandlet i bilag III kan behandles af de tegnebogsenheder, som de stiller til rådighed.

2. Tegnebogsforekomster skal kunne behandle og fremlægge indlejrede offentliggørelsespolitikker som omhandlet i stk. 1 sammen med data modtaget fra den anmodende tegnebogsmodtager.

3. Tegnebogsforekomster skal verificere, om tegnebogsmodtageren opfylder kravene i den indlejrede offentliggørelsespolitik, og informere tegnebogsbrugeren om resultatet.

Artikel 11

Kvalificerede elektroniske signaturer og segl

1. Tegnebogsudbydere sikrer, at tegnebogsbrugere kan modtage kvalificerede certifikater for kvalificerede elektroniske signaturer eller segl, der er knyttet til kvalificerede signatur- eller seglgenereringsenheder, som enten er lokale, eksterne eller fjerntliggende i forhold til tegnebogsforekomsterne.

2. Tegnebogsudbydere sikrer, at tegnebogsløsninger kan kommunikere sikkert med en af følgende typer kvalificerede signatur- eller seglgenereringsenheder: lokale, eksterne eller fjernstyrede kvalificerede signatur- eller seglgenereringssystemer med henblik på anvendelse af de kvalificerede certifikater, der er omhandlet i stk. 1.

3. Tegnebogsudbydere sikrer, at tegnebogsbrugere, som er fysiske personer, i det mindste til ikkeerhvervsmæssige formål har gratis adgang til signaturgenereringsapplikationer, der gør det muligt at generere gratis kvalificerede elektroniske signaturer ved hjælp af de certifikater, der er omhandlet i stk. 1.

Artikel 12

Signaturgenereringsapplikationer

1. De signaturgenereringsapplikationer, der anvendes af tegnebogsenheder, kan leveres af tegnebogsudbydere, af udbydere af tillidstjenester eller af tegnebogsmodtagere.

2. Signaturgenereringsapplikationer skal have følgende funktioner:

a) signering eller forsegling af data leveret af tegnebogsbrugere

b) signering eller forsegling af data leveret af tegnebogsmodtagere

c) generering af signaturer eller segl i overensstemmelse med mindst det obligatoriske format, der omhandlet i bilag IV

d) underretning af tegnebogsbrugere om resultatet af signatur- eller seglgenereringsprocessen.

3. Signaturgenereringsapplikationerne kan være integreret i eller være eksterne i forhold til tegnebogsforekomster. Hvis signaturgenereringsapplikationer er baseret på kvalificerede fjernsignaturgenereringssystemer, og hvis de er integreret i tegnebogsforekomster, skal de understøtte den API-grænseflade (Application Programming Interface), der er omhandlet i bilag IV.

Artikel 13

Dataeksport og -portabilitet

Tegnebogsenheder skal, hvor det er teknisk muligt og med undtagelse af tilfælde af kritiske aktiver, understøtte sikker eksport og portabilitet af tegnebogsbrugerens personoplysninger for at gøre det muligt for tegnebogsbrugeren at migrere til en tegnebogsenhed i en anden tegnebogsløsning på en måde, der garanterer sikringsniveauet »høj« som fastsat i gennemførelsesforordning (EU) 2015/1502.

Artikel 14

Pseudonymer

1. Tegnebogsenheder skal understøtte genereringen af pseudonymer for tegnebogsbrugere i overensstemmelse med de tekniske specifikationer i bilag V.

2. Efter anmodning fra en tegnebogsmodtager skal tegnebogsenheder understøtte genereringen af et pseudonym, der er specifikt og unikt for den pågældende tegnebogsmodtager, og give dette pseudonym til tegnebogsmodtageren enten for sig eller i kombination med eventuelle personidentifikationsdata eller elektroniske attesteringer af attributter, som den pågældende tegnebogsmodtager har anmodet om.

KAPITEL IV

AFSLUTTENDE BESTEMMELSER

Artikel 15

Ikrafttræden

Denne forordning træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 28. november 2024.

På Kommissionens vegne
Ursula VON DER LEYEN
Formand

BILAG I

LISTE OVER STANDARDER, JF. ARTIKEL 5

— SAM.01 (Secured Applications for Mobile) — Krav til understøttelse af applets fra tredjeparter på eSIM og eSE via SAM, v1.1 2023, GSMA

— GPC_GUI_ 217 GlobalPlatform SAM Configuration — Teknisk specifikation til gennemførelse af SAM, v1.0 2024-04

— GPC_SPE_0 34 GlobalPlatform Card Specification — Teknisk specifikation til smartcards, 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 mobilapps til tilgang af sikre elementer på brugerenheder, v3.3 2018-08, GlobalPlatform.

BILAG II

LISTE OVER STANDARDER, JF. ARTIKEL 8

— ISO/IEC.18013-5:2021

— »Verifiable Credentials Data Model 1.1«, W3C Recommendation, 3. marts 2022.

BILAG III

LISTE OVER FÆLLES INDLEJREDE OFFENTLIGGØRELSESPOLITIKKER, JF. ARTIKEL 10

1. »Ingen politik«, hvilket vil sige, at der ikke gælder nogen politik for elektroniske attesteringer af attributter.
2. »Politik om udelukkende godkendte modtagerparter«, hvilket vil sige, at tegnebogsbrugere kun må videregive elektroniske attesteringer af attributter til autentificerede modtagerparter, som udtrykkeligt er anført i offentliggørelsespolitikken.
3. »Specifik root-of-trust«, hvilket vil sige, at tegnebogsbrugere kun bør videregive den specifikke elektroniske attestering af attributter til autentificerede tegnebogsmodtagere med adgangscertifikater for tegnebogsmodtagere, der er afledt af en specifik rod (eller liste over specifikke rødder) eller et eller flere mellemliggende certifikater.

BILAG IV

FORMATER FOR SIGNATURER OG SEGL, JF. ARTIKEL 12

1. Obligatorisk signatur- eller seglformat:

   a) PAdES (PDF Advanced Electronic Signature) som specificeret i »ETSI EN 319 142-1 V1.1.1 (2016-04), Electronic Signatures and Infrastructures (ESI), PAdES digital signatures, Part 1: Building blocks and PAdES baseline signatures«.

2. Valgfrie signatur- eller seglformater:

   a) XAdES som specificeret i »ETSI EN 319 132-1 V1.2.1 (2022-02) Electronic Signatures and Infrastructures (ESI), XAdES digital signatures, Part 1: Building blocks and XAdES baseline signatures (XAdES)« til signering af XML-format

   b) JAdES som specificeret i »ETSI TS 119 182-1 V1.2.1 (2024-07) Electronic Signatures and Infrastructures (ESI), JAdES digital signatures, Part 1: Building blocks and JAdES baseline signatures« til signering af JSON-format

   c) CAdES (CMS Advanced Electronic Signature) som specificeret i »ETSI EN 319 122-1 V1.3.1 (2023-06) Electronic Signatures and Infrastructures (ESI), CAdES digital signatures, Part 1: Building blocks and CAdES baseline signatures« til signering af CMS-format

   d) ASiC (Associated Signature Container) som specificeret i »ETSI EN 319 162-1 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI), Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers and ETSI EN 319 162-2 V1.1.1 (2016-04) Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers« til signering af containere.

3. API-grænseflade:

   — Cloud Signature Consortium (CSC) specifikation v2.0 (20. april 2023).

BILAG V

TEKNISKE SPECIFIKATIONER FOR GENERERING AF PSEUDONYMER, JF. ARTIKEL 14

Tekniske specifikationer:

— WebAuthn — W3C Recommendation (8. april 2021), Level 2, https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.