2024/2981

4.12.2024

KOMMISSIONENS GENNEMFØRELSESFORORDNING (EU) 2024/2981

af 28. november 2024

om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår certificering af 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 5c, stk. 6, og

ud fra følgende betragtninger:

(1) I henhold til artikel 5c i forordning (EU) nr. 910/2014 skal certificeringen af europæiske digitale identitetstegnebøger (»tegnebøger«) foretages i overensstemmelse med krav til funktion, cybersikkerhed og databeskyttelse for at sikre et højt niveau af sikkerhed og tillid til tegnebøgerne. Disse certificeringskrav skal harmoniseres på tværs af medlemsstaterne for at forhindre markedsfragmentering og opbygge en solid ramme.

(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) 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 forordning, 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 ([4]) og navnlig den tekniske struktur og referenceramme, der indgår heri. I overensstemmelse med betragtning 75 til Europa-Parlamentets og Rådets forordning (EU) 2024/1183 ([5]) bør Kommissionen efter behov revidere og ajourføre denne gennemførelsesforordning for at sikre dens overensstemmelse med den globale udvikling, den tekniske struktur og referencerammen og for at følge bedste praksis på det indre marked.

(4) For at attestere overensstemmelse med cybersikkerhedskravene i certificeringsrammen bør certificeringen af tegnebogsløsninger, hvor det er muligt og relevant, henvise til europæiske cybersikkerhedscertificeringsordninger, der er oprettet i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/881 ([6]). Hvis sådanne ordninger ikke findes, eller hvis de delvist omfatter cybersikkerhedskrav, fastsætter denne forordning de generelle krav, der gælder for nationale certificeringsordninger, herunder funktionelle krav, cybersikkerhedskrav og databeskyttelseskrav.

([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]) EUT L 210 af 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.
([5]) 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).
([6]) Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(5) I henhold til artikel 5a, stk. 11, i forordning (EU) nr. 910/2014 skal tegnebøgerne certificeres på sikringsniveauet »høj« som fastsat i forordning (EU) nr. 910/2014 samt Kommissionens gennemførelsesforordning (EU) 2015/1502 ([7]). Dette sikringsniveau skal nås af tegnebogsløsningen som helhed. I henhold til denne forordning kan visse komponenter i tegnebogsløsningen certificeres på et lavere sikringsniveau, forudsat at dette er behørigt begrundet, og uden at det berører det sikringsniveau, der er nået af tegnebogsløsningen som helhed.

(6) Alle nationale certificeringsordninger bør udpege en ordningsansvarlig, som skal være ansvarlig for udviklingen og vedligeholdelsen af certificeringsordningen. Den ordningsansvarlige kan være et overensstemmelsesvurderingsorgan, et statsligt organ eller en offentlig myndighed, en brancheorganisation, en gruppe af overensstemmelsesvurderingsorganer eller ethvert relevant organ og kan være et andet organ end det, der forvalter den nationale certificeringsordning.

(7) Genstanden for certificeringen bør omfatte tegnebogsløsningens softwarekomponenter, som f.eks. tegnebogsforekomsten. Den sikre kryptografiske tegnebogsapplikation (»WSCA«), den sikre kryptografiske tegnebogsanordning (»WSCD«) og de platforme, som disse softwarekomponenter udføres på, bør, selv om de er en del af driftsmiljøet, kun medtages i genstanden for certificeringen, når de leveres af tegnebogsløsningen. I andre tilfælde, og navnlig når disse anordninger og platforme leveres af slutbrugere, bør udbyderne opstille antagelser om tegnebogsløsningens driftsmiljø, herunder om disse anordninger og platforme, og træffe foranstaltninger for at bekræfte antagelserne i praksis. For at sikre beskyttelse af kritiske aktiver gennem hardware og systemsoftware, der anvendes til at forvalte og beskytte kryptografiske nøgler, der oprettes, lagres eller behandles af den sikre kryptografiske tegnebogsanordning, skal tegnebogsanordningen opfylde høje certificeringsstandarder, der er i overensstemmelse med internationale standarder, f.eks. de fælles kriterier (»EUCC«), der er fastsat i Kommissionens gennemførelsesforordning (EU) 2024/482 ([8]), ved hjælp af EAL4-evaluering og avanceret metodisk sårbarhedsanalyse, som svarende til f.eks. AVA_VAN.5. Disse certificeringsstandarder bør anvendes senest, når der foretages certificering af tegnebøgers overensstemmelse efter en europæisk cybersikkerhedscertificeringsordning, der er vedtaget i henhold til forordning (EU) 2019/881.

(8) Fuldt mobile, sikre og brugervenlige tegnebøger understøttes af, at der findes standardiserede og certificerede manipulationssikrede løsninger, f.eks. indlejrede sikre elementer, eksterne anordninger såsom smartcards, eller indlejrede SIM-platforme i mobilenheder. Det er vigtigt at sikre rettidig adgang til indlejrede sikre elementer for nationale eID-midler og -tegnebøger og at koordinere medlemsstaternes indsats på dette område. Den Europæiske Samarbejdsgruppe for Digital Identitet, som er nedsat i henhold til artikel 46e, stk. 1, i forordning (EU) nr. 910/2014 (»samarbejdsgruppen«), bør derfor nedsætte en særlig undergruppe til dette formål. Undergruppen bør høre de relevante interessenter og nå til enighed om en fælles køreplan for adgang til indlejrede sikre elementer, som Kommissionen kan tage i betragtning i forbindelse med revisionsrapporten om forordning (EU) nr. 910/2014. For at lette udbredelsen af tegnebøger på nationalt plan bør Kommissionen desuden i samarbejde med medlemsstaterne udvikle og løbende ajourføre en håndbog med brugstilfælde som led i den tekniske struktur og referencerammen.

(9) Genstanden for certificeringen i nationale certificeringsordninger bør også omfatte de procedurer, der anvendes til at levere og drive tegnebogsløsningen, selv om definitionen eller gennemførelsen af disse procedurer gives i underentreprise til tredjeparter. For at påvise, at procedurerne opfylder kravene i ordningerne, kan oplysninger om sikring anvendes som dokumentation, forudsat at der anvendes en afhængighedsanalyse til at afgøre, om sikringsoplysningerne er tilstrækkelige. Oplysninger om sikring findes i mange forskellige former, herunder rapporter og overensstemmelsesattester, som kan være private, nationale, europæiske eller internationale, baseret på standarder eller tekniske specifikationer. Formålet med afhængighedsanalysen er at vurdere kvaliteten af de sikringsoplysninger om tegnebogens komponenter, der foreligger.

([7]) 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).

([8]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg/2024/482/oj).

(10) Samarbejdsgruppen bør efter procedurer, der er fastlagt til formålet, kunne afgive udtalelser og fremsætte henstillinger om de udkast til nationale certificeringsordninger, som forelægges for gruppen. Disse nationale certificeringsordninger bør være specifikke for tegnebogens tekniske struktur, og der bør være specifikke profiler for hver specifik teknisk struktur, der understøttes.

(11) For at sikre en fælles forståelse af og en harmoniseret tilgang til vurderingen af de mest kritiske risici, der kan påvirke leveringen og driften af tegnebøger, bør der udarbejdes et register over risici og trusler, der bør tages i betragtning ved udformningen af tegnebogsløsninger, uafhængigt af deres specifikke tekniske struktur. De cybersikkerhedsmål, der er beskrevet i forordning (EU) nr. 910/2014, f.eks. tegnebogsløsningens fortrolighed, integritet og tilgængelighed, samt beskyttelse af brugernes personoplysninger og privatliv, bør tages i betragtning, når det fastlægges, hvilke risici der bør medtages i registret. Hensyntagen til de risici og trusler, der er medtaget i dette risikoregister, bør være en del af kravene i de nationale certificeringsordninger. For at følge med trusselsbilledet, som hele tiden udvikler sig, bør risikoregistret vedligeholdes og ajourføres regelmæssigt i samarbejde med samarbejdsgruppen.

(12) Når de ordningsansvarlige udformer deres certificeringsordninger, bør de foretage en risikovurdering for at finjustere og supplere de risici og trusler, der er opført i registret, med risici og trusler, der er specifikke for tegnebogsløsningens tekniske struktur eller implementering. I risikovurderingen bør det overvejes, hvordan de relevante risici og trusler kan behandles korrekt. Tegnebogsudbydere bør supplere ordningens risikovurdering for at afdække eventuelle risici og trusler, der er specifikke for deres implementering, og foreslå passende behandlingsforanstaltninger, der evalueres af certificeringsorganet.

(13) For at påvise, at en tegnebogsløsnings tekniske struktur opfylder de gældende sikkerhedskrav, bør hver strukturspecifik ordning eller profil mindst indeholde en beskrivelse af tegnebogsløsningens tekniske struktur, en liste over, hvilke sikkerhedskrav der gælder for den pågældende tekniske struktur, en plan for evalueringen med henblik på at bekræfte, at en tegnebogsløsning baseret på denne tekniske struktur opfylder disse krav, og en risikovurdering. Nationale certificeringsordninger bør kræve, at tegnebogsudbydere påviser, hvordan udformningen af den tegnebogsløsning, de leverer, svarer til referencestrukturen, og beskriver sikkerhedskontrollerne og valideringsplanerne for den specifikke tegnebogsløsning. Nationale certificeringsordninger bør også fastlægge en overensstemmelsesvurderingsaktivitet til at kontrollere, at tegnebogens udformning korrekt afspejler den valgte profils referencestruktur. Nationale certificeringsordninger bør opfylde kravene i artikel 51 i forordning (EU) 2019/881, bortset fra nævnte artikels litra e) og f), vedrørende logning.

(14) For så vidt angår certificering af produkter bør det være tilladt at anvende overensstemmelsesattester, der er udstedt i henhold til EU's cybersikkerhedscertificeringsordning baseret på EUCC, og overensstemmelsesattester, der er udstedt i henhold til nationale certificeringsordninger inden for rammerne af SOG-IS-aftalen om gensidig anerkendelse. Andre nationale certificeringsordninger bør også kunne anvendes for mindre følsomme produktkomponenter, f.eks. dem, der er fastsat i henhold til standard CEN EN 17640 om tidsbestemt cybersikkerhedsevalueringsmetode for IKT-produkter.

(15) EU-tillidsmærket for europæiske digitale identitetstegnebøger (»tillidsmærket«) bør anvendes til på en klar, enkel og genkendelig måde at angive, at en tegnebog er leveret i overensstemmelse med forordning (EU) nr. 910/2014. Det bør derfor betragtes som et overensstemmelsesmærke for en tegnebogsløsning, der er certificeret i henhold til nationale certificeringsordninger. Nationale certificeringsordninger bør ikke fastsætte andre overensstemmelsesmærker.

(16) For at modvirke svig bør de nationale certificeringsordninger fastlægge, hvilke foranstaltninger der skal træffes, når der svigagtigt ansøges om certificering i henhold til ordningen.

(17) For at sikre en effektiv forvaltning af anmeldelser af sårbarhed bør udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, fastlægge og gennemføre procedurer med henblik på at evaluere sårbarhedernes alvor og potentielle indvirkning. I nationale certificeringsordninger bør der fastsættes en tærskel, over hvilken certificeringsorganet skal underrettes. En sådan anmeldelsespligt bør ikke berøre de kriterier, der er fastsat i databeskyttelseslovgivningen og af medlemsstaternes databeskyttelsesmyndigheder for anmeldelse af brud på persondatasikkerheden. Der kan skabes mulig synergi mellem den obligatoriske anmeldelse af brud vedrørende eller kompromittering af tegnebogsløsningerne og anmeldelsen af brud på persondatasikkerheden i henhold til forordning (EU) 2016/679. Certificeringsorganets vurdering af en rapport om sårbarhedskonsekvensanalyse bør ikke berøre en databeskyttelsesmyndigheds vurdering af en konsekvensanalyse vedrørende databeskyttelse i henhold til artikel 35 og 36 i forordning (EU) 2016/679.

(18) Udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, bør underrette den ordningsansvarlige om eventuelle begrundelser for undtagelser fra den sårbarhedsvurdering, der kræves til evalueringen af den sikre kryptografiske tegnebogsanordning og den sikre kryptografiske tegnebogsapplikation, jf. bilag IV.

(19) Annullering af en overensstemmelsesattest kan have alvorlige konsekvenser, f.eks. tilbagekaldelse af alle anvendte tegnebogsenheder. Certificeringsorganerne bør derfor kun overveje annullering, hvis en sårbarhed, der ikke afhjælpes, sandsynligvis i væsentlig grad vil svække pålideligheden af tegnebogsløsningen eller pålideligheden af en anden tegnebogsløsning.

(20) Der bør indføres en særlig procedure for ajourføring af nationale certificeringsordninger for at styre overgangen mellem successive udgaver af ordningerne, navnlig i forbindelse med foranstaltninger, som attestindehaveren skal træffe vedrørende kommende evalueringer, vedligeholdelse, fornyet certificering og særlige evalueringer.

(21) For at fremme gennemsigtigheden bør tegnebogsudbydere offentligt dele sikkerhedsoplysninger om deres tegnebogsløsning.

(22) Hvis nationale certificeringsordninger er baseret på sikringsoplysninger fra andre certificeringsordninger eller -kilder, bør der foretages en afhængighedsanalyse for at kontrollere, at sikringsdokumentationen, f.eks. sikringsrapporter og overensstemmelsesattester, er tilgængelig og tilstrækkelig for tegnebogsløsningerne og den elektroniske identifikationsordning, som de leveres under. Grundlaget for denne afhængighedsanalyse bør være risikovurderingen af tegnebogsløsningerne og den elektroniske identifikationsordning, som de leveres under. Evalueringen bør fastslå, om den sikringsdokumentation, der er til rådighed for en given tegnebogsløsning og den elektroniske identifikationsordning, som den leveres under, er tilstrækkelig til at give en sikkerhed, der svarer til det ønskede evalueringsniveau. Evalueringen bør også ajourføre afhængighedsanalysen eller, hvor det er nødvendigt, revurdere den fuldstændigt.

(23) Certificeringsorganerne bør udstede overensstemmelsesattester i nationale certificeringsordninger sammen med en offentligt tilgængelig certificeringsrapport som omhandlet i artikel 5d, stk. 2, litra a), i forordning (EU) nr. 910/2014. Den tilhørende certificeringsvurderingsrapport bør stilles til rådighed for samarbejdsgruppen.

(24) Nationale certificeringsordninger bør fastsætte årlige overvågningsevalueringer for at sikre, at procedurerne omkring forvaltning og vedligeholdelse af tegnebøgerne fungerer effektivt, dvs. at de fungerer i overensstemmelse med de politikker, der fastlægger procedurerne. Den toårige sårbarhedsvurdering er et krav i henhold til forordning (EU) nr. 910/2014 for at sikre, at tegnebogsløsningerne fortsat på passende vis dækker de cybersikkerhedsrisici og -trusler, der er identificeret i risikoregistret, herunder enhver udvikling i trusselsbilledet. Begreberne overvågningsevalueringer, evalueringer med henblik på fornyet certificering og særlige evalueringer bør være i overensstemmelse med EN ISO/IEC 17021-1:2015.

(25) En certificeringscyklus afsluttes med udløbet af overensstemmelsesattesten eller med udstedelsen af en ny overensstemmelsesattest efter en vellykket evaluering med henblik på fornyet certificering. Evalueringen med henblik på fornyet certificering bør omfatte en evaluering af alle komponenter i genstanden for certificeringen, herunder en evaluering af effektiviteten og, hvis det er relevant, en sårbarhedsvurdering. Under en evaluering med henblik på fornyet certificering bør det være muligt at genbruge resultater fra tidligere evalueringer af komponenter, der ikke er ændret.

(26) Når der vedtages en europæisk cybersikkerhedscertificeringsordning, bør nationale certificeringsordninger med samme anvendelsesområde ophøre med at udstede attester efter en fastsat overgangsperiode omhandlet i artikel 57, stk. 1, i forordning (EU) 2019/881.

(27) Nationale certificeringsordninger bør bygge på eksisterende rammer og genanvende dokumentation, hvis det er relevant, for at sikre harmonisering og interoperabilitet. Medlemsstaterne kan indgå aftaler om grænseoverskridende genanvendelse af certificeringsordninger eller dele heraf. Kommissionen og ENISA bør i samarbejde med samarbejdsgruppen støtte medlemsstaterne i udviklingen og vedligeholdelsen af deres nationale certificeringsordninger, der sikrer deling af viden og bedste praksis.

(28) Den Europæiske Tilsynsførende for Databeskyttelse blev hørt i overensstemmelse med artikel 42, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2018/1725 ([9]) og afgav udtalelse den 30. september 2024.

(29) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra det udvalg, der er nævnt i artikel 48, stk. 1, i forordning (EU) nr. 910/2014 —

VEDTAGET DENNE FORORDNING:

KAPITEL I

ALMINDELIGE BESTEMMELSER

Artikel 1

Genstand og anvendelsesområde

Ved denne forordning fastsættes der referencestandarder, specifikationer og procedurer med henblik på at opbygge en solid ramme for certificering af tegnebøger, 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 om en fælles EU-værktøjskasse for en koordineret tilgang til en ramme for en europæisk digital identitet, og navnlig den tekniske struktur og referencerammen.

Artikel 2

Definitioner

I denne forordning forstås ved:

(1) »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

(2) »ordningsansvarlig«: en organisation, der er ansvarlig for at udvikle og vedligeholde en certificeringsordning

(3) »genstand for certificering«: produkter, procedurer og tjenesteydelser eller en kombination heraf, for hvilke der gælder specifikke krav

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

(5) »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

([9]) 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).

(6) »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

(7) »risikoregister«: en fortegnelse over oplysninger, der er relevante for certificeringsproceduren, om identificerede risici

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

(9) »certificeringsorgan«: et tredjepartsoverensstemmelsesvurderingsorgan, der forvalter certificeringsordninger

(10) »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

(11) »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

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

(13) »hændelse«: en hændelse som defineret i artikel 6, nr. 6), i Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 ([10])

(14) »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.

KAPITEL II

NATIONALE CERTIFICERINGSORDNINGER

Artikel 3

Oprettelse af nationale certificeringsordninger

1. Medlemsstaterne udpeger en ordningsansvarlig for hver national certificeringsordning.

2. Genstanden for certificering som defineret i nationale certificeringsordninger skal være levering og drift af tegnebogsløsninger og af de elektroniske identifikationsordninger, som de leveres under.

3. I overensstemmelse med gennemførelsesforordning (EU) 2015/1502 skal genstanden for certificering i nationale certificeringsordninger omfatte følgende elementer:

a) softwarekomponenterne, herunder indstillinger og konfigurationer af en tegnebogsløsning og af den elektroniske identifikationsordning, som tegnebogsløsningen leveres under

b) de hardwarekomponenter og -platforme, som de softwarekomponenter, der er omhandlet i nr. b), kører på eller anvender til kritiske operationer, når de leveres direkte eller indirekte af tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under, og når de skal opfylde det ønskede sikringsniveau for disse softwarekomponenter. Hvis hardwarekomponenterne og -platformene ikke leveres af tegnebogsudbyderen, skal de nationale certificeringsordninger opstille antagelser med henblik på evaluering af de hardwarekomponenter og -platforme, hvorunder der kan ydes modstand mod angribere med en stor angrebskapacitet i overensstemmelse med gennemførelsesforordning (EU) 2015/1502, og præcisere evalueringsaktiviteterne for at bekræfte disse antagelser som omhandlet i bilag IV

([10]) Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333 af 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

c) de procedurer, der understøtter levering og drift af en tegnebogsløsning, herunder proceduren for onboarding af brugere omhandlet i artikel 5a i forordning (EU) nr. 910/2014, der mindst omfatter tilmelding, håndtering og organisering af elektroniske identifikationsmidler i henhold til afsnit 2.1, 2.2 og 2.4 i bilag I i Kommissionens gennemførelsesforordning (EU) 2015/1502.

4. Nationale certificeringsordninger skal indeholde en beskrivelse af tegnebogsløsningernes specifikke struktur og den elektroniske identifikationsordning, som de leveres under. Hvis nationale certificeringsordninger dækker mere end én specifik struktur, skal de omfatte en profil for hver specifik struktur.

5. For hver profil skal de nationale certificeringsordninger mindst indeholde følgende:

a) den specifikke struktur for tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under

b) de sikkerhedskontroller, der er knyttet til sikringsniveauer fastsat i artikel 8 i forordning (EU) nr. 910/2014

c) en evalueringsplan udarbejdet i overensstemmelse med afsnit 7.4.1 i EN ISO/IEC 17065:2012

d) de sikkerhedskrav, der er nødvendige for at håndtere de cybersikkerhedsrisici og -trusler, der er opført i risikoregistret i bilag I til denne forordning, op til det krævede sikringsniveau, og for, hvor det er relevant, at opfylde de mål, der er fastsat i artikel 51 i forordning (EU) 2019/881

e) en tilknytning af de kontroller, der er omhandlet i nærværende stykkes litra (b), til komponenter i strukturen

f) en beskrivelse af, hvordan de sikkerhedskontroller, den tilknytning, de sikkerhedskrav og den evalueringsplan, der er omhandlet i litra (b)-(c), gør det muligt for udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, på passende vis at håndtere de cybersikkerhedsrisici og -trusler, der er identificeret i det risikoregister, der er omhandlet i litra (d)), op til det krævede sikringsniveau baseret på en risikovurdering, der har til formål at finjustere og supplere de risici og trusler, der er opført i risikoregistret, med risici og trusler, der er specifikke for den tekniske struktur.

6. Den evalueringsplan, der er omhandlet i stk. 5, litra (c), skal indeholde en liste over de evalueringsaktiviteter, der skal indgå i evalueringen af tegnebogsløsninger og af den elektroniske identifikationsordning, som de leveres under.

7. Den evalueringsaktivitet, der er omhandlet i stk. 6, skal kræve, at udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, fremlægger oplysninger, der opfylder kravene i bilag II.

Artikel 4

Generelle krav

1. Nationale certificeringsordninger skal omfatte funktions-, cybersikkerheds- og databeskyttelseskrav ved at anvende følgende certificeringsordninger, når de er tilgængelige og relevante:

a) europæiske cybersikkerhedscertificeringsordninger, der er oprettet i henhold til forordning (EU) 2019/881, herunder EUCC

b) nationale cybersikkerhedscertificeringsordninger, der er omfattet af EUCC, i henhold til artikel 49 i gennemførelsesforordning (EU) 2024/482.

2. Nationale certificeringsordninger kan desuden, når oplysningerne foreligger og er relevante, henvise til:

a) andre relevante nationale certificeringsordninger

b) internationale, europæiske og nationale standarder

c) tekniske specifikationer, der opfylder kravene i bilag II til Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 ([11]).

3. Nationale certificeringsordninger skal:

a) specificere de elementer, der er anført i afsnit 6.5 i EN ISO/IEC 17067:2013

b) gennemføres som en type 6-ordning i overensstemmelse med afsnit 5.3.8 i EN ISO/IEC 17067:2013.

4. Nationale certificeringsordninger skal opfylde følgende krav:

a) kun udbydere omhandlet i artikel 5a, stk. 2, i forordning (EU) nr. 910/2014 er berettiget til at få udstedt attester i henhold til de nationale certificeringsordninger

b) kun tillidsmærket anvendes som overensstemmelsesmærke

c) udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, henviser til forordning (EU) nr. 910/2014 og denne forordning, når de henviser til ordningen

d) udbydere af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, supplerer ordningens risikovurdering, jf. artikel 3, stk. 5, litra f), for at identificere risici og trusler, der er specifikke for deres gennemførelse, og foreslå passende behandlingsforanstaltninger for alle relevante risici og trusler

e) ansvar og retsmidler fastlægges og indeholder henvisninger til gældende national lovgivning, som definerer ansvar og eventuelle retsmidler, hvis certificering i henhold til ordningen anvendes svigagtigt.

5. Den vurdering, der er omhandlet i stk. 4, litra (d), deles med certificeringsorganet med henblik på evaluering.

Artikel 5

Håndtering af hændelser og sårbarheder

1. Nationale certificeringsordninger skal indeholde krav til håndtering af hændelser og sårbarheder i overensstemmelse med stk. 2-9.

2. Indehaveren af en overensstemmelsesattest for en tegnebogsløsning og den elektroniske identifikationsordning, som den leveres under, underretter uden unødig forsinkelse sit certificeringsorgan om ethvert tilfælde af brud vedrørende eller kompromittering af tegnebogsløsningen eller den elektroniske identifikationsordning, som den leveres under, der sandsynligvis vil påvirke dens overensstemmelse med kravene i de nationale certificeringsordninger.

3. Indehaveren af en overensstemmelsesattest udarbejder, vedligeholder og anvender en politik og procedurer for sårbarhedsstyring under hensyntagen til de procedurer, der er fastsat i eksisterende europæiske og internationale standarder, herunder EN ISO/IEC 30111:2019.

4. Indehaveren af en overensstemmelsesattest underretter det udstedende certificeringsorgan om sårbarheder og ændringer, der påvirker tegnebogsløsningen, på grundlag af fastlagte kriterier for virkningen af disse sårbarheder og ændringer.

5. Indehaveren af en overensstemmelsesattest udarbejder en rapport om sårbarhedskonsekvensanalysen for enhver sårbarhed, der påvirker softwarekomponenterne i tegnebogsløsningen. Rapporten skal indeholde følgende oplysninger:

a) sårbarhedens indvirkning på den certificerede tegnebogsløsning

b) mulige risici i forbindelse med et angrebs nærhed eller sandsynlighed

([11]) Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EØS-relevant tekst) (EUT L 316 af 14.11.2012, s. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

c) om sårbarheden kan afhjælpes ved hjælp af tilgængelige midler

d) mulige måder at afhjælpe sårbarheden på, hvis sårbarheden kan afhjælpes ved hjælp af tilgængelige midler.

6. Hvis der kræves anmeldelse i henhold til stk. 4, fremsender indehaveren af overensstemmelsesattestten uden ugrundet ophold den rapport om sårbarhedskonsekvensanalysen, der er omhandlet i stk. 5, til certificeringsorganet.

7. Indehaveren af en overensstemmelsesattest udarbejder, vedligeholder og anvender en politik for sårbarhedsstyring, som opfylder kravene i bilag I til forordningen om cyberrobusthed ([12]).

8. Nationale certificeringsordninger fastsætter krav om offentliggørelse af sårbarheder, der gælder for certificeringsorganer.

9. Indehaveren af en overensstemmelsesattest offentliggør og registrerer enhver offentligt kendt og afhjulpet sårbarhed i tegnebogsløsningen eller i et af de onlineregistre, der er omhandlet i bilag V.

Artikel 6

Vedligeholdelse af nationale certificeringsordninger

1. Nationale certificeringsordninger skal indeholde en procedure for regelmæssig revision af den måde, de fungerer på. Denne procedure har til formål at bekræfte deres tilstrækkelighed og identificere aspekter, der kræver forbedringer, under hensyntagen til feedback fra interessenter.

2. Nationale certificeringsordninger skal indeholde bestemmelser om vedligeholdelsen heraf. Denne procedure skal mindst omfatte følgende krav:

a) regler for styringen af de nationale certificeringsordningers definition og krav

b) fastsættelse af tidsfrister for udstedelse af attester efter vedtagelsen af ajourførte udgaver af de nationale certificeringsordninger for både nye overensstemmelsesattester og tidligere udstedte attester

c) en regelmæssig revision af de nationale certificeringsordninger for at sikre, at de nationale certificeringsordningers krav anvendes på en ensartet måde, idet der tages hensyn til mindst følgende aspekter:

   — anmodninger til den ordningsansvarlige om præciseringer vedrørende kravene i den nationale certificeringsordning

   — feedback fra interessenter og andre interesserede parter

   — den nationale certificeringsordningsansvarliges lydhørhed over for anmodninger om oplysninger

d) regler for overvågning af referencedokumenter og procedurer for udvikling af referenceversioner af nationale certificeringsordninger, herunder som minimum overgangsperioder

e) en procedure for at sikre, at de seneste cybersikkerhedsrisici og -trusler, der er opført i risikoregistret i bilag I til denne forordning, er omfattet

f) en procedure for styring af andre ændringer i de nationale certificeringsordninger.

([12]) Europa-Parlamentets og Rådets forordning (EU) 2024/2847 af 23. oktober 2024 om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) nr. 168/2013 og (EU) 2019/1020 og direktiv (EU) 2020/1828 (forordningen om cyberrobusthed) (EUT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

3. Nationale certificeringsordninger skal indeholde krav til udførelse af evalueringer af aktuelt certificerede produkter inden for en vis periode efter revisionen af ordningen eller efter offentliggørelsen af nye specifikationer eller standarder eller nye versioner heraf, som tegnebogsløsningerne og den elektroniske identifikationsordning, som de leveres under, skal overholde.

KAPITEL III

KRAV VEDRØRENDE ORDNINGSANSVARLIGE

Artikel 7

Generelle krav

1. De ordningsansvarlige udvikler og vedligeholder nationale certificeringsordninger og styrer deres drift.

2. De ordningsansvarlige kan give alle eller en del af deres opgaver i underentreprise til en tredjepart. Ved underentreprise til en privat part fastlægger de ordningsansvarlige alle parters pligter og ansvar ved kontrakt. De ordningsansvarlige forbliver ansvarlige for alle aktiviteter, der udføres af deres underleverandører.

3. En ordningsansvarlig udfører sine relevante overvågningsaktiviteter på grundlag af mindst følgende oplysninger:

a) oplysninger fra certificeringsorganer, nationale akkrediteringsorganer og relevante markedsovervågningsmyndigheder

b) oplysninger fra sine egne eller en anden myndigheds revisioner og undersøgelser

c) klager modtaget i henhold til artikel 15.

4. De ordningsansvarlige underretter samarbejdsgruppen om revisioner af de nationale certificeringsordninger. Anmeldelsen skal indeholde tilstrækkelige oplysninger til, at samarbejdsgruppen kan fremsætte henstillinger til de ordningsansvarlige og udtalelser om de ajourførte nationale certificeringsordninger.

KAPITEL IV

KRAV VEDRØRENDE UDBYDERE AF TEGNEBOGSLØSNINGER OG DEN ELEKTRONISKE IDENTIFIKATIONSORDNING, SOM DE LEVERES UNDER

Artikel 8

Generelle krav

1. Nationale certificeringsordninger skal indeholde cybersikkerhedskrav baseret på en risikovurdering af hver specifik understøttet struktur. Disse cybersikkerhedskrav har til formål at behandle de identificerede cybersikkerhedsrisici og -trusler som fastsat i risikoregistret i bilag I.

2. I overensstemmelse med artikel 5a, stk. 23, i forordning (EU) nr. 910/2014 skal nationale certificeringsordninger kræve, at tegnebogsløsninger og de elektroniske identifikationsordninger, som de leveres under, er modstandsdygtige over for angribere med en stor angrebskapacitet for sikringsniveauet »høj« som omhandlet i gennemførelsesforordning (EU) 2015/1502.

3. Nationale certificeringsordninger skal fastsætte sikkerhedskriterier, som skal omfatte følgende krav:

a) Forordningen om cyberrobusthed, hvor det er relevant, eller krav, der opfylder de sikkerhedsmål, der er fastsat i artikel 51 i forordning (EU) 2019/881

b) fastlæggelse og gennemførelse af politikker og procedurer vedrørende risikostyring i forbindelse med driften af en tegnebogsløsning, herunder identifikation og vurdering af risici og afbødning af de identificerede risici

c) fastlæggelse og gennemførelse af politikker og procedurer vedrørende styring af ændringer og sårbarheder i overensstemmelse med denne forordnings artikel 5

d) fastlæggelse og gennemførelse af politikker og procedurer for forvaltning af menneskelige ressourcer, herunder krav til ekspertise, pålidelighed, erfaring, sikkerhedsuddannelse og kvalifikationer for personale, der er involveret i udviklingen eller driften af tegnebogsløsningen

e) krav vedrørende tegnebogsløsningens driftsmiljø, herunder i form af antagelser om sikkerheden af de anordninger og platforme, som tegnebogsløsningens softwarekomponenter kører på, herunder sikre kryptografiske tegnebogsanordninger og, hvor det er relevant, krav til overensstemmelsesvurdering for at bekræfte, at disse antagelser verificeres på de relevante anordninger og platforme

f) for hver antagelse, der ikke understøttes af en overensstemmelsesattest eller andre acceptable oplysninger om sikring, en beskrivelse af den mekanisme, som tegnebogsudbyderen anvender til at håndhæve antagelsen, samt en begrundelse for, at mekanismen er tilstrækkelig til at sikre, at antagelsen verificeres

g) fastlæggelse og gennemførelse af foranstaltninger til at sikre, at der anvendes en aktuelt certificeret version af tegnebogsløsningen.

4. Nationale certificeringsordninger skal indeholde funktionelle krav vedrørende opdateringsmekanismer for hver softwarekomponent i tegnebogsløsningerne og den elektroniske identifikationsordning, som de leveres under, til de operationer, der er opført i bilag III.

5. Nationale certificeringsordninger skal kræve, at ansøgeren om certificering fremlægger eller på anden måde tilgængeliggør følgende oplysninger og dokumentation for certificeringsorganet:

a) dokumentation vedrørende de oplysninger, der er omhandlet i bilag IV, punkt 1, herunder om nødvendigt nærmere oplysninger om tegnebogsløsningen og dens kildekode, herunder:

— *oplysninger om struktur:* for hver komponent i tegnebogsløsningen (herunder produkt-, procedure- og tjenestekomponenter) en beskrivelse af dens væsentlige sikkerhedsegenskaber, herunder dens eksterne afhængigheder

— *kontroller og sikringsniveauer:* for hver sikkerhedskontrol i tegnebogsløsningen en beskrivelse af kontrollen og det krævede sikringsniveau på grundlag af bilaget til gennemførelsesforordning (EU) 2015/1502, som fastsætter en række tekniske specifikationer og procedurer, der finder anvendelse på de forskellige kontroller, der gennemføres ved hjælp af de elektroniske identifikationsmidler

— *tilknytning af kontroller til strukturkomponenter:* en beskrivelse af, hvordan kontrollerne i tegnebogen gennemføres ved hjælp af tegnebogsløsningens forskellige komponenter, baseret på en begrundelse for, at et givet sikringsniveau er påkrævet, og hvordan kontrollen gennemføres med alle de krævede sikkerhedsaspekter på det relevante niveau

— *begrundelse for risikodækningen:* en begrundelse for:

  — tilknytningen af kontroller til komponenter

  — den foreslåede evalueringsplans egnethed til på passende vis at dække alle kontroller

  — den dækning, der sikres med kontrollen af cybersikkerhedsrisici og -trusler, der er identificeret i risikoregistret, suppleret med kontrol af risici og trusler, der er specifikke for implementeringen, på det relevante sikringsniveau.

b) de oplysninger, der er omhandlet i bilag V

c) en fuldstændig liste over de overensstemmelsesattester og andre oplysninger om sikring, der er anvendt som dokumentation under evalueringsaktiviteterne

d) alle andre oplysninger, der er relevante for evalueringsaktiviteterne.

KAPITEL V

KRAV VEDRØRENDE CERTIFICERINGSORGANER

Artikel 9

Generelle krav

1. Certificeringsorganer akkrediteres af nationale akkrediteringsorganer, der er udpeget i henhold til Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 ([13]) i overensstemmelse med EN ISO/IEC 17065:2012, forudsat at de opfylder kravene i de nationale certificeringsordninger i overensstemmelse med stk. 2.

2. Med henblik på akkreditering skal certificeringsorganerne opfylde alle følgende kompetencekrav:

a) detaljeret og teknisk viden om de relevante strukturer i en tegnebogsløsning og om den elektroniske identifikationsordning, som den leveres under, samt om de trusler og risici, der er relevante for disse strukturer

b) kendskab til tilgængelige sikkerhedsløsninger og deres egenskaber i henhold til bilaget til gennemførelsesforordning (EU) 2015/1502

c) kendskab til de aktiviteter, som udføres i henhold til de overensstemmelsesattester, der gælder for komponenter i tegnebogsløsningen og den elektroniske identifikationsordning, som en leveres under, som udpeget som genstand for certificering

d) detaljeret kendskab til den gældende nationale certificeringsordning, der er oprettet i overensstemmelse med kapitel II.

3. Certificeringsorganerne udfører deres overvågningsaktiviteter navnlig på grundlag af især følgende oplysninger:

a) oplysninger fra nationale akkrediteringsorganer og relevante markedsovervågningsmyndigheder

b) oplysninger fra deres egne eller en anden myndigheds revisioner og undersøgelser

c) klager modtaget i henhold til artikel 15.

Artikel 10

Underentrepriser

Certificeringsorganerne kan give evalueringsaktiviteterne omhandlet i artikel 13 i underentreprise til tredjeparter. Hvis evalueringsaktiviteter gives i underentreprise, skal de nationale certificeringsordninger fastsætte følgende:

(1) alle certificeringsorganets underleverandører, der udfører evalueringsaktiviteter, opfylder, hvor det er relevant og hensigtsmæssigt for de aktiviteter, der skal udføres, kravene i harmoniserede standarder som f.eks. EN ISO/IEC 17025:2017 for prøvning, EN ISO/IEC 17020:2012 for inspektion, EN ISO/IEC 17021-1:2015 for audit og EN ISO/IEC 17029:2019 for validering og verifikation

(2) certificeringsorganerne påtager sig ansvaret for alle evalueringsaktiviteter, der outsources til andre organer, og dokumenterer, at de har truffet passende foranstaltninger under deres akkreditering, herunder ved at basere sig på deres underleverandørers egen akkreditering, hvis det er relevant

(3) det omfang, hvori der skal indhentes forudgående samtykke til outsourcing fra de ordningsansvarlige eller den kunde, hvis tegnebogsløsning certificeres i henhold til certificeringsordningen.

([13]) Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 af 9. juli 2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af Rådets forordning (EØF) nr. 339/93 (EUT L 218 af 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Artikel 11

Anmeldelse til tilsynsorganet

Certificeringsorganerne underretter det tilsynsorgan, der er omhandlet i artikel 46a, stk. 1, i forordning (EU) nr. 910/2014, om udstedelse, suspension og annullering af overensstemmelsesattester for tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under.

Artikel 12

Håndtering af hændelser og sårbarheder

1. Certificeringsorganerne suspenderer uden unødig forsinkelse overensstemmelsesattesten for tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, når de har bekræftet, at det anmeldte sikkerhedsbrud eller den anmeldte kompromittering påvirker overensstemmelsen med kravene i de nationale certificeringsordninger, tegnebogsløsningen eller den elektroniske identifikationsordning, som den leveres under.

2. Certificeringsorganerne annullerer den overensstemmelsesattest, der er blevet suspenderet som følge af et sikkerhedsbrud eller en kompromittering, der ikke er blevet afhjulpet rettidigt.

3. Certificeringsorganerne annullerer overensstemmelsesattester, hvis en konstateret sårbarhed ikke er blevet afhjulpet rettidigt i forhold til dens alvor og potentielle indvirkning, jf. artikel 5c, stk. 4, og artikel 5e, stk. 2, i forordning (EU) nr. 910/2014.

KAPITEL VI

OVERENSSTEMMELSESVURDERINGSAKTIVITETER

Artikel 13

Evalueringsaktiviteter

1. Nationale certificeringsordninger skal indeholde metoder og procedurer, som overensstemmelsesvurderingsorganerne skal anvende, når de udfører deres evalueringsaktiviteter i overensstemmelse med EN ISO/IEC 17065:2012, som skal omfatte mindst følgende aspekter:

a) metoderne og procedurerne til gennemførelse af evalueringsaktiviteter, herunder dem, der vedrører den sikre kryptografiske tegnebogsanordning omhandlet i bilag IV

b) revisionen af implementeringen af tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under, på grundlag af risikoregistret omhandlet i bilag I, om nødvendigt suppleret med implementeringsspecifikke risici

c) funktionelle testaktiviteter, der, når de er tilgængelige og hensigtsmæssige, er baseret på testpakker, der er defineret i henhold til tekniske specifikationer eller standarder

d) vurdering af vedligeholdelsesprocedurernes eksistens og egnethed, herunder som minimum versionsstyring, opdateringsstyring og sårbarhedsstyring

e) vurdering af vedligeholdelsesprocedurernes driftseffektivitet, herunder som minimum versionsstyring, opdateringsstyring og sårbarhedsstyring

f) afhængighedsanalyse leveret af tegnebogsudbyderen, herunder en metode til vurdering af, hvorvidt oplysninger om sikring kan accepteres, som skal omfatte de elementer, der er fastsat i bilag VI

g) sårbarhedsvurdering på det relevante niveau, herunder:

— en gennemgang af tegnebogsløsningens design og dens kildekode, hvis det er relevant

— test af tegnebogsløsningens modstandsdygtighed over for angribere med en stor angrebskapacitet for sikringsniveauet »høj« i henhold til afsnit 2.2.1 i bilaget til gennemførelsesforordning (EU) 2015/1502

h) vurdering af udviklingen i trusselsmiljøet og dets indvirkning på tegnebogsløsningens dækning af risiciene for at fastslå, hvilke evalueringsaktiviteter der er nødvendige for tegnebogsløsningens forskellige komponenter.

2. Nationale certificeringsordninger skal indeholde en evaluering for at fastslå, om implementeringen af tegnebogsløsninger og den elektroniske identifikationsordning, som disse tegnebogsløsninger leveres under, stemmer overens med den struktur, der er fastsat i artikel 3, stk. 5, litra a), samt en evaluering for at fastslå, om den foreslåede evalueringsplan sammen med implementeringen stemmer overens med den evalueringsplan, der er omhandlet i artikel 3, stk. 5, litra c).

3. Nationale certificeringsordninger skal fastsætte regler for stikprøveudtagning for at undgå gentagelse af identiske evalueringsaktiviteter og for at fokusere på aktiviteter, der er specifikke for en given variant. Med disse stikprøveregler sikres det, at funktions- og sikkerhedstest kan udføres på en prøve af varianter af en målkomponent i en tegnebogsløsning og den elektroniske identifikationsordning, som den leveres under, og på en prøve af målanordninger. Nationale certificeringsordninger skal kræve, at alle certificeringsorganer begrunder deres anvendelse af stikprøver.

4. Nationale certificeringsordninger skal kræve, at certificeringsorganet evaluerer den sikre kryptografiske tegnebogsapplikation på grundlag af de metoder og procedurer, der er fastsat i bilag IV.

Artikel 14

Certificeringsaktiviteter

1. Nationale certificeringsordninger skal fastsætte en attesteringsaktivitet med henblik på udstedelse af en overensstemmelsesattest i overensstemmelse med afsnit V, litra a), i EN ISO/IEC 17067:2013, tabel 1, der omfatter følgende aspekter:

a) indholdet af overensstemmelsesattesten, jf. bilag VII

b) hvordan resultaterne af evalueringen skal rapporteres i den offentlige certificeringsrapport, herunder mindst et resumé af den foreløbige revisions- og valideringsplan, jf. bilag VIII

c) indholdet af de indberettede evalueringsresultater i certificeringsvurderingsrapporten, herunder de elementer, der er fastsat i bilag VIII.

2. Certificeringsvurderingsrapporten kan stilles til rådighed for samarbejdsgruppen og Kommissionen.

Artikel 15

Klageadgang

Nationale certificeringsordninger skal indeholde procedurer eller henvisninger til gældende national lovgivning, som definerer mekanismen til effektivt at indgive og behandle klager i forbindelse med gennemførelsen af certificeringsordningen eller udstedelsen af en overensstemmelsesattest. Disse procedurer skal omfatte underretning af klageren om forløbet af proceduren og om den trufne afgørelse samt underretning af klageren om retten til et effektivt retsmiddel. Nationale certificeringsordninger skal kræve, at alle klager, der ikke er blevet løst eller ikke kan løses af certificeringsorganet, sendes til den ordningsansvarlige med henblik på vurdering og løsning.

Artikel 16

Overvågningsaktiviteter

1. Nationale certificeringsordninger skal kræve, at certificeringsorganerne gennemfører overvågningsaktiviteter, som omfatter overvågningsevaluering af procedurer kombineret med stikprøver eller inspektioner.

2. Nationale certificeringsordninger skal omfatte krav om, at de ordningsansvarlige skal overvåge, at certificeringsorganerne overholder deres forpligtelser i henhold til forordning (EU) nr. 910/2014 og i henhold til nationale certificeringsordninger, hvis det er relevant.

3. Nationale certificeringsordninger skal omfatte krav om, at certificeringsorganerne skal overvåge følgende:

a) indehavere af en overensstemmelsesattest, der er udstedt i henhold til nationale certificeringsordninger, overholder deres forpligtelser vedrørende certificering i henhold til forordning (EU) nr. 910/2014 og i henhold til nationale certificeringsordninger

b) den certificerede tegnebogsløsning overholder de krav, der er fastsat i de nationale certificeringsordninger.

Artikel 17

Konsekvenser i tilfælde af manglende overholdelse

Nationale certificeringsordninger skal redegøre for konsekvenserne af manglende overensstemmelse, der er konstateret for en certificeret tegnebogsløsning og for den elektroniske identifikationsordning, som den leveres under, med de krav, der er fastsat i denne forordning. De potentielle konsekvenser skal omfatte følgende aspekter:

(1) certificeringsorganets forpligtelse til at underrette indehaveren af en overensstemmelsesattest og anmode indehaveren af en overensstemmelsesattest om at træffe afhjælpende foranstaltninger

(2) certificeringsorganets forpligtelse til at underrette andre relevante markedsovervågningsmyndigheder, hvis den manglende overensstemmelse vedrører relevant EU-lovgivning

(3) betingelserne for, at indehaveren af en overensstemmelsesattest kan træffe afhjælpende foranstaltninger

(4) betingelserne for certificeringsorganets suspension af en overensstemmelsesattest og for genaktivering af overensstemmelsesattesten, efter at den manglende overensstemmelse er blevet afhjulpet

(5) betingelserne for certificeringsorganets annullering af en overensstemmelsesattest

(6) konsekvenserne af certificeringsorganets manglende overholdelse af kravene i den nationale certificeringsordning.

KAPITEL VII

LIVSCYKLUS FOR CERTIFICERING

Artikel 18

Livscyklus for certificering

1. Gyldigheden af udstedte overensstemmelsesattester under nationale certificeringsordninger skal være omfattet af certificeringsorganets regelmæssige evalueringsaktiviteter udført i overensstemmelse med kravene i bilag IX.

2. Nationale certificeringsordninger skal indeholde en procedure for fornyet certificering af tegnebogsløsninger og den elektroniske identifikationsordning, som de leveres under, efter anmodning fra indehaveren af en overensstemmelsesattest inden udløbet af den oprindelige overensstemmelsesattest. Denne procedure for fornyet certificering skal omfatte en fuldstændig evaluering af tegnebogsløsningen og af den elektroniske identifikationsordning, som den leveres under, herunder en sårbarhedsvurdering, efter principperne i bilag IX.

3. Nationale certificeringsordninger skal indeholde en procedure for styring af ændringer i en certificeret tegnebogsløsning og den elektroniske identifikationsordning, som den leveres under. Denne procedure skal omfatte regler med henblik på at fastlægge, om en ændring skal være omfattet af en særlig evaluering, jf. stk. 4, eller af verifikationen af vedligeholdelsesprocedurernes driftseffektivitet, jf. bilag IV.

4. Nationale certificeringsordninger skal indeholde en procedure for særlige evalueringer i overensstemmelse med EN ISO/IEC 17065:2012. Denne procedure for særlige evalueringer skal omfatte et udvalg af aktiviteter, der skal udføres for at løse det specifikke problem, der udløste den særlige evaluering.

5. Nationale certificeringsordninger skal fastsætte regler for annullering af en overensstemmelsesattest.

KAPITEL VIII

REGISTRERING OG BESKYTTELSE AF OPLYSNINGER

Artikel 19

Opbevaring af optegnelser

1. Nationale certificeringsordninger skal indeholde krav om, at certificeringsorganerne skal have et registreringssystem for alle relevante oplysninger, der fremkommer i forbindelse med de overensstemmelsesvurderingsaktiviteter som de udfører, herunder data udstedt og modtaget af udbydere af tegnebogsløsninger og de elektroniske identifikationsordninger, som de leveres under. Optegnelserne af sådanne oplysninger skal opbevares på en sikker måde. Optegnelserne kan opbevares elektronisk og skal forblive tilgængelige, så længe det kræves i henhold til EU-retten eller national ret, og i mindst fem år efter annulleringen eller udløbet af den relevante overensstemmelsesattest.

2. Nationale certificeringsordninger skal kræve, at indehaveren af en overensstemmelsesattest opbevarer følgende oplysninger sikkert med henblik på denne forordning og i mindst fem år efter annulleringen eller udløbet af den relevante overensstemmelsesattest:

a) optegnelser af de oplysninger, der er givet til certificeringsorganet eller dets underleverandører under certificeringsproceduren

b) prøver af hardwarekomponenter, der er omfattet af certificeringen for tegnebogsløsningen.

3. Nationale certificeringsordninger skal kræve, at indehaveren af en overensstemmelsesattest efter anmodning stiller de oplysninger, der er omhandlet i stk. 1, til rådighed for certificeringsorganet eller det tilsynsorgan, der er omhandlet i artikel 46a, stk. 1, i forordning (EU) nr. 910/2014.

Artikel 20

Beskyttelse af oplysninger

I henhold til nationale certificeringsordninger er alle personer eller organisationer, der har fået adgang til oplysninger i forbindelse med udførelsen af aktiviteter under den nationale certificeringsordning, forpligtet til at sikre sikkerheden og beskyttelsen af forretningshemmeligheder og andre fortrolige oplysninger, samt beskytte intellektuelle ejendomsrettigheder og træffe de nødvendige og passende tekniske og organisatoriske foranstaltninger for at sikre denne fortrolighed.

KAPITEL IX

AFSLUTTENDE BESTEMMELSER

Artikel 21

Overgang til en europæisk cybersikkerhedscertificeringsordning

Denne forordning revideres ved vedtagelsen af den første europæiske cybersikkerhedscertificeringsordning for tegnebogsløsninger og de elektroniske identifikationsordninger, som de leveres under, med det formål at tage hensyn til bidraget fra en sådan europæisk cybersikkerhedscertificeringsordning til den overordnede certificering af tegnebogsløsninger og de elektroniske identifikationsordninger, som de leveres under.

Artikel 22

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

RISIKOREGISTER FOR EUROPÆISKE DIGITALE IDENTITETSTEGNEBØGER

Indledning

Risikoregistret beskriver de vigtigste sikkerheds- og privatlivsrisici og -trusler, der gælder for tegnebøger, og som skal håndteres korrekt i hver enkelt tegnebogsstruktur og -implementering. **Risiciene på højt niveau** (afsnit I) vedrører brugeres og tegnebogsmodtageres brug af tegnebøger, og de er forbundet med direkte trusler rettet mod tegnebøgers aktiver. Derudover identificeres enkelte **risici på systemniveau** (afsnit II) for tegnebøger, som typisk er resultatet af en kombination af trusler, der gælder for hele tegnebogssystemet.

Risikotype	Risiko-ID	Relaterede risikobetegnelser
Risici på højt niveau for tegnebøger	R1	Oprettelse eller brug af en eksisterende elektronisk identitet
	R2	Oprettelse eller brug af en falsk elektronisk identitet
	R3	Oprettelse eller brug af falske attributter
	R4	Identitetstyveri
	R5	Datatyveri
	R6	Videregivelse af data
	R7	Datamanipulation
	R8	Tab af data
	R9	Uautoriseret transaktion
	R10	Manipulation af transaktioner
	R11	Afvisning
	R12	Videregivelse af transaktionsdata
	R13	Tjenesteafbrydelse
	R14	Overvågning
Systemrelaterede risici	SR1	Omfattende overvågning
	SR2	Skade på omdømmet
	SR3	Manglende overholdelse af lovgivningen

Registret identificerer også **tekniske trusler** (afsnit III) målrettet mod implementeringen af tegnebogsløsningen. Disse trusler er relateret til risiciene på højt niveau, hvilket betyder, at de hver især kan anvendes til at udløse mange risici på højt niveau.

Trusselstype	Trussels-ID	Relaterede trusselsbetegnelser	Underkategorier af trusler
Teknisk trussel	TT1	Fysiske angreb	1.1. *Tyveri*
			1.2. *Informationslækage*
			1.3. *Manipulation*
	TT2	Fejl og fejlkonfigurationer	2.1. *Fejl i forbindelse med administration af et IT-system*
			2.2. *Fejl på applikationsniveau eller brugsfejl*
			2.3. *Udviklingstidsfejl og fejlkonfiguration af systemer*

Trusselstype	Trussels-ID	Relaterede trusselsbetegnelser	Underkategorier af trusler
	TT3	Brug af upålidelige ressourcer	3.1. *Fejlagtig brug eller konfiguration af tegnebogskomponenter*
	TT4	Fejl og udfald	4.1. *Fejl eller funktionssvigt i udstyr, anordninger eller systemer*
			4.2. *Tab af ressourcer*
			4.3. *Tab af støttetjenester*
	TT5	Ondsindede handlinger	5.1. *Opsnapning af oplysninger*
			5.2. *Phishing og spoofing*
			5.3. *Gentagelse af meddelelser*
			5.4. *Brute force-angreb*
			5.5. *Sårbarheder i software*
			5.6. *Angreb i forsyningskæden*
			5.7. *Malware*
			5.8. *Forudsigelse af tilfældige tal*

Endelig opregner registret **direkte trusler mod tegnebøgerne**, og hver enkelt er forbundet med et (ikkeudtømmende) udvalg af risici (afsnit IV).

AFSNIT I

Risici på højt niveau for tegnebøger

R1. Oprettelse eller brug af en eksisterende elektronisk identitet

Ved oprettelse eller brug af en eksisterende elektronisk identitet forstås oprettelse af en elektronisk identitet i en tegnebog, der eksisterer i den virkelige verden og er tildelt en anden bruger. I det væsentlige fører denne risiko til risikoen for identitetstyveri (R4) og uautoriserede transaktioner (R9).

R2. Oprettelse eller brug af en falsk elektronisk identitet

Ved oprettelse eller brug af en falsk elektronisk identitet forstås oprettelse af en elektronisk identitet i en tegnebog, der ikke eksisterer i den virkelige verden.

R3. Oprettelse eller brug af falske attributter

Ved oprettelse eller brug af falske attributter forstås oprettelse eller brug af attributter, der ikke kan valideres og udstedes af den påståede udbyder, og som man ikke kan stole på.

R4. Identitetstyveri

Ved identitetstyveri forstås uautoriseret erhvervelse eller tab af tegnebogsenhedens autentifikationsfaktorer, der gør det muligt at udgive sig for at være en person.

R5. Datatyveri

Ved datatyveri forstås uautoriseret udtrækning af data. Datatyveri er også forbundet med trusler, f.eks. opsnapning af data (uautoriseret indsamling af data under overførsel) og dekryptering af data (uautoriseret afkodning af krypterede data), som i nogle tilfælde sandsynligvis vil føre til videregivelse af data (R6).

R6. Videregivelse af data

Ved videregivelse af data forstås uautoriseret eksponering af personoplysninger, herunder særlige kategorier af personoplysninger. Svarer til risikoen for krænkelse af privatlivets fred, når den betragtes fra et privatlivssynspunkt snarere end et sikkerhedsmæssigt synspunkt.

R7. Datamanipulation

Ved datamanipulation forstås uautoriseret ændring af data.

R8. Tab af data

Ved datatab forstås den situation, hvor data, der er gemt i tegnebogen, går tabt ved misbrug eller ondsindet handling. Denne risiko er ofte en sekundær risiko i forhold til datamanipulation (R7) eller tjenesteafbrydelse (R13), hvor alle eller en del af dataene ikke kan gendannes.

R9. Uautoriseret transaktion

Ved uautoriserede transaktioner forstås driftsaktiviteter, der udføres uden tegnebogsbrugerens tilladelse eller viden. I mange tilfælde kan en uautoriseret transaktion føre til identitetstyveri (R4) eller videregivelse af data (R6). Uautoriserede transaktioner er også relateret til f.eks. misbrug af kryptografiske nøgler.

R10. Manipulation af transaktioner

Ved manipulation af transaktioner forstås uautoriseret ændring af foranstaltning. Manipulation af transaktioner er et angreb på integritet, og det er relateret til et brud på dataintegriteten.

R11. Afvisning

Ved afvisning forstås en situation, hvor en interessent kan nægte at udføre en handling eller at blive involveret i en transaktion, og andre interessenter ikke har tilstrækkelig dokumentation til at modsige dem.

R12. Videregivelse af transaktionsdata

Ved videregivelse af transaktionsdata forstås videregivelse af oplysninger om en transaktion mellem interessenter.

R13. Tjenesteafbrydelse

Ved tjenesteafbrydelse forstås en afbrydelse eller forringelse af tegnebogens normale drift. En særlig form for tjenesteafbrydelse er brugerlockout, der defineres som en situation, hvor en bruger ikke kan få adgang til sin konto eller tegnebog.

R14. Overvågning

Ved overvågning forstås uautoriseret sporing eller observation af en tegnebogsbrugers aktiviteter, kommunikation eller data. Overvågning er ofte relateret til inferens, som defineres som udledning af følsomme eller personlige oplysninger fra tilsyneladende uvigtige data.

AFSNIT II

Systemrelaterede risici

Disse risici er ikke opført på listen over trusler, da de normalt er en konsekvens af flere trusler, der gentages på en måde, der truer hele systemet.

SR1. Omfattende overvågning

Ved omfattende overvågning forstås sporing eller observation af mange brugeres aktiviteter gennem deres tegnebogs kommunikation eller data. Omfattende overvågning er ofte forbundet med overvågning (R14) og inferens på globalt plan, hvor oplysninger om mange brugere kombineres for at udlede følsomme eller personlige data om brugere eller for at identificere statistiske tendenser, der kan bruges til at designe yderligere angreb.

SR2. Skade på omdømmet

Ved skade på omdømmet forstås skade på en organisations eller et offentligt organs omdømme. Skader på omdømmet udspringer også af andre risici, når et brud eller en hændelse dækkes af medierne og stiller organisationen i et ugunstigt lys. Skade på omdømmet kan føre til yderligere risici som f.eks. tab af tillid som følge af brugerens rimelige tvivl og tab af økosystemet, når hele økosystemet kollapser.

SR3. Manglende overholdelse af lovgivningen

Ved manglende overholdelse af lovgivningen forstås en situation, hvor relevante love, forskrifter eller standarder ikke overholdes. I forbindelse med tegnebogen, hvor løsningens sikkerhed og beskyttelse af privatlivets fred er juridiske krav, vil alle trusler sandsynligvis føre til en form for manglende overholdelse af lovgivningen.

AFSNIT III

Tekniske trusler

De tekniske trusler er ikke alle forbundet med specifikke risici for tegnebøger, fordi mange af dem er midler, som kan bruges til at gennemføre angreb, der svarer til mange forskellige risici.

TT1. Fysiske angreb

1.1. *Tyveri*

Ved tyveri forstås tyveri af anordninger, der kan ændre tegnebogens korrekte funktion (hvis anordningen bliver stjålet, og tegnebogsenheden ikke er tilstrækkeligt beskyttet). Dette kan bidrage til mange risici, herunder identitetstyveri (R4), datatyveri (R5) og uautoriserede transaktioner (R9).

1.2. *Informationslækage*

Ved informationslækage forstås uautoriseret adgang, informationseksponering eller deling efter fysisk adgang til tegnebogen. Dette kan især bidrage til videregivelse af data (R6) og datatyveri (R5).

1.3. *Manipulation*

Ved manipulation forstås krænkelse af integriteten af en eller flere komponenter i tegnebogsenheden eller af de komponenter, som tegnebogsenheden anvender, f.eks. brugerenheden eller dens operativsystem. Dette kan især bidrage til datamanipulation (R7), datatab (R8) og manipulation af transaktioner (R10). Når manipulation er rettet mod softwarekomponenter, kan det bidrage til mange risici.

TT2. Fejl og fejlkonfigurationer

2.1. *Fejl i forbindelse med administration af et IT-system*

Ved fejl i forbindelse med administration af et IT-system forstås informationslækage, -deling eller -skade forårsaget af brugernes misbrug af IT-aktiver (manglende kendskab til applikationsfunktioner) eller ukorrekt konfiguration eller styring af IT-aktiver.

2.2. *Fejl på applikationsniveau eller brugsfejl*

Ved fejl på applikationsniveau eller brugsfejl forstås funktionsfejl i applikationen på grund af en fejl i selve applikationen eller en fejl begået af en af brugerne (tegnebogsbrugere og tegnebogsmodtagere).

2.3. *Udviklingstidsfejl og fejlkonfiguration af systemer*

Ved udviklingstidsfejl og fejlkonfiguration af systemer forstås funktionsfejl eller sårbarheder forårsaget af ukorrekt udviklede eller konfigurerede IT-aktiver eller forretningsprocesser (utilstrækkelige specifikationer for IT-produkter, utilstrækkelig anvendelighed, usikre grænseflader, ukorrekte politik- og procedurestrømme eller designfejl).

TT3. Brug af upålidelige ressourcer

Ved brug af upålidelige ressourcer forstås en aktivitet, der fører til utilsigtet skade på grund af dårligt definerede tillidsforhold, f.eks. tillid til en tredjepartsudbyder uden tilstrækkelig sikring.

3.1. *Fejlagtig brug eller konfiguration af tegnebogskomponenter*

Ved fejlagtig brug eller konfiguration af tegnebogskomponenter forstås utilsigtet skade på tegnebogskomponenter på grund af tegnebogsbrugeres eller utilstrækkeligt uddannede udvikleres fejlagtige brug eller konfiguration eller på grund af manglende tilpasning til ændringer i trusselsbilledet, herunder typisk brugen af sårbare tredjepartskomponenter eller runtime-platforme.

TT4. Fejl og udfald

4.1. *Fejl eller funktionssvigt i udstyr, anordninger eller systemer*

Ved fejl eller funktionssvigt i udstyr forstås utilsigtede skader på IT-aktiver som følge af fejl eller funktionssvigt i udstyr, herunder udbyderens infrastruktur og brugerenhederne.

4.2. *Tab af ressourcer*

Ved tab af ressourcer forstås en afbrydelse eller funktionsforstyrrelse som følge af manglende tilgængelighed af sådanne ressourcer, f.eks. vedligeholdelsesdele.

4.3. *Tab af støttetjenester*

Ved tab af supporttjenester forstås en afbrydelse eller funktionsforstyrrelse som følge af manglende adgang til de supporttjenester, der er nødvendige for en korrekt drift af systemet, herunder netværksforbindelse til udbyderens infrastruktur og brugerenheden.

TT5. Ondsindede handlinger

5.1. *Opsnapning af oplysninger*

Ved opsnapning af oplysninger forstås indsamling af oplysninger, der er utilstrækkeligt beskyttet under transmission, herunder man-in-the-middle-angreb.

5.2. *Phishing og spoofing*

Ved phishing forstås indsamling af oplysninger fra brugeren efter en vildledende interaktion, der ofte er forbundet med forfalskning af legitime kommunikationsmidler og websteder. Disse trusler er rettet mod brugeren og bidrager typisk til identitetstyveri (R4) og uautoriserede transaktioner (R9), ofte gennem datatyveri (R5) eller videregivelse af data (R6).

5.3. *Gentagelse af meddelelser*

Ved gentagelse af meddelelser forstås genanvendelse af tidligere opsnappede meddelelser til at udføre uautoriserede transaktioner, ofte på protokolniveau. Denne tekniske trussel bidrager hovedsagelig til uautoriserede transaktioner, som derefter kan føre til andre risici afhængigt af transaktionen.

5.4. *Brute force-angreb*

Ved brute force-angreb forstås et brud på sikkerheden, ofte fortrolighed, hvor der udføres et stort antal interaktioner, indtil svarene giver værdifulde oplysninger.

5.5. *Sårbarhed i software*

Truslen i forbindelse med softwaresårbarheder er et brud på sikkerheden, der omfatter udnyttelse af en softwaresårbarhed i tegnebogens komponenter eller i de software- og hardwarekomponenter, der anvendes til implementeringen af tegnebogen, herunder offentliggjorte sårbarheder og ikkeoffentliggjorte sårbarheder (dag 0).

5.6. *Angreb i forsyningskæden*

Ved et angreb i forsyningskæden forstås et brud på sikkerheden gennem angreb på udbyderen af tegnebogen eller dennes brugere for at muliggøre yderligere angreb på selve tegnebogen.

5.7. *Malware*

Ved malware forstås et brud på sikkerheden gennem ondsindede applikationer, der udfører uønskede og ulovlige handlinger på tegnebogen.

5.8. *Forudsigelse af tilfældige tal*

Ved forudsigelse af tilfældige tal forstås en handling, hvor brute force-angreb muliggøres gennem delvis eller fuldstændig forudsigelse af genererede tilfældige tal.

AFSNIT IV

Trusler mod tegnebøgerne

I dette sidste afsnit præsenteres et udvalg af typiske trusselsscenarier, der er specifikke for tegnebøgerne, som er knyttet til de vigtigste relaterede risici på højt niveau, som anført ovenfor. Denne liste angiver trusler, der skal dækkes, men den udgør ikke en udtømmende liste over trusler, som i høj grad afhænger af strukturen i den valgte tegnebogsløsning og af udviklingen i trusselsmiljøet. I risikovurderingen og de foreslåede foranstaltninger kan tegnebogsudbyderen desuden kun være ansvarlig for de komponenter, der er omfattet af certificering (*).

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel* (*)	Risikobetegnelse *Tilknyttede risici*
TR1	En angriber kan tilbagekalde pseudonymer uden gyldig grund.	Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR2	En angriber kan udstede fabrikerede elektroniske identiteter, der ikke eksisterer.	Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR3	En angriber kan begynde at udstede uautoriserede PID'er.	Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR4	En angriber kan få en administrator til at indtaste en forkert PID-udbyder på listen over PID-udbydere, der er tillid til.	Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR5	En angriber kan omgå tjenesten til fjernidentitetskontrol.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR6	En angriber kan omgå tjenesten til fysisk identitetskontrol.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR7	En angriber kan omgå de identitetskontroltjenester, der er knyttet til brugen af en ekstern (kvalificeret) attest.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR8	En angriber kan få adgang til en tegnebog, der ikke er bundet til en person.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR9	En angriber kan omgå tekniske og proceduremæssige kontroller og oprette forkerte PID'er.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR10	En angriber kan aktivere en ny tegnebog på en ugyldig WSCD.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2)
TR11	En angriber kan omgå identitetskontroltjenesten i forbindelse med brugen af eksisterende eID-midler.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR12	En angriber kan omgå PID-udbyderens kontrol af, at tegnebogen kontrolleres af brugeren, og få udstedt en PID i en kompromitteret tegnebog under angriberens kontrol.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR13	En angriber kan anbringe en gyldig PID i en ugyldig tegnebogsenhed.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR14	En PID-udbyder kan udstede fabrikerede identiteter, hvor identiteten er knyttet til en eksisterende person.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR15	En angriber kan forbinde en PID med den forkerte tegnebog, fordi PID-udbyderen ikke kan knytte PID'en til den korrekte tegnebog.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR16	En angriber kan få brugeren til at godkende aktiveringen af en ny tegnebogsenhed/-forekomst under angriberens kontrol, herunder med efterfølgende kontrol af attesteringer.	Oprettelse eller brug af en eksisterende elektronisk identitet (R1) / Oprettelse eller brug af en falsk elektronisk identitet (R2) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR17	En angriber kan udstede en PID fra en anden stat for at få adgang til data/digitale aktiver hos de borgere, angrebet er rettet mod.	Oprettelse eller anvendelse af en eksisterende elektronisk identitet (R1) / Identitetstyveri (R4) / Uautoriseret transaktion (R9)
TR18	En angriber kan omgå tekniske og proceduremæssige kontroller og oprette forkerte (Q)EAA'er.	Oprettelse eller brug af falske attributter (R3)
TR19	En angriber kan præsentere (Q)EAA'er, der ikke er gyldigt udstedt til vedkommende.	Oprettelse eller brug af falske attributter (R3)
TR20	En angriber kan angribe tegnebogens kryptografiske forbindelsesmekanisme mellem PID'en og en (Q)EAA, der ikke bør udstedes til vedkommende.	Oprettelse eller brug af falske attributter (R3)
TR21	En angriber kan bruge en (Q)EAA i en tegnebog, selv om (Q)EAA'ens fysiske modpart er udløbet eller er ugyldig.	Oprettelse eller brug af falske attributter (R3)
TR22	En angriber kan omgå (Q)EAA-udbyderens kontrol af, at tegnebogen kontrolleres af brugeren, og få udstedt en (Q)EAA i en kompromitteret tegnebog under angriberens kontrol.	Oprettelse eller brug af falske attributter (R3)
TR23	En angriber kan forfalske elektroniske attesteringer af attributter.	Oprettelse eller brug af falske attributter (R3)
TR24	En angriber kan indsætte falske elektroniske attesteringer af attributter i en tegnebog.	Oprettelse eller brug af falske attributter (R3)
TR25	Tegnebogen kan præsentere attributter til en tegnebogsmodtager uden brugerens godkendelse.	Videregivelse af data (R6)
TR26	PID, (Q)EAA'er eller pseudonymer kan præsenteres for en forkert tegnebogsmodtager.	Videregivelse af data (R6)
TR27	En angriber kan indlede en ondsindet fornyelse af EAA.	Videregivelse af data (R6)
TR28	En angriber kan få en bruger til uretmæssigt at godkende en anmodning om elektroniske attesteringer af attributter (phishing eller andet).	Videregivelse af data (R6)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR29	En angriber kan lække attributter fra tegnebogen og identificere tegnebogsbrugeren, hvor identifikation ikke er påkrævet/tilladt.	Videregivelse af data (R6)
TR30	En angriber kan omgå tekniske og proceduremæssige kontroller for at udtrække data.	Videregivelse af data (R6)
TR31	En anmodning kan lækkes til en angriber.	Videregivelse af data (R6)
TR32	En angriber kan få kendskab til den indlejrede offentliggørelsespolitik for attributter og præsentere attributter, der er indeholdt i den aktuelle anmodning fra tegnebogsenheder.	Videregivelse af data (R6)
TR33	En angriber kan udtrække logfiler eller dele af dem.	Videregivelse af data (R6)
TR34	En angriber kan vide, om en tegnebog er installeret på den samme anordning, som han bruger, eller på en anden, og få oplysninger om den.	Videregivelse af data (R6)
TR35	En angriber kan opnå en videnfaktor, der bruges til brugerautentificering til WSCA'en.	Videregivelse af data (R6)
TR36	Den elektroniske attestering af attributter om en person, der præsenteres i flere transaktioner med en tegnebogsmodtager eller på tværs af forskellige tegnebogsmodtagere, gør det utilsigtet muligt at knytte flere transaktioner til den relevante person.	Videregivelse af data (R6)
TR37	En liste over tilbagekaldte offentlige attesteringer/ tegnebogsmodtagere kan indeholde oplysninger om brugerens brug af deres attestering (f.eks. placering, IP-adresse osv.).	Videregivelse af data (R6)
TR38	Tegnebogsmodtagere, der ikke kan bevise brugerens samtykke til delte attributter, kan påvirke logfilernes integritet.	Videregivelse af data (R6)
TR39	En angriber kan ulovligt spore tegnebogsbrugere ved hjælp af unikke/sporbare identifikatorer.	Videregivelse af data (R6) / Overvågning (R14)
TR40	En tegnebogsmodtager, der består af flere enheder, som hver især har forskelligt omfang af, hvad de har lov til at anmode om/behandle, kan anmode om og behandle data, som de ikke har lovlige grunde til.	Videregivelse af data (R6) / Uautoriseret transaktion (R9)
TR41	En angriber kan undergrave integritets- og ægthedskontrollen af tegnebogen for PID'er, så den altid returnerer succes.	Datamanipulation (R7)
TR42	En angriber kan omgå eller undergrave tegnebogens kontrol, der verificerer integriteten og ægtheden af de anmodede attributter for altid at returnere succes.	Datamanipulation (R7)
TR43	En angriber kan omgå eller undergrave tegnebogens kontrol af, at alle anmodede attributter tilhører den samme bruger, for altid at returnere succes.	Datamanipulation (R7)
TR44	En angriber kan omgå eller undergrave tegnebogens kontrol, der bekræfter, at PID'en er gyldig og udstedt af en betroet PID-udbyder for altid at returnere succes.	Datamanipulation (R7)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR45	En angriber kan omgå eller undergrave tegnebogens kontrol, der verificerer, at en QEAA er gyldig og udstedt af en kvalificeret TSP, der er registreret til at udstede QEAA, for altid at returnere succes.	Datamanipulation (R7)
TR46	En angriber kan omgå eller undergrave tegnebogens kontrol, der kontrollerer, om PID'en er blevet tilbagekaldt af PID-udbyderen for altid at returnere succes.	Datamanipulation (R7)
TR47	En angriber kan omgå eller undergrave tegnebogens kontrol, der verificerer, om (Q)EAA er blevet tilbagekaldt af (Q)EAA-udbyderen, for altid at returnere succes.	Datamanipulation (R7)
TR48	En angriber kan ændre indholdet af sikkerhedskopierings- og gendannelsesdata, der udelukkende bør være under brugerens kontrol.	Datamanipulation (R7) / Datatab (R8)
TR49	En angriber kan ændre transaktionshistorikken for en given tegnebogsforekomst fra aktivitetslogfilerne.	Datamanipulation (R7) / Datatab (R8)
TR50	En angriber kan aflytte under forbindelsen fra tegnebogen til tegnebogsmodtagerne.	Datatyveri (R5) / Videregivelse af data (R6)
TR51	En angriber kan overbevise en bruger om at dele personoplysninger (dvs. PID, EAA-s, pseudonymer, elektroniske signaturer, logfiler og andre data) med angriberen eller med en tredjepart, som brugeren ikke havde til hensigt at gøre.	Datatyveri (R5) / Videregivelse af data (R6)
TR52	En angriber kan læse transaktionshistorikken for en given tegnebogsforekomst fra aktivitetslogfilerne.	Datatyveri (R5) / Videregivelse af data (R6)
TR53	En angriber kan eksportere eller udtrække kryptografisk nøglemateriale uden for WSCD'en.	Datatyveri (R5) / Videregivelse af data (R6) / Uautoriseret transaktion (R9)
TR54	En angriber kan læse indholdet af sikkerhedskopierings- og gendannelsesdata, der udelukkende bør være under brugerens kontrol.	Datatyveri (R5) / Videregivelse af data (R6)
TR55	En angriber kan omgå brugergodkendelsesmetoden for at bruge et pseudonym genereret af en tegnebogsenhed.	Identitetstyveri (R4)
TR56	En angriber kan foreslå en applikation, der efterligner en bestemt legitim tegnebog for brugerne.	Identitetstyveri (R4)
TR57	En angriber kan eksportere tegnebogsdata, herunder PID, (Q) EAA'er eller logfiler.	Identitetstyveri (R4)
TR58	En angriber kan eksportere kryptografisk bindende materiale.	Identitetstyveri (R4)
TR59	En angriber kan overtage identiteter via tegnebogens kryptografiske nøgler.	Identitetstyveri (R4)
TR60	En angriber kan duplikere en anden brugers personlige tegnebogsenhed på sin personlige anordning og bruge den.	Identitetstyveri (R4) / Oprettelse eller brug af en eksisterende elektronisk identitet (R1)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR61	Myndigheder i en anden stat kan bede brugeren om at vise og/eller dele alle tegnebogsdata i en nærhedsbaseret situation, f.eks. når vedkommende krydser grænsen til den pågældende stat.	Identitetstyveri (R4) / Overvågning (R14)
TR62	Brugere kan ikke overføre deres transaktionslogfiler efter svigt af en brugerenhed, hvilket resulterer i tab af sporbarhed af tidligere transaktioner på den nye tegnebog.	Afvisning (R11)
TR63	Brugere kan ikke gendanne deres transaktionslogfiler efter svigt af en brugerenhed, hvilket resulterer i tab af sporbarhed for den nye tegnebog.	Afvisning (R11)
TR64	Tegnebogsmodtagerne kan have vanskeligt ved at bevise, at de har givet deres samtykke til elektroniske signaturer på afstand.	Afvisning (R11)
TR65	En angriber kan oversvømme forbindelsen/forbindelserne med forespørgsler under forbindelsen til tegnebogsmodtagere.	Tjenesteafbrydelse (R13)
TR66	En angriber kan oversvømme en statusleveringstjeneste med forbindelser til tegnebogsmodtagere.	Tjenesteafbrydelse (R13)
TR67	En angriber kan få attributpræsentationen til at fremstå som anfægtet/afvist, selv om attributpræsentationen angiver, at den er gyldig.	Tjenesteafbrydelse (R13)
TR68	En angriber kan tilbagekalde en PID uden gyldig grund.	Tjenesteafbrydelse (R13)
TR69	En angriber kan tilbagekalde en PID uden brugerens samtykke.	Tjenesteafbrydelse (R13)
TR70	En angriber kan tilbagekalde en (Q)EAA uden gyldig grund.	Tjenesteafbrydelse (R13)
TR71	En angriber kan tilbagekalde en (Q)EAA uden brugerens samtykke.	Tjenesteafbrydelse (R13)
TR72	En angriber kan udløse flere identifikationsanmodninger, uden at de anerkendes som forsætlige ugyldige anmodninger.	Tjenesteafbrydelse (R13)
TR73	En angriber kan sende flere anmodninger uden opfølgende transaktion.	Tjenesteafbrydelse (R13)
TR74	En angriber kan tillade, at en tegnebogsmodtager anmoder om identifikation uden en matchende identifikation (svar) og fuld kontrol.	Tjenesteafbrydelse (R13)
TR75	En angriber kan sende et svar på en anmodning efter dens timeout eller lignende situationer, der fører til en tjenesteafbrydelse.	Tjenesteafbrydelse (R13)
TR76	En tegnebogsmodtager kan sende flere ugyldige anmodninger.	Tjenesteafbrydelse (R13)
TR77	En angriber kan sende flere ugyldige anmodninger til en tegnebogsudbyder.	Tjenesteafbrydelse (R13)
TR78	En angriber kan bevirke, at en medlemsstat ikke kan tilbagekalde en PID-udbyder, der ikke er tillid til, fra listen over betroede PID-udbydere.	Tjenesteafbrydelse (R13)
TR79	En angriber kan forhindre suspension eller tilbagekaldelse af en tegnebog.	Tjenesteafbrydelse (R13)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR80	En angriber kan blokere transaktioner fra tegnebogsmodtagere, brugere og/eller en PID-udbyder.	Tjenesteafbrydelse (R13)
TR81	En angriber kan deaktivere eller gøre en WSCD utilgængelig.	Tjenesteafbrydelse (R13)
TR82	En angriber kan bevirke, at en PID-udbyder ikke kan tilbagekalde eller suspendere PID'er.	Tjenesteafbrydelse (R13) / Uautoriseret transaktion (R9)
TR83	En tegnebogsmodtager kan udlede brugerens identitetsdata ud over de data, der deles med vedkommende.	Overvågning (R14)
TR84	En gruppe af samarbejdende tegnebogsmodtagere eller PID-udbydere kan udlede brugerens identitetsdata ud over de data, de kender.	Overvågning (R14)
TR85	En angriber kan spore en bruger ved hjælp af brugerens personidentifikationsdata, hvor identifikation af brugeren ikke er påkrævet.	Overvågning (R14)
TR86	En angriber kan kombinere en forfalsket præsentation af (Q) EAA-kombinationer.	Manipulation af transaktioner (R10)
TR87	En angriber kan fjernaktivere eller overtage tegnebogen på afstand (f.eks. en bankapp, der integrerer en anmodning om godkendelse eller attestering) uden brugerens udtrykkelige samtykke eller enekontrol i situationer, hvor brugeren er uvidende om (f.eks. sover) eller ikke kan se tegnebogsmodtageren.	Manipulation af transaktioner (R10)
TR88	Angribere kan foretage ændringer i en anmodnings metadata (tjenestenavn, brug osv.).	Manipulation af transaktioner (R10)
TR89	Angribere kan foretage ændringer i svaroplysninger (servicetilstand, nonce osv.).	Manipulation af transaktioner (R10)
TR90	Angribere kan foretage ændringer i en anmodnings attributoplysninger (»over asking« osv.).	Manipulation af transaktioner (R10)
TR91	En tegnebogsmodtager kan gentage elementer fra en tidligere session i en anden session.	Manipulation af transaktioner (R10)
TR92	En angriber kan erstatte eller ændre PID'en under overførslen fra PID-udbyderen til tegnebogsenheden.	Manipulation af transaktioner (R10)
TR93	En angriber kan erstatte eller ændre PID'en under overførslen fra tegnebogsenheden til tegnebogsmodtageren, når denne er online.	Manipulation af transaktioner (R10)
TR94	En angriber kan erstatte eller ændre PID'en under overførslen fra tegnebogsenheden til tegnebogsmodtageren, når denne er offline.	Manipulation af transaktioner (R10)
TR95	En angriber kan udstede en PID uden brugerens samtykke.	Uautoriseret transaktion (R9)
TR96	En angriber kan anvende tilbagekaldte eller ugyldige indlejrede offentliggørelsespolitikker, muligvis uden tegnebogsmodtagernes viden.	Uautoriseret transaktion (R9)
TR97	En angriber kan snyde tegnebogen til at verificere forkerte elektroniske signaturer.	Uautoriseret transaktion (R9)
TR98	En angriber kan bruge tegnebogen uden for brugerens kontrol.	Uautoriseret transaktion (R9)

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR99	En angriber kan overbevise en bruger om at autentificere og godkende transaktioner med en angriber eller en uautoriseret tredjepart.	Uautoriseret transaktion (R9)
TR100	En angriber kan få en bruger til at underskrive elektronisk uden at præsentere indholdet for brugeren eller efter at have præsenteret forkert indhold.	Uautoriseret transaktion (R9)
TR101	En angriber kan omgå adgangskontrollen på brugerens konto hos tegnebogsudbyderen.	Uautoriseret transaktion (R9)
TR102	En angriber kan udgive sig for at være tegnebogsmodtagere under tilslutningen til tegnebogsmodtagere.	Uautoriseret transaktion (R9) / Videregivelse af data (R6)
TR103	Brugeren bag forbindelsen mellem tegnebogsmodtageren og browseren kan være forskellig fra brugeren bag forbindelsen mellem tegnebogsmodtageren og tegnebogen.	Uautoriseret transaktion (R9) / Videregivelse af data (R6) / Identitetstyveri (R4)
TR104	En angriber kan overbevise brugeren om at tilbagekalde brugerens tegnebog uden grund.	Uautoriseret transaktion (R9) / Tjenesteafbrydelse (R13)
TR105	En angriber kan udføre man-in-the-middle-angreb.	Uautoriseret transaktion (R9) / Videregivelse af data (R6) / Overvågning (R14)
TR106	En angriber kan præsentere ugyldige eller tilbagekaldte attributter fra en tegnebog, der ikke regelmæssigt opretter forbindelse til netværket.	Indvirkning på forskellige risici
TR107	En angriber kan stjæle oplysninger fra en bruger ved at spoofe en tegnebog.	Indvirkning på forskellige risici
TR108	En angriber kan udgive sig for at være brugeren ved at gentage/efterligne en dataanmodning (f.eks. autentificering), som ser ud til at være gyldig.	Indvirkning på forskellige risici
TR109	En angriber kan gentage en indlejret offentliggørelsespolitik over for en bruger for at efterligne en godkendt anmodning.	Indvirkning på forskellige risici
TR110	En angriber kan udnytte manglen på oplysninger fra tegnebogsbrugere eller unødige forsinkelser efter et sikkerhedsbrud eller en kompromittering.	Indvirkning på forskellige risici
TR111	En angriber kan ændre en tidligere installeret legitim tegnebogsforekomst for at tilføje ondsindede funktioner.	Indvirkning på forskellige risici
TR112	En angriber kan ændre en legitim tegnebogsforekomst og foreslå den til brugerne som en legitim forekomst.	Indvirkning på forskellige risici
TR113	En angriber kan ændre selve brugergodkendelsesmekanismen, så den omgår godkendelsen af tegnebogsbrugeren.	Indvirkning på forskellige risici
TR114	En angriber kan indsætte ondsindet kode eller bagdøre i tegnebogskoden, når den implementeres i brugerenheden.	Indvirkning på forskellige risici
TR115	En angriber kan indsætte ondsindet kode eller bagdøre i tegnebogskoden under dens udvikling.	Indvirkning på forskellige risici
TR116	En angriber kan manipulere med genereringen af tilfældige tal for at reducere deres entropi tilstrækkeligt til at muliggøre angreb.	Indvirkning på forskellige risici

ID *Identifikator*	Trusselsbeskrivelse *Beskrivelse af den identificerede trussel (*)*	Risikobetegnelse *Tilknyttede risici*
TR117	En angriber kan manipulere brugerenheder i forsyningskæden for at indsætte kode eller konfigurationer, der ikke opfylder betingelserne for brug af tegnebogen.	Indvirkning på forskellige risici
TR118	En angriber kan aktivere en tegnebogsenhed, mens han bruger en forfalsket WSCD, der kontrolleres af angriberne.	Indvirkning på forskellige risici
TR119	En angriber kan læse oplysninger, der sendes til WSCA'en og/eller WSCD'en.	Indvirkning på forskellige risici
TR120	En angriber kan sende vilkårlige oplysninger til WSCA'en.	Indvirkning på forskellige risici
TR121	En angriber kan stjæle oplysninger ved at opsnappe udvekslingerne mellem WSCA'en og WSCD'en.	Indvirkning på forskellige risici
TR122	En angriber kan sende vilkårlige oplysninger til WSCD'en.	Indvirkning på forskellige risici
TR123	En angriber kan sende oplysninger til WSCD'en og omgå WSCA'en.	Indvirkning på forskellige risici
TR124	En angriber kan bruge phishing til at få brugere til at anvende en falsk tegnebog og webapplikation til PID-styring.	Indvirkning på forskellige risici
TR125	En angriber kan erstatte en tegnebogs nøgler med andre nøgler for at oprette meddelelser, der skal bruges i et andet angreb.	Indvirkning på forskellige risici
TR126	En angriber kan ændre eller ødelægge en tegnebogs nøgler, så nogle funktioner i tegnebogen bliver ubrugelige.	Indvirkning på forskellige risici
TR127	En angriber kan kontrollere malware for at få adgang til data, der er gemt i tegnebogen.	Indvirkning på forskellige risici
TR128	En angriber kan få adgang til dokumentation, der er genereret i tegnebogen.	Indvirkning på forskellige risici
TR129	Tegnebogsudbydere kan få adgang til genstande i tegnebogen.	Indvirkning på forskellige risici
TR130	Tegnebogsudbydere kan få adgang til dokumentation, der er genereret i tegnebogen.	Indvirkning på forskellige risici
TR131	En angriber kan stjæle en ulåst tegnebogsanordning.	Indvirkning på forskellige risici
TR132	En angriber kan manipulere systemet, så visse hændelser ikke logføres.	Indvirkning på forskellige risici
TR133	En angriber kan opsnappe kommunikation mellem tegnebogsforekomsten og WSCA'en eller gentage/efterligne en bruger (f.eks. ved at kapre autentifikationsmekanismen).	Indvirkning på forskellige risici

BILAG II

KRITERIER FOR VURDERING AF, OM OPLYSNINGER OM SIKRING ER ACCEPTABLE

Betegnelse	Genstand	Fokuspunkter
EUCC	IKT-produkter	Om udstederen: ingen (akkrediterede certificeringsorganer) Om omfanget: — Tjek beskyttelsesprofilen og sikkerhedsmålet — Tjek evalueringssikringsniveauet og forøgelser Om sikringen: — Tjek begrænsninger i brugerdokumentationen — Med hensyn til sammensætning kan der kræves adgang til den tekniske evalueringsrapport
EUCS (hvis tilgængelig)	Cloudtjenester	Om udstederen: ingen (akkrediterede certificeringsorganer) Om omfanget: — Tjek beskrivelsen af cloudtjenesten — Tjek evalueringsniveauet og udvidelsesprofilerne Om sikringen: — Tjek oplysningerne om gennemsigtighed og om nødvendigt oplysningerne om sammensætningen
ordninger med fælles kriterier, der anvendes i EU, herunder SOG-IS-ordninger	IKT-produkter	Om udstederen: ingen (medlemsstater) Om omfanget: — Tjek beskyttelsesprofilen og sikkerhedsmålet — Tjek evalueringssikringsniveauet og forøgelser Om sikringen: — Tjek begrænsninger i brugerdokumentationen — Med hensyn til sammensætning kan der kræves adgang til den tekniske evalueringsrapport
EN 17640:2018 (FITCEM, herunder CSPN, BSZ, LINCE, BSZA)	IKT-produkter	Om udstederen: — Tjek ordningen og kravene til certificeringsorganer Om omfanget: — Tjek produktbeskrivelsen — Tjek sikkerhedsanprisningerne — Tjek sikringsniveauet Om sikringen: — Tjek de udførte aktiviteter og resultaterne i rapporten
Certificeringsordninger for kvalificerede signaturgenereringssystemer i overensstemmelse med artikel 30 i forordning (EU) nr. 910/2014	QSCD	Om udstederen: — Tjek ordningen og kravene til certificeringsorganer Om omfanget: — Tjek produktbeskrivelsen — Tjek sikkerhedsanprisningerne — Tjek sikringsniveauet Om sikringen: — Tjek de udførte aktiviteter

Betegnelse	Genstand	Fokuspunkter
EN ISO/IEC 27001:2022	ISMS	Om udstederen: ingen (akkrediterede certificeringsorganer) Om omfanget: — Tjek beskrivelsen af styringssystemet — Tjek erklæringen om anvendelighed Om sikringen: — Tjek de udførte aktiviteter
SOC2	Organisationer	Om udstederen: — Tjek deres status som offentlig revisor Om omfanget: — Tjek ledelseserklæringen og beskrivelsen af kontrollerne — Tjek erklæringen om anvendelighed Om sikringen: — Tjek resultaterne i rapporten — Tjek eventuelle overgangsskrivelser
MDSCert (GSMA) (hvis tilgængelig)	Mobilenheder	Om udstederen: — Tjek kravene til certificeringsorganer Om omfanget: — Tjek sikringsniveauet — Tjek ordningens krav Om sikringen: — Tjek aktiviteterne og resultaterne i rapporten
Andre ordninger	Alle komponenter	Om ordningen: — Tjek ordningens relevans og bestemmelser Om udstederen: — Tjek kravene til certificeringsorganer Om omfanget: — Tjek ordningens krav — Tjek sikkerhedsmålet eller et lignende dokument, der beskriver kravene til sikkerhedsfunktionalitet og sikring — Tjek produktbeskrivelsen og udvalgte krav til sikkerhedsfunktionalitet Om sikringen: — Tjek aktiviteterne og resultaterne i rapporten

BILAG III

FUNKTIONELLE KRAV TIL TEGNEBOGSLØSNINGER

I henhold til artikel 5a, stk. 4, 5, 8 og 14, i forordning (EU) nr. 910/2014 skal de funktionelle kriterier, der skal opfyldes af en certificeret tegnebogsløsning og den elektroniske identifikationsordning, som den leveres under, omfatte de funktionelle krav til de operationer, der er anført i det følgende:

1) Kommissionens gennemførelsesforordning (EU) 2024/2979 ([1]) om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 for så vidt angår integritet og centrale funktioner

2) Kommissionens gennemførelsesforordning (EU) 2024/2982 ([2]) 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

3) Kommissionens gennemførelsesforordning (EU) 2024/2977 ([3]) 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.

([1]) 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 integritet og centrale funktioner (EUT L, 2024/2979, 4.12.2024, ELI:http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([2]) 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).

([3]) 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).

BILAG IV

EVALUERINGSAKTIVITETER — METODER OG PROCEDURER

1. Revision af gennemførelsen af en tegnebogsløsning

En overensstemmelsesvurderingsaktivitet består i at udvælge specifikke evalueringsaktiviteter.

Nationale certificeringsordninger skal specificere en evalueringsaktivitet med henblik på at vurdere de fremlagte oplysninger, der mindst omfatter følgende:

a) en analyse af de fremlagte oplysninger for at bekræfte, at de er egnede til en af de strukturer, der er angivet i de nationale certificeringsordninger

b) en analyse af dækningen af de cybersikkerhedsrisici og -trusler, der er identificeret i risikoregistret i bilag I ved de beskrevne sikkerhedskontroller.

Den analyse, der er nævnt i litra a) og b), skal baseres på det rationale og den begrundelse, som tegnebogsudbyderen har fremlagt.

2. Evalueringsaktiviteter vedrørende den sikre kryptografiske tegnebogsanordning (WSCD)

1) Kritiske operationer, herunder kryptografiske beregninger, skal ikke gennemføres fuldt ud i WSCD'en. Den del, der implementeres i WSCD'en, skal imidlertid, når den fungerer som en del af tegnebogsløsningen, garantere beskyttelsen af de kritiske operationer, den udfører, mod angreb fra angribere med stort angrebspotentiale i overensstemmelse med Kommissionens gennemførelsesforordning (EU) 2015/1502 ([1]).

2) WSCD'en eller en del heraf kan være certificeringsgenstand, når den leveres af attestindehaveren eller ansøgeren, eller uden for dens omfang, når den er indlejret i en anordning, der leveres af slutbrugeren. Nationale certificeringsordninger skal desuden specificere evalueringsaktiviteterne med henblik på at kontrollere egnetheden af WSCD'en i følgende to tilfælde:

   a) hvis WSCA'en afhænger af den specifikke WSCD (dvs. hvis den skal evalueres som et sammensat produkt på grundlag af WSCD'en), skal evalueringen af WSCA'en kræve adgang til yderligere oplysninger vedrørende certificeringen af WSCD'en, herunder navnlig dens tekniske evalueringsrapport

   b) hvis en struktur, der indgår i ordningen, anvender flere WSCD'er, eller hvis nogle af operationerne på kritiske aktiver udføres uden for WSCD'en, skal de nationale certificeringsordninger omfatte evalueringsaktiviteter for at sikre, at den samlede løsning giver det forventede sikkerhedsniveau.

3) Som en forudsætning for certificering i henhold til nationale certificeringsordninger skal WSCD'en vurderes i forhold til kravene for sikringsniveauet »høj« som fastsat i gennemførelsesforordning (EU) 2015/1502.

   Når betingelserne i artikel 3, stk. 3, litra b), er opfyldt, skal evalueringen af WSCD'en eller en del heraf omfatte en sårbarhedsvurdering som fastsat i EN ISO/IEC 15408-3:2022 på niveau AVA_VAN.5, jf. bilag I til Kommissionens gennemførelsesforordning (EU) 2024/482 ([2]), medmindre det over for certificeringsorganet er behørigt begrundet, at sikkerhedskarakteristikaene for WSCA'en gør det muligt at anvende et lavere vurderingsniveau, samtidig med at det overordnede sikringsniveau stadig er højt som fastsat i Kommissionens gennemførelsesforordning (EU) 2015/1502.

([1]) 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).

([2]) Kommissionens gennemførelsesforordning (EU) 2024/482 af 31. januar 2024 om regler for anvendelsen af Europa-Parlamentets og Rådets forordning (EU) 2019/881 for så vidt angår vedtagelsen af den europæiske cybersikkerhedscertificeringsordning baseret på fælles kriterier (EUCC) (EUT L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

4) I dokumentationen vedrørende hver specifik struktur skal de nationale certificeringsordninger desuden opstille antagelser for denne evaluering af WSCD'en, hvorunder der kan ydes modstand mod angribere med stort angrebspotentiale i overensstemmelse med Kommissionens gennemførelsesforordning (EU) 2015/1502, og de skal præcisere evalueringsaktiviteterne for at bekræfte disse antagelser og bekræfte, at antagelserne stadig er verificerede efter udstedelsen af attesten. De nationale ordninger skal også kræve, at kandidaterne til certificering finjusterer disse antagelser for deres specifikke implementering og beskriver de foranstaltninger, der er indført for at sikre, at antagelserne verificeres gennem hele livscyklussen for certificeringen.

5) I alle tilfælde skal de nationale certificeringsordninger omfatte en evalueringsaktivitet for at kontrollere, at de tilgængelige sikringsoplysninger om WSCD'en, er egnede til formålet med tegnebogsløsningen, gennem en analyse af oplysningerne om sikring, f.eks. sikkerhedsmål for EUCC-attester, herunder følgende aktiviteter:

   a) kontrol af, at omfanget af evalueringen er passende, hvilket for EUCC-attester f.eks. betyder kontrol af, at sikkerhedsmålets påstande er i overensstemmelse med en af de beskyttelsesprofiler, der anbefales i EUCC

   b) kontrol af, at antagelserne om driftsmiljøet er forenelige med tegnebogsløsningen, hvilket for EUCC-attester f.eks. betyder, at disse antagelser kan findes i sikkerhedsmålet

   c) kontrol af, at anbefalingerne i brugervejledningen eller -dokumentationen er forenelige med de betingelser, hvorpå WSCD'en skal anvendes i tegnebogsløsningen

   d) kontrol af, at antagelserne i den nationale certificeringsordning om WSCD'er er verificeret og omfattet af sikringsoplysningerne.

6) I tilfælde, hvor nogle af kontrollerne ikke fører til en endelig konklusion, skal de nationale certificeringsordninger kræve, at certificeringsorganerne specificerer kompenserende krav til WSCA'en baseret på WSCD'en, der skal medtages i evalueringen af WSCA'en. Hvis dette ikke er muligt, skal de nationale certificeringsordninger anse WSCD'en for uegnet. Det betyder, at der ikke kan udstedes en overensstemmelsesattest for tegnebogsløsningen.

3. **Evalueringsaktiviteter i forbindelse med den sikre kryptografiske tegnebogsapplikation (WSCA)**

1) Nationale certificeringsordninger skal kræve, at en WSCA, som er en del af en tegnebogsløsning, evalueres i forhold til kravene for mindst sikringsniveauet »høj« som fastsat i gennemførelsesforordning (EU) 2015/1502.

2) Denne evaluering skal omfatte en sårbarhedsvurdering som fastsat i EN ISO/IEC 15408-3:2022 på niveau AVA_VAN.5, jf. bilag I til gennemførelsesforordning (EU) 2024/482, medmindre det over for certificeringsorganet er behørigt begrundet, at sikkerhedskarakteristikaene for WSCA'en gør det muligt at anvende et lavere vurderingsniveau, samtidig med at det overordnede sikringsniveau stadig er højt som fastsat i gennemførelsesforordning (EU) 2015/1502.

3) Hvis WSCA'en ikke leveres af tegnebogsudbyderen, skal de nationale certificeringsordninger desuden opstille antagelser for denne evaluering af WSCA'en, under hvilke der kan ydes modstand mod angribere med en stor angrebskapacitet i overensstemmelse med gennemførelsesforordning (EU) 2015/1502, og de skal præcisere evalueringsaktiviteterne for at bekræfte disse antagelser og for efter udstedelsen af attesten at bekræfte, at antagelserne stadig er verificerede. De nationale ordninger skal også kræve, at kandidaterne til certificering finjusterer disse antagelser for deres specifikke implementering og beskriver de foranstaltninger, der er indført for at sikre, at antagelserne verificeres gennem hele livscyklussen for certificeringen.

4) I alle tilfælde skal de nationale certificeringsordninger omfatte en evalueringsaktivitet for at kontrollere, at de tilgængelige sikringsoplysninger om WSCA'en er egnede til formålet med tegnebogsløsningen, ved hjælp af en analyse af sikringsoplysningerne, f.eks. sikkerhedsmål for EUCC-attester, herunder følgende aktiviteter:

   a) kontrol af, at omfanget af evalueringen er passende, hvilket for EUCC-attester f.eks. betyder kontrol af, at sikkerhedsmålets påstande er i overensstemmelse med en af de beskyttelsesprofiler, der anbefales i EUCC

   b) kontrol af, at antagelserne om driftsmiljøet er forenelige med tegnebogsløsningen, hvilket for EUCC-attester f.eks. betyder, at disse antagelser kan findes i sikkerhedsmålet

c) kontrol af, at anbefalingerne i brugervejledningen eller -dokumentationen er forenelige med de betingelser, hvorpå WSCA'en skal anvendes i tegnebogsløsningen

d) kontrol af, at antagelserne i den nationale certificeringsordning om WSCA'er er verificeret og omfattet af sikringsoplysningerne.

5) Nationale certificeringsordninger skal kræve, at evalueringen af WSCA'en omfatter alle sikkerhedskontroller, der gennemføres af den pågældende WSCA.

4. **Evalueringsaktiviteter i forbindelse med slutbrugerenheden**

Da risikoregistret, jf. bilag I til denne forordning, identificerer risici, der er direkte forbundet med slutbrugerenhedens sikkerhed, skal de nationale certificeringsordninger fastsætte sikkerhedskrav til slutbrugerenheder. Da disse enheder imidlertid leveres af slutbrugeren og ikke af tegnebogsudbyderen, skal disse krav være omfattet af antagelser.

For hver antagelse skal tegnebogsløsningen omfatte en mekanisme til for hver tegnebogsenhed at kontrollere, at den underliggende slutbrugerenhed opfylder antagelsen. Sådanne mekanismer skal betragtes som sikkerhedskontrol og omfattes af evalueringsaktiviteter for at påvise både deres egnethed og deres effektivitet på det relevante sikringsniveau.

To eksempler beskrives i det følgende:

a) En slutbrugerenhed kan omfatte en certificeret WSCD, hvilket skal påvises. Dette vil typisk ske ved at verificere tilstedeværelsen af en kryptografisk hemmelighed, der kun er tilgængelig i den certificerede WSCD, ved hjælp af en kryptografisk mekanisme. I dette tilfælde bør den kryptografiske hemmelighed betragtes som et kritisk aktiv og være omfattet af certificeringen af WSCD'en og/eller WSCA'en.

b) Et typisk krav til slutbrugerenheder vil være, at enhederne skal modtage sikkerhedsopdateringer. Da dette krav vedrører tegnebogsforekomsten, skal den mekanisme, der anvendes til at kontrollere tilgængeligheden af sikkerhedsopdateringer, kun være omfattet af evalueringsaktiviteter på et sikringsniveau, der er egnet til tegnebogsforekomsten, navnlig da den sandsynligvis vil blive integreret i tegnebogsforekomsten.

5. **Evalueringsaktiviteter i forbindelse med tegnebogsforekomsten**

1) Ved evalueringen af tegnebogsforekomsten skal der tages hensyn til følgende to vigtige udfordringer:

a) tegnebogsforekomsten findes sandsynligvis i et sæt varianter af samme basisapplikation, hvor hver variant er tilpasset en bestemt kategori af slutbrugerenheder

b) de forskellige varianter af tegnebogsforekomsten har sandsynligvis behov for hyppige opdateringer for at følge udviklingen af den underliggende sikkerhedsplatform, f.eks. når der identificeres sårbarheder, der kræver ændringer af applikationer.

2) Ved evalueringen af tegnebogsforekomsten skal der tages hensyn til disse specifikke udfordringer. En af de umiddelbare konsekvenser er, at rammen for fælles kriterier muligvis ikke er egnet i alle tilfælde. Alternative evalueringsmetoder skal derfor overvejes, hvor det er nødvendigt. Nationale certificeringsordninger skal overveje at anvende EN 17640:2018-metoden:

a) som en del af selve ordningen

b) gennem nationale ordninger baseret på metoden

c) gennem nationale ordninger som er baseret på lignende principper, men som blev oprettet, inden EN 17640:2018-metoden blev udviklet.

3) Da der kan være begrænset merværdi ved at foretage en fuldstændig specifik evaluering af hver variant, skal de nationale certificeringsordninger desuden overveje at specificere kriterier, der gør det muligt at foretage stikprøveudtagning, for at undgå gentagelse af identiske evalueringsaktiviteter og for at fokusere på aktiviteter, der er specifikke for en given variant. Nationale certificeringsordninger skal kræve, at alle certificeringsorganer begrunder deres anvendelse af stikprøver.

4) Nationale certificeringsordninger skal omfatte opdateringer af tegnebogsforekomsten i den overordnede procedure for styring af ændringer, der er angivet for tegnebogsløsningen. De skal også fastsætte regler om de procedurer, der skal udføres af tegnebogsudbyderen for hver opdatering (f.eks. analyse af ændringernes indvirkning på sikkerhedskontrollen), og om de evalueringsaktiviteter, som certificeringsorganet skal udføre i forbindelse med opdateringer på nærmere angivne betingelser (f.eks. vurdering af driftseffektiviteten af en ændret sikkerhedskontrol). Proceduren for ændringsstyring er en af de procedurer, hvis driftseffektivitet skal kontrolleres årligt i overensstemmelse med artikel 18, stk. 3.

6. **Evalueringsaktiviteter i forbindelse med de tjenester og procedurer, der anvendes til levering og drift af tegnebogsløsningen**

1) Med henblik på evaluering af tjenester og procedurer, der anvendes i forbindelse med leveringen og driften af tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under, indsamler evalueringsholdet dokumentation ved at gennemføre evalueringsaktiviteter, der kan omfatte revisions-, inspektions-, verifikations- og valideringsaktiviteter.

2) Certificeringsorganet skal bekræfte, at dokumentationen er tilstrækkelig og hensigtsmæssig til at give tilstrækkelig sikkerhed for, at tjenesterne og procedurerne opfylder certificeringskravene, ved at bekræfte følgende:

   a) nøjagtigheden af de oplysninger, der præsenteres i beskrivelsen af procedurerne og tjenesterne

   b) egnetheden af udformningen af og kontrollen med procedurerne og tjenesterne til at opfylde evalueringskriterierne

   c) driftseffektiviteten af implementeringen af disse kontroller i en nærmere angivet periode forud for evalueringen.

3) Nøjagtigheden af beskrivelsen og driftseffektiviteten af en implementering af kontroller kan betragtes som verifikationsmål i henhold til ISO/IEC 17000:2020 for de tilsvarende påstande fra tegnebogsudbyderen (dvs. bekræftelse af rimeligheden af begivenheder, der allerede er indtruffet, eller resultater, der allerede er opnået), mens egnetheden af udformningen og kontrollerne af tjenesterne og procedurerne til at opfylde evalueringskriterierne kan betragtes som et valideringsmål i henhold til ISO/IEC 17000:2020 for den tilsvarende påstand fra tegnebogsudbyderen (dvs. bekræftelse af plausibilitet med hensyn til en planlagt fremtidig anvendelse eller et forventet resultat).

4) Eftersom en tegnebogsløsning ikke må fungere, før den er certificeret, kan driftseffektiviteten ikke bekræftes på grundlag af løsningens faktiske drift. Dette skal derfor bekræftes ved hjælp af dokumentation indsamlet under test eller pilotprojekter.

5) Der findes muligvis allerede nationale certificeringsordninger for specifikke tjenester og procedurer, f.eks. for onboarding af brugere. Anvendelsen af sådanne ordninger skal overvejes i nationale certificeringsordninger, hvis det er relevant.

7. **Evalueringsaktiviteter i forbindelse med de IKT-tjenester, der anvendes til levering og drift af tegnebogsløsningen**

1) Nogle tegnebogsstrukturer kan være afhængige af særlige IKT-tjenester, herunder cloudtjenester til levering og drift af en tegnebogsløsning, og disse tjenester kan indeholde følsomme data samt følsomme operationer. I så fald skal de nationale certificeringsordninger specificere sikkerhedskravene til disse IKT-tjenester.

2) Der findes allerede mange certificeringsordninger for IKT-tjenester, cloudtjenester og andre kilder til oplysninger om sikring, herunder dem, der er anført i bilag II. Nationale certificeringsordninger skal, når de er tilgængelige og anvendelige, bygge på disse eksisterende mekanismer gennem en af følgende mekanismer:

   a) det bliver muligt at anvende en bestemt ordning eller et udvalg af ordninger ved at specificere de betingelser, hvorunder IKT- eller cloudtjenester skal vurderes ved hjælp af disse ordninger

   b) valget af vurdering overlades til tegnebogsudbyderen, og afhængighedsanalyseaktiviteten anvendes til at analysere egnetheden af de oplysninger om sikring, der indhentes gennem disse vurderinger.

3) I begge tilfælde skal de nationale certificeringsordninger specificere yderligere evalueringsaktiviteter, der er nødvendige for at analysere eller supplere de oplysninger, der indhentes gennem disse ordninger.

BILAG V

LISTE OVER OFFENTLIGT TILGÆNGELIGE OPLYSNINGER OM TEGNEBØGER

1. De oplysninger, der skal offentliggøres i henhold til artikel 8, stk. 5 skal mindst omfatte følgende:
   a) eventuelle begrænsninger i brugen af en tegnebogsløsning
   b) vejledning og anbefalinger fra tegnebogsudbyderen med henblik på at bistå slutbrugerne med sikker konfiguration, installation, udrulning, drift og vedligeholdelse af tegnebøger
   c) den periode, hvor slutbrugere tilbydes sikkerhedsstøtte, navnlig for så vidt angår tilgængelighed af cybersikkerhedsrelaterede opdateringer
   d) producentens eller udbyderens kontaktoplysninger og accepterede metoder til modtagelse af sårbarhedsoplysninger fra slutbrugere og sikkerhedsforskere
   e) en henvisning til onlineregistre over offentliggjorte sårbarheder vedrørende tegnebøger og til eventuel relevant cybersikkerhedsrådgivning.

2. De oplysninger, der er omhandlet i stk. 1, skal stilles til rådighed på en klar, forståelig og letforståelig måde på et offentligt tilgængeligt sted for enhver person, der ønsker at anvende en tegnebogsløsning.

BILAG VI

METODE TIL VURDERING AF, OM OPLYSNINGERNE OM SIKRING ER ACCEPTABLE

1. Vurdering af tilgængeligheden af sikringsdokumentation

Evaluatorerne skal angive den sikringsdokumentation, der er tilgængelig for hver relevant komponent i tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under. Derefter skal evaluatorerne vurdere den overordnede relevans af hver del af sikringsdokumentationen for afhængighedsvurderingen.

Følgende aspekter skal tages i betragtning i analysen:

1) vedrørende selve sikringsdokumentationen:

   a) typen af sikringsdokumentation med alle nødvendige oplysninger

      (eksempler på sådanne dokumenter er overensstemmelsesattester i henhold til EN ISO/IEC 27001:2022 eller type 1 eller type 2 for ISAE-rapporter)

   b) den omfattede periode eller gyldighedsperiode

      (denne periode kan suppleres med en overgangsskrivelse (et dokument, der dækker en periode mellem slutdatoen for indberetningsperioden for den aktuelle ISAE-rapport og offentliggørelsen af en ny ISAE-rapport) eller en lignende erklæring)

   c) den gældende ramme (f.eks. eksisterende standard)

   d) om sikringsdokumentationen omfatter en tilknytning til ordningens krav

2) om rapportudstederens faglige kompetence og upartiskhed:

   a) navnet på certificeringsorganet og, hvis det foreligger, navnet på den ledende evaluator

   b) dokumentation for certificeringsorganets og evaluatorens kompetence (f.eks. akkreditering, personlig certificering osv.)

   c) dokumentation for certificeringsorganets og evaluatorens upartiskhed (f.eks. akkreditering osv.).

2. Vurdering af sikring i forbindelse med individuelle krav

Evaluatorerne skal kontrollere, at den sikringsdokumentation, der er tilgængelig for tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under, er tilstrækkelig til at fastslå, at tegnebogsløsningen opfylder forventningerne i forhold til certificeringsordningens individuelle krav.

Denne vurdering foretages for hver relevant komponent i tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under, ved at formulere en antagelse om tegnebogsløsningens sikkerhedskontroller.

For hver sådan antagelse afgør evalueringsholdet, om den sikring, der gives i den tilgængelige dokumentation for sikkerhed, er tilstrækkelig.

Konstateringen af, at sikringen er tilstrækkelig, baseres på følgende:

1) de krævede oplysninger er tilgængelige med det forventede sikringsniveau i sikringsdokumentationen

2) de oplysninger, der er tilgængelige i sikringsdokumentationen, dækker ikke kravets fulde omfang, men yderligere kontroller eller kompenserende kontroller (dvs. interne kontroller, der mindsker risikoen for eksisterende eller potentielle svagheder i kontrollen), som erimplementeret i tegnebogsløsningen eller i den elektroniske identifikationsordning, som den leveres under, gør det muligt for evaluatorerne at fastslå, at oplysningerne er tilstrækkelige

3) de oplysninger, der er tilgængelige i sikringsdokumentationen, giver ikke det forventede sikringsniveau, men de kontroller, der er implementeret for at vurdere og overvåge tegnebogsudbyderen, gør det muligt for evaluatorerne at fastslå, at oplysningerne er tilstrækkelige

4) hvis sikringsdokumentationen nævner manglende overensstemmelse med hensyn til udformningen eller implementeringen af de kontroller, der anvendes til at opfylde en antagelse, skal de afhjælpende foranstaltninger, der foreslås og gennemføres af tegnebogsudbyderen, og som gennemgås af dennes evaluatorer, være tilstrækkelige til at sikre, at antagelsen rent faktisk opfyldes.

BILAG VII

OVERENSSTEMMELSESATTESTENS INDHOLD

1. En entydig identifikator tildelt af det certificeringsorgan, der udsteder overensstemmelsesattesten.

2. Oplysninger om den certificerede tegnebogsløsning og de elektroniske identifikationsordninger, som den leveres under, og om indehaveren af overensstemmelsesattesten, herunder:
   a) betegnelsen for tegnebogsløsningen
   b) betegnelsen for de elektroniske identifikationsordninger, i henhold til hvilke tegnebogsløsningen leveres
   c) version af tegnebogsløsningen, der blev evalueret
   d) navn og kontaktoplysninger på indehaveren af overensstemmelsesattesten
   e) link til webstedet for indehaveren af overensstemmelsesattesten med de oplysninger, der skal gøres offentligt tilgængelige.

3. Oplysninger vedrørende evaluering og certificering af tegnebogsløsningen og de elektroniske identifikationsordninger, som den leveres under, herunder:
   a) navn og kontaktoplysninger på det certificeringsorgan, der udstedte overensstemmelsesattesten
   b) hvis forskelligt fra certificeringsorganet, navnet på det overensstemmelsesvurderingsorgan, der har foretaget evalueringen sammen med oplysninger om dets akkreditering
   c) navnet på den ordningsansvarlige
   d) henvisninger til forordning (EU) nr. 910/2014 og til denne forordning
   e) en henvisning til den certificeringsrapport, der er knyttet til overensstemmelsesattesten
   f) en henvisning til den certificeringsvurderingsrapport, der er knyttet til overensstemmelsesattesten
   g) en henvisning til de standarder, der er anvendt til evalueringen, herunder deres versioner
   h) datoen for underskrivelsen af overensstemmelsesattesten
   i) overensstemmelsesattestens gyldighedsperiode.

BILAG VIII

INDHOLDET AF DEN OFFENTLIGE CERTIFICERINGSRAPPORT OG CERTIFICERINGSVURDERINGSRAPPORTEN

1. Den offentlige certificeringsrapport skal mindst indeholde:
   a) et resumé
   b) identifikation af tegnebogsløsningen og den elektroniske identifikationsordning, som den leveres under
   c) en beskrivelse af tegnebogsløsningen og af den elektroniske identifikationsordning, som den leveres under
   d) de sikkerhedsoplysninger, der skal gøres offentligt tilgængelige, jf. bilag V, eller en henvisning til disse oplysninger
   e) et resumé af den foreløbige revisions- og valideringsplan
   f) et resumé af gennemgangen og afgørelsen om certificering.

2. Certificeringsvurderingsrapporten skal mindst indeholde:
   a) en beskrivelse af tegnebogsløsningens design, identifikationssystemet og onboardingproceduren sammen med risikovurderingen og den specifikke valideringsplan
   b) en beskrivelse af, hvordan tegnebogsløsningen opfylder kravene til sikringsniveauet »høj«, og hvordan dette fremgår af resultaterne af certificeringsvurderingen af tegnebogsløsningen, der er foretaget i overensstemmelse med denne forordning
   c) en beskrivelse af resultatet af vurderingen af tegnebogsløsningens overensstemmelse og af den elektroniske identifikationsordning, som de tilsvarende tegnebogsenheder leveres under, navnlig overensstemmelsen med:
      — kravene i artikel 5a, stk. 4, 5 og 8, i forordning (EU) nr. 910/2014
      — kravet om logisk adskillelse i artikel 5a, stk. 14, i forordning (EU) nr. 910/2014
      — hvor det er relevant, de standarder og tekniske specifikationer, der er omhandlet i artikel 5a, stk. 24, i forordning (EU) nr. 910/2014, samtidig med at det beskrives, hvordan disse krav hænger sammen med de tilsvarende normative krav, der er fastsat i nationale certificeringsordninger
   d) et resumé af resultatet af valideringsplanens gennemførelse, herunder alle konstaterede afvigelser.

BILAG IX

TIDSPLAN FOR OBLIGATORISKE OVERVÅGNINGSEVALUERINGER

1. I artikel 18 fastsættes kravene til certificeringens livscyklus, navnlig udførelsen af regelmæssige evalueringsaktiviteter. Disse aktiviteter skal mindst omfatte:

   a) en fuldstændig evaluering af genstanden for overensstemmelsesvurderingen i forbindelse med den indledende evaluering og ved hver evaluering af den fornyede certificering, herunder en opdatering af enhver produktkomponent

   b) en sårbarhedsvurdering i den indledende evaluering og ved hver evaluering med henblik på fornyet certificering og mindst hvert andet år i overvågningsevalueringer, der mindst omfatter ændringerne i genstanden for overensstemmelsesvurderingen og ændringerne i trusselsmiljøet siden den seneste sårbarhedsvurdering

   c) yderligere aktiviteter, f.eks. penetrationstest i tilfælde af et øget risikoniveau eller nye trusler

   d) en evaluering af vedligeholdelsesprocedurernes driftseffektivitet mindst hvert år i overvågningsevalueringer og evalueringer med henblik på fornyet certificering, der som minimum omfatter versionsstyrings-, opdaterings- og sårbarhedsstyringsprocedurer

   e) efter en vellykket afgørelse om revision og certificering, udstedelse af en overensstemmelsesattest efter den indledende evaluering og efter hver evaluering med henblik på fornyet certificering.

2. Der er fastsat en referenceplan i tabel 1 baseret på en fireårig cyklus, hvor:

   a) år 1 begynder, når overensstemmelsesattesten udstedes første gang, samt

   b) alle evalueringsaktiviteter skal udføres senest 12 måneder efter det foregående års evaluering.

3. Tidsplanen i tabel 1 er en anbefaling om at sikre rettidig fornyet certificering og undgå forstyrrelser i leveringen af tegnebogsløsningen. Andre tidsplaner kan være mulige, så længe overensstemmelsesattestens gyldighed ikke overstiger fem år, som fastsat i artikel 5c, stk. 4, i forordning (EU) nr. 910/2014.

4. Ud over de regelmæssige evalueringer kan der efter anmodning fra certificeringsorganet eller indehaveren af en overensstemmelsesattest udløses en særlig evaluering efter en væsentlig ændring af certificeringsgenstanden eller af trusselsmiljøet.

5. Enhver evaluering, herunder overvågningsevalueringer og særlige evalueringer, kan føre til udstedelse af en ny overensstemmelsesattest, navnlig i tilfælde af væsentlige ændringer af certificeringsgenstanden, men med samme udløbsdato som den oprindelige overensstemmelsesattest.

Tabel 1

En fuld fireårig evalueringscyklus

Tidspunkt	Evalueringstype	Aktiviteter
År 0	Indledende	— Fuld evaluering af certificeringsgenstanden, herunder sårbarhedsvurdering — herunder en funktion til at udføre opdateringer på hver softwarekomponent — Evaluering af vedligeholdelsesprocedurerne, ekskl. deres driftseffektivitet — Udstedelse af overensstemmelsesattest og påbegyndelse af den fireårige cyklus
År 1	Overvågning	— Evaluering af vedligeholdelsesprocedurernes driftseffektivitet — mindst versionskontrol, opdatering og sårbarhedsstyring — Evaluering af ændringer, der påvirker produktets sikkerhed

Tidspunkt	Evalueringstype	Aktiviteter
År 2	Overvågning	— Sårbarhedsvurdering af hele løsningen — Evaluering af vedligeholdelsesprocedurernes driftseffektivitet — mindst versionskontrol, opdatering og sårbarhedsstyring — Evaluering af ændringer, der påvirker produktets sikkerhed
År 3	Overvågning	— Evaluering af vedligeholdelsesprocedurernes driftseffektivitet — mindst versionskontrol, opdatering og sårbarhedsstyring — Evaluering af ændringer, der påvirker produktets sikkerhed
År 4	Fornyet certificering	1) Fuld evaluering af certificeringsgenstanden, herunder sårbarhedsvurdering 2) Forenklet evaluering af funktioner/procedurer, der ikke er ændret 3) herunder en funktion til at udføre opdateringer på hver softwarekomponent 4) Evaluering af vedligeholdelsesprocedurerne, herunder deres driftseffektivitet 5) Udstedelse af en ny overensstemmelsesattest