REG.NUMMER: 2022-0941
KLASSIFICERINGS-ID: 3.2.3

Tillidsramme

for svensk e-identifikation

Version 2022-10-04

1. Baggrund og formål

Tillidsrammen for svensk e-identifikation har til formål at fastsætte fælles krav til udstedere af elektroniske ID'er, der er gennemgået og godkendt af den svenske myndighed for digital forvaltning (DIGG). Kravene er opdelt i forskellige beskyttelsesniveauer – kendt som tillidsniveauer – som svarer til forskellige grader af teknisk og operationel sikkerhed fra udstederens side og forskellige grader af kontrol af, at den person, som et elektronisk identifikationsdokument udstedes til, rent faktisk er den, vedkommende udgiver sig for at være.

Kravene i denne tillidsramme finder anvendelse på tillidsniveau 2 til 4, hvor niveau 4 svarer til det højeste beskyttelsesniveau.

Opfyldelse af krav skal fortolkes på følgende måde:

(a) hvis tillidsniveauet ikke er angivet, skal kravet opfyldes på alle niveauer

(b) hvis tillidsniveauet er angivet, skal opfyldelse af krav sikres mindst på det relevante niveau.

Krav, der er fastsat på et lavere niveau end det relevante niveau, lades ude af betragtning.

2. Organisation og ledelse

Overordnede driftskrav

K2.1 Udstedere af svenske eID'er, der ikke er offentlige organer, skal fungere som registrerede juridiske enheder og tegne og vedligeholde den forsikring, der kræves for virksomheden.

K2.2 Udstedere af svenske eID'er skal have en etableret virksomhed, være fuldt operationelle i alle de dele, der er angivet i dette dokument, og være velbevandrede i de retlige krav, der stilles til dem som udstedere af svenske eID'er.

K2.3 Udstedere af svenske eID'er skal have kapacitet til at bære risikoen for erstatningsansvar og besidde tilstrækkelige finansielle ressourcer til at drive deres virksomhed i mindst et år.

Informationssikkerhed

K2.4 Udstedere af svenske eID'er skal have etableret et system til forvaltning af informationssikkerhed (ISMS) for de dele af deres aktiviteter, der er berørt af tillidsrammen, som, hvor det er relevant, er baseret på ISO/IEC 27001 eller tilsvarende principper for forvaltning og kontrol af informationssikkerhedsarbejde, herunder følgende:

(a) Alle sikkerhedskritiske administrative og tekniske processer skal dokumenteres og baseres på et formelt fundament, hvor roller, ansvar og beføjelser er klart defineret.

(b) Udstedere af svenske eID'er skal sikre, at de til enhver tid har tilstrækkelige menneskelige ressourcer til at opfylde deres forpligtelser.

(c) Udstedere af svenske eID'er skal etablere en risikostyringsproces, der på passende vis løbende eller mindst hver 12. måned analyserer trusler og sårbarheder i virksomheden, og som gennem indførelse af sikkerhedsforanstaltninger afvejer risiciene til et acceptabelt niveau.

(d) Udstedere af svenske eID'er skal etablere en hændelseshåndteringsproces, der systematisk sikrer tjenestens kvalitet, former for videresapportering, og at der træffes passende reaktive og forebyggende foranstaltninger for at afbøde eller forebygge skader som følge af sådanne hændelser.

(e) Udstedere af svenske eID'er skal udarbejde og regelmæssigt afprøve en kontinuitetsplan, der opfylder virksomhedens tilgængelighedskrav gennem evnen til at genoprette kritiske processer i tilfælde af en krise eller alvorlige hændelser.

(f) Udstedere af svenske eID'er skal regelmæssigt evaluere informationssikkerhedsarbejdet og indføre forbedringsforanstaltninger i forvaltningssystemet.

K2.5 Ledelsessystemets omfang og modenhed:

Niveau 4: Informationssikkerhedsstyringssystemet skal være i overensstemmelse med SS-ISO/IEC 27001:2017 eller tilsvarende efterfølgende eller internationale versioner af standarden og omfatte alle krav, der pålægges udstedere af svenske eID'er.

Betingelser for underleverandører

K2.6 En udsteder af svenske eID'er, der har outsourcet udførelsen af en eller flere sikkerhedskritiske processer til en anden part, skal ved kontrakt definere, hvilke kritiske processer underleverandøren er ansvarlig for, og hvilke krav der gælder for disse, og præcisere kontraktforholdet i udstedererklæringen.

Sporbarhed, sletning og opbevaring af dokumenter

K2.7 Udstedere af svenske eID'er skal opbevare:

(a) ansøgningsdokumenter og dokumenter vedrørende udstedelse, modtagelse eller blokering af eID'er

(b) kontrakter, politikdokumenter og udstedererklæringer

(c) behandlingshistorik og anden sådan dokumentation, som er nødvendig for at bevise overholdelse af de krav, der pålægges udstedere af svenske eID'er, og som muliggør opfølgning, der viser, at de sikkerhedskritiske processer og kontroller er på plads og effektive.

K2.8 Opbevaringsperioden skal være på mindst fem år, og materialet skal kunne fremstilles i læselig form i hele denne periode, medmindre et krav om sletning er nødvendigt af hensyn til privatlivets fred og understøttes af lov eller anden regulering.

Gennemgang og opfølgning

K2.9 Udstedere af svenske eID'er skal oprette en intern revisionsfunktion, der regelmæssigt gennemgår udstedelsesaktiviteterne. Den interne revisor skal være uafhængig i udførelsen af sit hverv på en måde, der sikrer en objektiv og upartisk kontrol, og skal have den kompetence og erfaring, der er nødvendig for udførelsen af vedkommendes hverv. Den interne revisor planlægger uafhængigt gennemførelsen af revisionen og dokumenterer dette i en revisionsplan, der dækker en periode på tre år. Revisionselementer udvælges på grundlag af en risiko- og væsentlighedsanalyse og baseres på de beskrivelser af operationer, som udstederen har forelagt myndigheden for digital forvaltning.

Niveau 3 og 4: Intern revision udføres på grundlag af accepterede revisionsstandarder.

3. Fysisk, administrativ og personorienteret sikkerhed

K3.1 De centrale dele af operationen skal være fysisk beskyttet mod skader som følge af miljøhændelser, uautoriseret adgang eller andre eksterne forstyrrelser. Adgangskontrol skal anvendes på en sådan måde, at adgangen til følsomme områder begrænses til autoriseret personale, at informationsbærende medier opbevares og bortskaffes sikkert, og at adgangen til disse beskyttede områder løbende overvåges.

K3.2 Inden en person påtager sig nogen af de roller, der er identificeret i overensstemmelse med K2.4, litra a), og som er af særlig betydning for sikkerheden, skal udstederen af svenske eID'er have foretaget baggrundskontrol for at sikre, at personen kan betragtes som pålidelig, og at personen har de kvalifikationer og den uddannelse, der er nødvendig for sikkert og forsvarligt at udføre de opgaver, der følger af rollen.

K3.3 Udstedere skal have indført procedurer, der sikrer, at kun specifikt autoriseret personale har adgang til de data, der indsamles og opbevares i overensstemmelse med K2.7.

K3.4 **Niveau 3 og 4:** Udstedere skal sikre gennem hele udstedelsesprocessen, at adskillelsen af funktioner anvendes på en sådan måde, at ingen enkelt person er i stand til at opnå et eID i en anden persons navn.

4. Teknisk sikkerhed

K4.1 Udstedere af svenske eID'er skal sikre, at de indførte tekniske kontroller er tilstrækkelige til at opnå det beskyttelsesniveau, der anses for nødvendigt med hensyn til virksomhedens art, omfang og andre forhold, og at disse kontroller fungerer og er effektive.

K4.2 Elektroniske kommunikationsmidler, der anvendes til overførsel af følsomme oplysninger, skal beskyttes mod opsnappelse, manipulation og afspilning.

K4.3 Følsomt kryptografisk nøglemateriale, der anvendes til at udstede eID'er, identificere indehavere og udstede identitetscertifikater, skal beskyttes på en sådan måde, at:

(a) adgangen er begrænset, logisk og fysisk, til de roller og applikationer, der er strengt nødvendige

(b) nøglematerialet aldrig lagres i klartekst på vedvarende lagringsmedier

(c) nøglematerialet er beskyttet ved brug af et kryptografisk hardwaremodul med aktive sikkerhedsmekanismer, der modvirker både fysiske og logiske forsøg på at kompromittere nøglematerialet

(d) sikkerhedsmekanismerne til beskyttelse af nøglemateriale er gennemsigtige og baseret på anerkendte og veletablerede standarder

(e) **Niveau 3 og 4:** aktiveringsdata til beskyttelse af nøglemateriale håndteres gennem flerpersonskontrol.

K4.4 Udstedere skal have indført dokumenterede procedurer for at sikre, at det krævede beskyttelsesniveau i det relevante IT-miljø kan opretholdes over tid og i forbindelse med ændringer, herunder regelmæssige sårbarhedsvurderinger og passende beredskab til at imødegå skiftende risikoniveauer og hændelser, der opstår.

5. Ansøgning, identifikation og registrering

Oplysninger om betingelser

K5.1 Udstedere af svenske eID'er skal give oplysninger om kontrakter, vilkår og betingelser samt relaterede oplysninger og eventuelle begrænsninger i brugen af tjenesten til forbundne brugere, e-tjenesteudbydere og andre, der kan være afhængige af udstederens tjeneste.

K5.2 En udsteder af svenske eID'er skal klart henvise til vilkår og betingelser og udforme procedurerne, således at vilkår og betingelser stilles til rådighed for ansøgeren i udstedelsesprocessen.

K5.3 Udstedere af svenske eID'er skal fremlægge en udstedererklæring, der omfatter:

(a) udstederens identitet og kontaktoplysninger

(b) kortfattede beskrivelser af de tjenester og løsninger, som udstederen leverer, herunder anvendte metoder til ansøgning, udstedelse og spærring

(c) betingelser i forbindelse med den leverede tjeneste, herunder brugerens forpligtelser til at beskytte sit elektroniske ID, udstederens forpligtelser og ansvar, eventuelle garantier og lovet tilgængelighed

(d) oplysninger om behandlingen af personoplysninger og den måde, hvorpå den udføres

(e) ordninger for ændring af vilkårene eller andre betingelser for den leverede tjeneste, herunder de skridt, der skal tages for at afbryde tjenesten på en kontrolleret måde.

K5.4 **Niveau 3 og 4:** Udstedere af svenske eID'er skal, efter anmodning fra myndigheden for digital forvaltning (DIGG) eller en anden kontraherende part, der er afhængig af tjenester leveret af udstederen, give oplysninger om, hvordan virksomheden ejes og forvaltes.

K5.5 En udsteder af svenske eID'er, der indstiller sine aktiviteter, skal følge en på forhånd fastlagt plan for indstilling af tjenesten. Planen skal omfatte underretning af alle brugere af tjenesten og DIGG. Udstederen skal endvidere holde arkiveret materiale tilgængeligt i overensstemmelse med K2.7 og K2.8 efter ophør.

Ansøgning

K5.6 Et svensk eID kan kun udstedes på ansøgerens anmodning eller gennem en anden tilsvarende godkendelsesprocedure, og kun efter at ansøgeren er blevet gjort opmærksom på de betingelser, hvorunder det udstedes, og det ansvar, der vil blive pålagt vedkommende.

Udstedelse af et eID, der erstatter eller supplerer et gyldigt eller nyligt spærret eID-dokument, der tidligere er udstedt af samme udsteder, kan dog finde sted uden nogen forudgående ansøgningsprocedure.

K5.7 En ansøgning om et svensk eID skal være knyttet til et personnummer eller koordineringsnummer samt de oplysninger, der ellers er nødvendige for, at udstederen kan levere et sådant eID.

Fastlæggelse af ansøgerens identitet

K5.8 Udstedere af svenske eID'er skal kontrollere, at de oplysninger, der er knyttet til ansøgningen, er fuldstændige og svarer til de oplysninger, der er registreret i et officielt register.

K5.9 Hvis oplysninger, der skal kontrolleres i et officielt register, er mærket som fortrolige ("beskyttet identitet"), kan den nødvendige kontrol foretages på anden tilsvarende måde.

K5.10 Identifikation af ansøgeren under et personligt besøg:

Udstedere af svenske eID'er kan kontrollere ansøgerens identitet under et personligt besøg på samme måde som ved udstedelse af et standardidentitetsdokument.

K5.11 Fjernidentifikation af ansøgeren i det eksisterendeforhold:

Niveau 3: Udstedere af svenske eID'er, som allerede har identificeret ansøgeren i et forhold, der involverer transaktioner af økonomisk eller juridisk betydning, og hvor ansøgeren kan identificeres på afstand ved hjælp af andre pålidelige midler svarende til niveau 3-kravene for det svenske eID-kvalitetsmærke, kan anvende denne metode til at fastslå ansøgerens identitet.

Niveau 4: Ikke relevant.

K5.12 Identifikation ved hjælp af svensk eID:

En udsteder af svenske eID'er kan fjernidentificere ansøgeren ved hjælp af et eksisterende gyldigt svensk eID med mindst samme tillidsniveau som det, der skal udstedes, hvis udstederen uden kontraktmæssige hindringer kan anvende en sådan identifikation som grundlag for udstedelse af et nyt eID.

Niveau 4: Gyldighedsperioden for det nyudstedte eID skal være begrænset til ikke at strække sig ud over gyldighedsperioden for det eksisterende eID.

K5.13 Fjernidentifikation af ansøgeren:

Niveau 2: Udstedere af svenske eID'er kan anvende pålidelige billedoptagelser af et gyldigt standardidentitetsdokument og ansøgerens ansigtsbillede som grundlag for at fastslå ansøgerens identitet på afstand, hvis sammenligningen ikke giver anledning til tvivl om ansøgerens sande identitet.

Niveau 3: Udstedere af svenske eID'er kan ved hjælp af en sikker aflæsning af et gyldigt standardidentitetsdokument, der indeholder elektronisk lagrede biometriske oplysninger, fastslå ansøgerens identitet på afstand på grundlag af disse oplysninger, hvis de tilsvarende biometriske oplysninger om den person, der skal identificeres, kan indsamles på en tilstrækkelig sikker måde, således at

der kan foretages en sammenligning med samme pålidelighed som ved et personligt besøg, og hvis sammenligningen ikke giver anledning til tvivl om ansøgerens sande identitet.

Niveau 4: Ikke relevant.

Registrering

K5.14 Udstedere af svenske eID'er skal, under hensyntagen til de gældende regler om beskyttelse af personoplysninger, føre et register over forbundne brugere og de tildelte elektroniske identifikationsdokumenter og ajourføre dette register.

6. Udstedelse og spærring af eID

Udformning af tekniske hjælpemidler

K6.1 Tekniske hjælpemidler:

Niveau 2 og 3: Tekniske hjælpemidler til elektronisk identifikation ved hjælp af eID med det svenske eID-kvalitetsmærke udformes efter et tofaktorprincip, hvor den ene del består af elektronisk lagrede oplysninger, som brugeren skal være i besiddelse af, og den anden del består af, hvad brugeren skal bruge til at aktivere eID'et.

Niveau 4: Tekniske hjælpemidler til elektronisk identifikation ved hjælp af eID med det svenske eID-kvalitetsmærke udformes efter et tofaktorprincip, hvor den ene del består af et personligt sikkerhedsmodul, som brugeren skal være i besiddelse af, og den anden del består af, hvad brugeren skal bruge til at aktivere sikkerhedsmodulet.

K6.2 Aktiveringsmekanismen og den personlige kode skal være udformet på en sådan måde, at det er usandsynligt, at tredjeparter bryder beskyttelsen, selv ved mekaniske midler.

Niveau 3 og 4: Beskyttelsen skal omfatte mekanismer til at forhindre kopiering og manipulation af det elektroniske identifikationsdokument.

K6.3 Brugere af eID med det svenske eID-kvalitetsmærke skal på eget initiativ, inden for eID'ets gyldighedsperiode, vederlagsfrit og uden væsentlig ulempe kunne ændre eller anmode om en ny personlig kode og gennem vejledning eller automatisk produktion hjælpes til at opretholde kravene i K6.2.

Hvis eID'et er udformet på en sådan måde, at en personlig kode ikke kan ændres, bør brugeren i stedet på de samme betingelser straks kunne få et nyt eID med en ny personlig kode, der erstatter den tidligere kode via en spærringsprocedure.

K6.4 Udstedere af svenske eID'er skal sikre, at de data, der er registreret med henblik på elektronisk identifikation af indehavere, entydigt repræsenterer ansøgeren og tilskrives den pågældende person, når de udsteder eID-dokumentet.

K6.5 Gyldighedsperioden for udstedte eID'er skal begrænses under hensyntagen til eID-dokumentets sikkerhedselementer og risikoen for misbrug. Den maksimale gyldighedsperiode for eID skal være fem år.

MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government

Levering af eID-dokument

K6.6 Fjernlevering:

Niveau 2: En udsteder af svenske eID'er skal levere e-ID-dokumentet på en måde, der bekræfter kontaktoplysninger, der opbevares i det officielle register, eller sådanne oplysninger, der er registreret i forbindelse med den elektroniske procedure i henhold til K5.13 niveau 2.

Niveau 3: En udsteder af svenske eID'er, der leverer et eID via en elektronisk procedure, der er i overensstemmelse med K5.11 niveau 3, K5.12 niveau 3 eller K5.13 niveau 3, skal ved nyudstedelse, separat og uafhængigt af leveringen med hensyn til sikkerhed, sikre, at brugeren informeres om, at sådanne e-ID-dokumenter er udleveret, eller ved andre foranstaltninger sikre en tilsvarende grad af kontrol med, at personen advares om risikoen for identitetstyveri i forbindelse med udleveringen.

Niveau 4: En udsteder af svenske eID'er, der leverer et eID via en elektronisk procedure, der er i overensstemmelse med K5.12, niveau 4, skal ved nyudstedelse, separat og uafhængigt af leveringen med hensyn til sikkerhed, sikre, at brugeren underrettes om, at et sådant eID-dokument er blevet udleveret.

K6.7 Levering ved et personligt besøg:

En udsteder af svenske eID'er skal under et personligt besøg og efter en identitetskontrol i overensstemmelse med K5.10 stille det elektroniske identifikationsdokument til rådighed mod underskrevet kvittering og skal endvidere stille den del til rådighed, som brugeren skal bruge til at aktivere eID'et separat og uafhængigt af leveringen af eID-dokumentet med hensyn til sikkerhed, på grundlag af kontaktoplysninger, der opbevares i et officielt register, eller andre oplysninger af tilsvarende troværdighed.

Spærringstjeneste

K6.8 Udstedere af svenske eID'er skal stille en spærringstjeneste til rådighed med god tilgængelighed, således at brugeren kan spærre deres eID.

K6.9 Udstedere af svenske eID'er skal straks og sikkert behandle og effektuere anmodninger om spærring og træffe foranstaltninger til at forhindre systematisk misbrug af spærringstjenesten eller andre forsætlige handlinger, der fører til udbredt spærring af elektroniske identifikationsdokumenter, og sikre, at brugernes eID'er er tilgængelige, når det er nødvendigt

7. Kontrol af indehaveres elektroniske identiteter

K7.1 Udstedere af svenske eID'er skal sikre, at der ved kontrol af indehaverens identitet foretages pålidelig kontrol af eID-dokumentets ægthed og gyldighed.

K7.2 Udstedere af svenske eID'er skal sikre, at der er gennemført tekniske sikkerhedskontroller i forbindelse med kontrol af indehavernes elektroniske identitet, således at det er usandsynligt, at tredjeparter ved at gætte, aflytte, afspille eller manipulere processen kan bryde beskyttelsesmekanismerne.

8. Udstedelse af identitetscertifikater

Udstedere af svenske eID'er, der leverer en tjeneste til udstedelse af identitetscertifikater til afhængige e-tjenester, skal også overholde bestemmelserne i denne afdeling.

K8.1 Udstedere af svenske eID'er skal sikre, at tjenesten for udstedelse af identitetscertifikater har god tilgængelighed, og at der forud for udstedelsen af identitetscertifikater foretages pålidelig identifikation i overensstemmelse med bestemmelserne i afdeling 7.

Niveau 4: Certifikater skal indeholde en henvisning til kryptografisk nøglemateriale, der af udstederen er verificeret som værende i indehaverens enebesiddelse.

K8.2 Udleverede identitetscertifikater skal kun være gyldige, så længe det er nødvendigt for at give brugeren adgang til den anmodede e-tjeneste, og skal beskyttes, således at oplysningerne kun kan læses af den tiltænkte modtager, og certifikaternes ægthed kan verificeres af modtagerne af certifikaterne.

K8.3 Udstedere af svenske eID'er skal, under hensyntagen til risikoen for misbrug af certificeringstjenesten, begrænse den periode, inden for hvilken der kan udstedes flere på hinanden følgende identitetscertifikater til en bestemt indehaver, inden indehaveren identificeres igen i overensstemmelse med bestemmelserne i afdeling 7.