ÄRENDENUMMER: 2022-0941
KLASSIFICERINGS-ID: 3.2.3

Tillitsramverk

för Svensk e-legitimation

Version 2022-10-04

1. Bakgrund och syfte

Tillitsramverket för Svensk e-legitimation syftar till att etablera gemensamma krav för utfärdare av Myndigheten för digital förvaltning (DIGG) granskade och godkända e-legitimationer. Kraven är fördelade på olika skyddsklasser – tillitsnivåer – som svarar mot olika grader av teknisk och operationell säkerhet hos utfärdaren och olika grader av kontroll av att den person som tilldelas en elektronisk legitimationshandling verkligen är den han eller hon utgett sig för att vara.

Kraven i detta tillitsramverk gäller tillitsnivå 2 till 4, där nivå 4 svarar mot den högsta graden av skydd.

Kravuppfyllnad ska tolkas så att

(a) om tillitsnivå inte anges ska kravet uppfyllas på samtliga nivåer, och

(b) om tillitsnivå finns angiven, ska kravuppfyllnad ske på som lägst den aktuella nivån.

Krav som anges för en lägre nivå än den aktuella ska bortses från.

2. Organisation och styrning

Övergripande krav på verksamheten

K2.1 Utfärdare av Svensk e-legitimation som inte är ett offentligt organ ska drivas som registrerad juridisk person samt teckna och vidmakthålla för verksamheten erforderliga försäkringar.

K2.2 Utfärdare av Svensk e-legitimation ska ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta dokument, samt vara väl insatt i de juridiska krav som ställs på denne som utfärdare av Svensk e-legitimation.

K2.3 Utfärdare av Svensk e-legitimation ska ha förmåga att bära risken för skadeståndsskyldighet samt förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år.

Informationssäkerhet

K2.4 Utfärdare av Svensk e-legitimation ska för de delar av verksamheten som berörs genom tillitsramverket ha inrättat ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, innefattande bland annat att:

(a) Samtliga säkerhetskritiska administrativa och tekniska processer ska vara dokumenterade och vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

(b) Utfärdare av Svensk e-legitimation ska säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden.

(c) Utfärdare av Svensk e-legitimation ska inrätta en process för riskhantering som på ett ändamålsenligt sätt, kontinuerligt eller minst var tolfte månad, analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer.

(d) Utfärdare av Svensk e-legitimation ska inrätta en process för incidenthantering som systematiskt säkerställer kvaliteten i tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada till följd av sådana händelser.

(e) Utfärdare av Svensk e-legitimation ska upprätta och regelbundet testa en kontinuitetsplan som tillgodoser verksamhetens tillgänglighetskrav genom en förmåga att återställa kritiska processer vid händelse av kris eller allvarliga incidenter.

(f) Utfärdare av Svensk e-legitimation ska regelbundet utvärdera arbetet med informationssäkerheten och införa förbättringsåtgärder i ledningssystemet.

K2.5 Ledningssystemets omfattning och mognadsgrad:

Nivå 4: Ledningssystemet för informationssäkerhet ska följa SS-ISO/IEC 27001:2017 eller därmed jämställbara efterföljande eller internationella versioner av standarden, och inom avgränsningen för detta inkludera samtliga krav som ställs på Utfärdare av Svensk e-legitimation.

Villkor för underleverantörer

K2.6 En Utfärdare av Svensk e-legitimation som på annan part har lagt ut utförandet av en eller flera säkerhetskritiska processer, ska genom avtal definiera vilka kritiska processer som underleverantören är ansvarig för och vilka krav som är tillämpliga på dessa, samt tydliggöra avtalsförhållandet i utfärdardeklarationen.

Spårbarhet, gallring och handlingars bevarande

K2.7 Utfärdare av Svensk e-legitimation ska bevara

(a) ansökningshandlingar och handlingar som rör utlämnande, mottagande eller spärr av e-legitimationer

(b) avtal, policydokument och utfärdardeklarationer, och

(c) behandlingshistorik och annan sådan dokumentation som krävs för att styrka efterlevnaden av de krav som ställs på Utfärdare av Svensk e-legitimation och som möjliggör uppföljning som visar att de säkerhetskritiska processerna och kontrollerna är införda och effektiva.

K2.8 Tiden för bevarande ska inte understiga fem år och material ska kunna tas fram i läsbar form under hela denna tid, såvida inte krav på gallring påkallas ur integritetssynpunkt och har stöd i lag eller annan författning.

Granskning och uppföljning

K2.9 Utfärdare av Svensk e-legitimation ska inrätta en funktion för internrevision som periodiskt granskar utfärdarverksamheten. Internrevisorn ska vara oberoende i utförandet av uppdraget på ett sätt som tryggar en objektiv och opartisk granskning och ha den kompetens och erfarenhet som krävs för uppdraget. Internrevisorn ska självständigt planera genomförandet av revisionen och dokumentera detta i en revisionsplan som sträcker sig över en 3-årsperiod. Revisionsmoment ska väljas utifrån en risk- och väsentlighetsanalys och grundas i de beskrivningar av verksamheten som Utfärdaren lämnat till Myndigheten för digital förvaltning.

Nivå 3 och 4: Internrevision ska ske med utgångspunkt i vedertagna revisionsstandarder.

3. Fysisk, administrativ och personorienterad säkerhet

K3.1 För verksamheten centrala delar ska skyddas fysiskt mot skada som följd av miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till behörig personal, att informationsbärande media förvaras och utmönstras på ett säkert sätt, samt att tillträde till dessa skyddade utrymmen kontinuerligt övervakas.

K3.2 Innan en person antar någon av de roller som identifierats i enlighet med K2.4.1(a), och som är av särskild betydelse för säkerheten, ska Utfärdare av Svensk e-legitimation ha genomfört bakgrundskontroll i syfte att förvissa sig om att personen kan anses vara pålitlig samt att personen har de kvalifikationer och den utbildning som krävs för att på ett säkert och betryggande sätt utföra de arbetsuppgifter som följer av rollen.

K3.3 Utfärdare ska ha rutiner som säkerställer att endast särskilt bemyndigad personal har åtkomst till de uppgifter som samlas in och bevaras i enlighet med K2.7.

K3.4 **Nivå 3 och 4:** Utfärdare ska genom hela kedjan i utfärdandeprocessen säkerställa att separation av arbetsuppgifter tillämpas på ett sådant sätt att ingen ensam person har möjlighet att tillskansa sig en e-legitimation i en annan persons namn.

4. Teknisk säkerhet

K4.1 Utfärdare av Svensk e-legitimation ska säkerställa att de tekniska kontroller som finns införda är tillräckliga för att uppnå den skyddsnivå som bedöms nödvändig med hänsyn till verksamhetens art, omfattning och övriga omständigheter, och att dessa kontroller fungerar och är effektiva.

K4.2 Elektroniska kommunikationsvägar som nyttjas i verksamheten för överföring av känsliga uppgifter ska skyddas mot insyn, manipulation och återuppspelning.

K4.3 Känsligt kryptografiskt nyckelmaterial som används för att utfärda e-legitimationer, identifiera innehavare och ställa ut identitetsintyg ska skyddas så att

(a) åtkomst begränsas, logiskt och fysiskt, till de roller och de tillämpningar som oundgängligen kräver det,

(b) nyckelmaterialet aldrig lagras i klartext på beständigt lagringsmedia,

(c) nyckelmaterialet skyddas genom användning av kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer som motverkar mot både fysiska och logiska försök att röja nyckelmaterialet,

(d) säkerhetsmekanismerna för skydd av nyckelmaterial är genomlysta och baserade på erkända och väletablerade standarder; och

(e) **Nivå 3 och 4:** aktiveringsdata för skydd av nyckelmaterial hanteras genom flerpersonkontroll.

K4.4 Utfärdare ska ha infört dokumenterade rutiner som säkerställer att erforderlig skyddsnivå i den berörda IT-miljön kan upprätthållas över tid och i samband med förändringar, innefattande regelbundna sårbarhetsundersökningar samt ändamålsenlig beredskap för att möta förändrade risknivåer och inträffade incidenter.

5. Ansökan, identifiering och registrering

Information om villkor

K5.1 Utfärdare av Svensk e-legitimation ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till anslutna användare, tillhandahållare av e-tjänster och andra som kan komma att förlita sig på utfärdarens tjänst.

K5.2 En Utfärdare av Svensk e-legitimation ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda i utgivningsprocessen.

K5.3 Utfärdare av Svensk e-legitimation ska tillhandahålla en utfärdardeklaration som innefattar

(a) utfärdarens identitet och kontaktuppgifter,

(b) översiktliga beskrivningar av de tjänster och lösningar som utfärdaren tillhandahåller, innefattande tillämpade metoder för ansökan, utgivning och spärr,

(c) villkor förknippade med den tillhandahållna tjänsten, innefattande användarens skyldigheter att skydda sin elektroniska id-handling, utfärdarens skyldigheter och ansvar, eventuella utfästa garantier och utlovad tillgänglighet,

(d) information om behandling av personuppgifter, och på vilket sätt detta sker, samt,

(e) tillvägagångssätt för att ändra villkor eller andra förutsättningar för den tillhandahållna tjänsten, inklusive de steg som ska tas för att avveckla tjänsten på ett kontrollerat sätt.

K5.4 **Nivå 3 och 4:** Utfärdare av Svensk e-legitimation ska på begäran, av Myndigheten för digital förvaltning (DIGG) eller annan avtalspart som förlitar sig på av utfärdaren tillhandahållna tjänster, lämna uppgifter om hur verksamheten ägs och styrs.

K5.5 En Utfärdare av Svensk e-legitimation som upphör med sin verksamhet ska följa en på förhand upprättad plan för avveckling av tjänsten. Planen ska innefatta att informera samtliga användare av tjänsten och DIGG. Utfärdaren ska vidare hålla arkiverat material tillgängligt i enlighet med K2.7 och K2.8 efter avvecklingen.

Ansökan

K5.6 En Svensk e-legitimation får utfärdas endast på begäran av sökanden eller genom annat likvärdigt acceptförfarande, och först efter att sökanden uppmärksammats om på vilka villkor utfärdande sker samt vilket ansvar som kommer att komma vila på denne.

Utgivning av e-legitimation som ersätter eller kompletterar en av samma utfärdare tidigare utgiven giltig eller nyligen spärrad e-legitimationshandling, får dock ske utan det föregås av ett sådant ansökningsförfarande.

K5.7 En ansökan om en Svensk e-legitimation ska knytas till personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att utfärdaren ska kunna tillhandahålla sådan e-legitimation.

Fastställande av sökandens identitet

K5.8 Utfärdare av Svensk e-legitimation ska kontrollera att uppgifterna knutna till ansökan är fullständiga och stämmer överens med uppgifter som finns registrerade i ett officiellt register.

K5.9 Om uppgifter som ska kontrolleras i ett officiellt register är sekretessmarkerade (s.k. skyddad identitet) får nödvändiga kontroller göras på annat likvärdigt sätt.

K5.10 Identifiering av sökanden vid personligt besök:

Utfärdare av Svensk e-legitimation får kontrollera sökandens identitet vid ett personligt besök, på likvärdigt sätt som vid utgivning av en fullgod identitetshandling.

K5.11 Identifiering av sökanden i befintlig distansrelation:

Nivå 3: Utfärdare av Svensk e-legitimation som redan har identifierat sökanden i en relation som rör ekonomiskt eller rättsligt betydelsefulla mellanhavanden och där sökanden kan identifieras på distans på annat tillförlitligt sätt likvärdigt med kraven för kvalitetsmärket Svensk e-legitimation Nivå 3, får använda detta sätt för att fastställa sökandens identitet.

Nivå 4: Ej tillämpligt.

K5.12 Identifiering genom Svensk e-legitimation:

En Utfärdare av Svensk e-legitimation får identifiera sökanden på distans genom befintlig giltig Svensk e-legitimation på minst samma tillitsnivå som den som ska ges ut, om denne utan avtalsrättsliga hinder kan lägga sådan identifiering till grund för utfärdande av en ny e-legitimation.

Nivå 4: Giltighetstiden för den nyutgivna e-legitimationen ska begränsas till att inte sträcka sig bortom giltighetstiden för den befintliga e-legitimationen.

K5.13 Identifiering av sökanden på distans:

Nivå 2: Utfärdare av Svensk e-legitimation får lägga tillförlitliga bildupptagningar av giltig fullgod identitetshandling och sökandens ansiktsbild till grund för att fastställa sökandens identitet på distans om jämförelsen inte ger anledning till tvivel om sökandens rätta identitet.

Nivå 3: Utfärdare av Svensk e-legitimation får, genom säker avläsning av giltig fullgod identitetshandling som innehåller elektroniskt lagrade biometriska uppgifter, fastställa sökandens identitet på distans med utgångspunkt i dessa uppgifter om motsvarande biometriska uppgifter om personen som ska identifieras kan upptas på ett tillräckligt säkert sätt så att jämförelse kan göras

med likvärdig tillförlitlighet som vid ett personligt besök, och där jämförelsen inte ger anledning till tvivel om sökandens rätta identitet.

Nivå 4: Ej tillämpligt.

Registrering

K5.14 Utfärdare av Svensk e-legitimation ska, med beaktande av tillämpliga regler för persondataskydd, föra register över anslutna användare och de tilldelade elektroniska legitimationshandlingarna, och hålla detta register aktuellt.

6. Utfärdande och spärr av e-legitimation

Utformning av tekniska hjälpmedel

K6.1 Tekniska hjälpmedel:

Nivå 2 och 3: Tekniska hjälpmedel för elektronisk identifiering genom e-legitimation med kvalitetsmärket Svensk e-legitimation, ska utformas enligt sådan tvåfaktorsprincip att en del består i elektroniskt lagrad information som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera e-legitimationen.

Nivå 4: Tekniska hjälpmedel för elektronisk identifiering genom e-legitimation med kvalitetsmärket Svensk e-legitimation, ska utformas enligt sådan tvåfaktorsprincip att en del består i en personlig säkerhetsmodul som användaren ska inneha, och en del i det som användaren ska bruka för att aktivera säkerhetsmodulen.

K6.2 Aktiveringsmekanismen och personlig kod ska utformas så att det är osannolikt att utomstående kan forcera skyddet, ens på maskinell väg.

Nivå 3 och 4: Skyddet ska innefatta mekanismer som förhindrar kopiering och manipulation av e-legitimationshandlingen.

K6.3 Användare av e-legitimation med kvalitetsmärket Svensk e-legitimation ska på eget initiativ, inom e-legitimationens giltighetstid, utan kostnad, och utan väsentliga olägenheter, kunna byta eller begära en ny personlig kod och genom vägledning eller automatisk framställning få hjälp att upprätthålla kraven i K6.2.

Om e-legitimationen är utformad på sådant sätt att personlig kod inte kan bytas, ska användare istället, under samma förutsättningar, skyndsamt kunna erhålla en ny e-legitimation med ny personlig kod som via ett spärrförfarande ersätter den föregående.

K6.4 Utfärdare av Svensk e-legitimation ska säkerställa att de uppgifter som registreras för elektronisk identifiering av innehavare unikt representerar sökanden och tillskrivs personen i fråga vid utfärdandet av e-legitimationshandlingen.

K6.5 Giltighetstiden för utfärdade e-legitimationer ska begränsas med hänsyn till e-legitimationshandlingens säkerhetsegenskaper och riskerna för missbruk. E-legitimationens giltighetstid får vara längst 5 år.

MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government

Tillhandahållande av e-legitimationshandling

K6.6 Tillhandahållande på distans:

Nivå 2: En Utfärdare av Svensk e-legitimation ska tillhandahålla e-legitimationshandlingen på ett sätt som bekräftar kontaktuppgifter förda i officiellt register eller sådana uppgifter som registrerats i samband med elektroniskt förfarande enligt K5.13 Nivå 2.

Nivå 3: En Utfärdare av Svensk e-legitimation som tillhandahåller en e-legitimation via elektroniskt förfarande som är förenligt med K5.11 Nivå 3, K5.12 Nivå 3 eller K5.13 Nivå 3 ska vid nyutgivning, separat och säkerhetsmässigt oberoende från tillhandahållandet, säkerställa att användaren informeras om att sådan e-legitimationshandling har överlämnats, eller genom andra åtgärder säkerställa motsvarande grad av kontroll över att denne uppmärksammas vid risk för identitetsstöld i samband med tillhandahållandet.

Nivå 4: En utfärdare av Svensk e-legitimation som tillhandahåller en e-legitimation via elektroniskt förfarande som är förenligt Error: Reference source not found Nivå 4 ska vid nyutgivning, separat och säkerhetsmässigt oberoende från tillhandahållandet, säkerställa att användaren informeras om att sådan e-legitimationshandling har överlämnats.

K6.7 Tillhandahållande vid personligt besök:

En Utfärdare av Svensk e-legitimation ska, vid personligt besök och efter utförd identitetskontroll i enlighet med K5.10, tillhandahålla den elektroniska legitimationshandlingen mot undertecknad kvittens, och ska vidare tillhandahålla den del som användaren ska bruka för att aktivera e-legitimationen separat och säkerhetsmässigt oberoende från tillhandahållandet av e-legitimationshandlingen, på basis av kontaktuppgifter förda i officiellt register eller andra uppgifter av motsvarande trovärdighetsgrad.

Spärrtjänst

K6.8 Utfärdare av Svensk e-legitimation ska tillhandahålla en spärrtjänst med god tillgänglighet där användaren kan spärra sin e-legitimation.

K6.9 Utfärdare av Svensk e-legitimation ska skyndsamt och på ett säkert sätt behandla och effektuera spärrbegäran, och vidta sådana åtgärder för att förhindra systematiskt missbruk av spärrtjänsten eller andra sådana avsiktliga handlingar som leder till omfattande spärr av elektroniska legitimationshandlingar, så att användares e-legitimationer är tillgängliga när de behövs

7. Kontroll av innehavares elektroniska identiteter

K7.1 Utfärdare av Svensk e-legitimation ska säkerställa att det vid verifieringen av innehavarens identitet sker tillförlitliga kontroller av e-legitimationshandlingens äkthet och giltighet.

K7.2 Utfärdare av Svensk e-legitimation ska säkerställa att tekniska säkerhetskontroller införts vid verifiering av innehavares elektroniska identiteter så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller manipulation av processen kan forcera skyddsmekanismerna.

8. Utställande av identitetsintyg

Utfärdare av Svensk e-legitimation som tillhandahåller tjänst för utställande av identitetsintyg till förlitande e-tjänster, ska även efterleva bestämmelserna i detta avsnitt.

K8.1 Utfärdare av Svensk e-legitimation ska säkerställa att tjänsten för utställande av identitetsintyg har god tillgänglighet samt att utlämnande av identitetsintyg föregås av en tillförlitlig identifiering i enlighet med bestämmelserna i avsnitt 7.

Nivå 4: Intygen ska innefatta en referens till kryptografiskt nyckelmaterial som utfärdaren verifierat att endast innehavaren förfogar över.

K8.2 Lämnade identitetsintyg ska vara giltiga endast så länge som det krävs för att användaren ska kunna beredas tillgång till den efterfrågade e-tjänsten, samt skyddas så att informationen endast är läsbar för den avsedda mottagaren och att de som tar emot intygen kan kontrollera att intygen är äkta.

K8.3 Utfärdare av Svensk e-legitimation, ska med hänsyn till riskerna för missbruk av intygstjänsten, begränsa den tidsperiod inom vilken flera på varandra följande identitetsintyg kan ställas ut för en viss innehavare, innan denne på nytt ska identifieras i enlighet med bestämmelserna i avsnitt 7.