MYNDIGHETEN FÖR DIGITAL FÖRVALTNING
Agency for Digital Government

Ärendenr 2018-158

Tillitskrav
för Valfrihetssystem 2017 E-legitimering

1. Anvisningar

Leverantör **skall** uppfylla samtliga krav i detta dokument. Leverantör som är godkänd e-legitimationsutfärdare på minst tillitsnivå 3 enligt Svensk e-legitimation behöver endast säkerställa att kraven i avsnitt 7 nedan är uppfyllda.

2. Organisation och styrning

Övergripande krav på verksamheten

K2.1 Utfärdare av e-legitimation ska teckna och vidmakthålla för verksamheten erforderliga försäkringar.

K2.2 Utfärdare av e-legitimation ska, vid avtals tecknande, 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 e-legitimation.

Informationssäkerhet

K2.4 Utfärdare av e-legitimation ska för de delar av verksamheten som berörs i detta dokument ha 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 bl.a. att:

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

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

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

(f) Utfärdare av e-legitimation ska regelbundet utvärdera informationssäkerhetsskyddet och införa förbättringsåtgärder i ledningssystemet och säkerhetskontroller.

Villkor för underleverantörer

K2.6 En utfärdare av 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 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, dokumentation och övriga uppgifter som styrker efterlevnaden av de krav som ställs på Utfärdare av e-legitimation, som möjliggör uppföljning och som visar att de säkerhetskritiska processerna och kontrollerna är införda och effektiva.

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

Granskning och uppföljning

K2.9 Ledningssystemet för informationssäkerhet och efterlevnaden av samtliga de krav som ställs på Utfärdare av e-legitimation ska under en treårsperiod vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar att revision sker på annat sätt.

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(a), och som är av särskild betydelse för säkerheten, ska Utfärdare av 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 tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

K3.3 Utfärdare av e-legitimation 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.

4. Teknisk säkerhet

K4.1 Utfärdare av 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 Kommunikation över allmänna telekommunikationsnät eller andra kommunikationslänkar som inte är fysiskt skyddade i enlighet med K3.1, ska begränsas och ömsesidigt identifieras med en styrka som minst motsvarar kraven för den aktuella e-legitimationen.

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 när det inte är under användning, direkt eller indirekt, via kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer som skyddar 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) aktiveringsdata för skydd av nyckelmaterial hanteras genom flerpersonkontroll.

K4.4 Utfärdare av e-legitimation 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 ändamålsenlig beredskap för att möta förändrade risknivåer och inträffade incidenter.

5. Ansökan, identifiering och registrering

Information om villkor

K5.1 Utfärdare av e-legitimation ska tillhandahålla uppgifter om avtal, villkor samt anknytande uppgifter och eventuella be-gränsningar i användandet av tjänsten till anslutna användare och e-tjänsteleverantörer.

K5.2 Utfärdare av e-legitimation ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne undertecknar eller annars ingår avtal med utfärdaren.

K5.3 Utfärdare av 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 utgivning, spärr och avveckling,

(c) villkor förknippade med den tillhandahållna tjänsten, innefattande användarens skyldigheter att skydda sin elektroniska identitet, utfärdarens skyldigheter och an- svar, eventuella utfästa garantier och utlovad tillgänglig- het,

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

(e) tillvägagångssätt för att ändra utfärdardeklarationen, villkor eller andra förutsättningar för den tillhandahållna tjänsten.

K5.4 Utfärdare av e-legitimation ska på begäran, av DIGG eller Förlitande part lämna uppgifter om hur verksamheten ägs och styrs.

K5.5 En utfärdare av e-legitimation som upphör med sin verksamhet ska informera sina användare och DIGG. Utfärdaren ska hålla arkiverat material tillgängligt i enlighet med K2.7 och K2.8.

Ansökan

K5.6 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 av e-legitimation tidigare utgiven giltig eller nyligen spärrad e-legitimationshandling, får dock ske utan det föregås av ett sådant ansökningsförfarande.

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

Fastställande av sökandens identitet

K5.8 Utfärdare av 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 e-legitimation ska kontrollera sökandens identitet vid ett personligt besök, på likvärdigt sätt som vid utgivning av en fullgod identitetshandling.

K5.11 Identifiering av sökanden på distans

Utfärdare av 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 som motsvarar kraven enligt Svensk e-legitimation på minst tillitsnivå 3, får använda detta sätt för att fastställa sökandens identitet.

K5.12 Identifiering grundad på e-legitimation

En Utfärdare av e-legitimation får, utöver vad som angetts i K5.11, även identifiera sökanden på distans med annan e-legitimation som motsvarar kraven enligt Svensk e-legitimation på minst tillitsnivå 3.

Registrering

K5.13 Utfärdare av 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

Tekniska hjälpmedel för elektronisk identifiering genom 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.

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

K6.3 Användare av e-legitimation ska inom e-legitimationens giltighetstid, utan kostnad, och utan väsentliga olägenheter, skyndsamt kunna erhålla en ny personlig kod som uppfyller kravet i K6.2. Om e-legitimationen är utformad på sådant sätt att personlig kod inte kan bytas, ska användare i stället, 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 e-legitimation ska säkerställa att varje användare knyts till en unik elektronisk identitet som är entydigt kopplad till den tillhandahållna 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 högst 5 år.

Tillhandahållande av e-legitimationshandling

K6.6 Tillhandahållande på distans

En utfärdare av e-legitimation som tillhandahåller e-legitimation via elektroniskt förfarande som är förenligt med K5.11 eller K5.12 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.

K6.7 Tillhandahållande vid personligt besök

En Utfärdare av e-legitimation ska, vid personligt besök och efter utförd identitetskontroll i enlighet med K5.10, tillhandahålla den elektroniska legitimationshandlingen mot under- tecknad kvittens, och ska vidare tillhandahålla den del som an- vändaren 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 e-legitimation ska tillhandahålla en spärrtjänst med god tillgänglighet där användaren kan spärra sin e- legitimation.

K6.9 Utfärdare av e-legitimation ska skyndsamt och på ett säkert sätt behandla och effektuera spärrbegäran, och vidta sådana åtgärder för att förhindra systematiskt missbruk av spärr- tjänsten, eller andra sådana avsiktliga handlingar som leder till omfattande spärr av elektroniska legitimationshandlingar.

7. Kontroll av elektronisk identitet och utställande av identitetsintyg

K7.1 Utfärdare av e-legitimation ska säkerställa att denna tjänst har god tillgänglighet samt att utlämnande av identitetsintyg föregås av en tillförlitlig kontroll av den angivna elektroniska identiteten och den elektroniska legitimationshandlingens giltighet.

K7.2 Lämnade identitetsintyg ska skyddas så att informationen endast är läsbar för den avsedda mottagaren och att den som tar emot intyget kan kontrollera att mottagna intyg är äkta.

K7.3 Utfärdare av e-legitimation ska säkerställa att tekniska säkerhetskontroller införts vid kontroll av elektronisk identitet och vid utställande av identitetsintyg, så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller

manipulation av kommunikation kan forcera skyddsmekanismerna.

K7.4 Identifierade användares anslutningar mot legitimeringsfunktionen ska tidsbegränsas.
