LEGITIMATIONS NÄMNDEN

Svarsformulär
för Valfrihetssystem 2017 E-legitimering

1. Anvisningar

Leverantör **skall** i detta Svarsformulär beskriva samt hänvisa till eventuella bilagor som visar hur kraven i Tillitskrav för Valfrihetssystem 2017 E-legitimering är uppfyllda.

Leverantör som är godkänd e-legitimationsutfärdare på minst tillitsnivå 3 enligt Svensk e-legitimation behöver endast beskriva samt hänvisa till eventuella bilagor i avsnitt 5.5.1, 6.3.4, 8.1 och 8.2 i detta Svarsformulär för att säkerställa att kraven i avsnitt 7 i Tillitskrav för Valfrihetssystem 2017 E-legitimering är uppfyllda.

2. Inledande krav

2.1 Allmän beskrivning

Detta avsnitt ska innehålla en allmän beskrivning av utfärdaren och den tillhandahållna tjänsten. Beskrivningen ska innefatta vid vilka verksamhetsställen utfärdarverksamheten bedrivs samt strukturen för utfärdarorganisationen. Utfärdaren ska även bifoga en utfärdardeklaration med sådant innehåll som följer av Tillitskrav för Valfrihetssystem 2017 E-legitimering.

- Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.2, K5.3

Svar 2.1a – Allmän beskrivning:

Svar 2.1b – Bifoga utfärdardeklaration:

Bekräfta att utfärdarens utfärdardeklaration finns bilagerad ansökan.	**Ja** ☐

2.2 Tillhandahållna e-legitimationer och tillitsnivåer

Ange nedan vilka typer av e-legitimationer med angivelse av tillitsnivå som utfärdaren avser tillhandahålla.

Svar 2.2 – Beskrivning av tillhandahållna e-legitimationer och tillitsnivåer:

2.3 Kontaktuppgifter

Här ska de uppgifter E-legitimationsnämnden ska använda för att komma i kontakt med ansvariga inom utfärdarens organisation anges. Roller vars kontaktuppgifter ska anges innefattar informationssäkerhetsansvarig, ansvarig för dokumentförvaltning, ansvarig för kontroll av överensstämmelse, personuppgiftsombud samt jourhavande för incidentberedskap.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4

Svar 2.3 – Beskrivning av kontaktuppgifter:

3. Allmänna åtaganden

3.1 Parter och deras ansvarsområden

I denna del ska redogöras för hur utfärdarens, och eventuell tredje parts, verksamhet är organiserad med avseende på e-legitimationers livscykelhantering, samt vilket ansvar som åligger respektive part eller organisationsenhet i denna del.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4

Svar 3.1 – Beskrivning av organisation, parter och deras respektive ansvarsområden:

3.2 Informationsutbyte

Under detta avsnitt ska utfärdaren beskriva former för vidarerapportering av händelser relevanta för säkerheten.

3.2.1 Rapporteringsskyldighet

I detta avsnitt ska utfärdaren beskriva vilka fastställda rutiner som införts för att säkerställa att skyldigheten att rapportera incidenter efterlevs. Denna beskrivning ska innefatta vilka rapporteringsvägar som inrättats, vilka kriterier som tillämpas för att avgöra om en incident ska rapporteras utan dröjsmål, samt vilken roll inom organisationen som bär ansvaret för vidarerapporteringen till E-legitimationsnämnden.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4

Svar 3.2.1 – Beskrivning av rutiner för rapporteringsskyldighet:

3.2.2 Periodicitet och former för rapportering

Allvarliga incidenter som kan komma att föranleda omedelbara åtgärder från E-legitimationsnämndens sida ska rapporteras utan dröjsmål. Mindre allvarliga incidenter och andra uppgifter som omfattas av rapporteringsskyldigheten ska rapporteras med vissa intervall. I detta avsnitt ska utfärdaren beskriva periodiciteten och formerna för den regelbundna rapporteringen.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4 e)

Svar 3.2.2 – Beskrivning av periodicitet och former för rapportering:

4. Organisation och styrning

4.1 Ledningssystem för informationssäkerhet

I detta avsnitt ska utfärdaren beskriva det ledningssystem för informationssäkerhet som denne infört för att styra informationssäkerhetsarbetet och kontrollera risker. Redogörelsen ska fokusera på det övergripande ledningssystemet och metodiken för riskhantering, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra informationssäkerheten inom utfärdarorganisationen.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4

Svar 4.1 – Beskrivning av ledningssystem för informationssäkerhet:

5. Fysisk, administrativ och personalorienterad säkerhet

5.1 Fysisk säkerhet

5.1.1 Driftanläggningars beskaffenhet och lokalisering

I detta avsnitt ska utfärdaren beskriva de driftanläggningar inklusive eventuella alternativa driftanläggningar som utfärdaren använder eller kan komma att använda för att tillhandahålla de tjänster som ska levereras; innefattande tjänster för intygsutgivning, spärrtjänst och utfärdande av e-legitimationer.

Driftanläggningars lokalisering ska preciseras på minst regionnivå, och anläggningens beskaffenhet bör beskrivas utifrån den klassificering som finns i stöldskyddsföreningens normer för mekaniskt stöldskydd (SSF 200:3) och larmanläggningar (SSF 130).

I den mån även andra utrymmen än de aktuella driftanläggningarna kan komma att användas för att förvara informationsbärande media eller utrustning innehållande känsliga uppgifter, så ska även dessa utrymmen innefattas i beskrivningarna.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.1

Svar 5.1.1 – Beskrivning av driftanläggningars beskaffenhet och lokalisering:

5.1.2 Fysiskt tillträde till skyddade utrymmen

I detta avsnitt ska utfärdaren beskriva formerna för fysisk åtkomstkontroll till de skyddade utrymmen i vilka informationsbärande media eller utrustning innehållande känsliga uppgifter kan komma att förvaras. Beskrivningen ska innefatta den krets av personer som har fysiskt tillträde till utrymmena, samt eventuellt tillkommande kontroller avsedda att begränsa obehöriga personers möjlighet att komma åt utfärdarens utrustning.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.1

Svar 5.1.2 – Beskrivning av principer för fysiskt tillträde till skyddade utrymmen:

5.1.3 Strömförsörjning, miljö och brandskydd

Utfärdaren ska under denna rubrik beskriva driftanläggningarnas förutsättningar till kontinuerlig strömförsörjning och kontrollerad miljö samt de åtgärder som vidtagits för skydd mot brand i de skyddade utrymmena.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.1

Svar 5.1.3 – Beskrivning av strömförsörjning, miljö och brandskydd:

5.2 Administrativ säkerhet

5.2.1 Betrodda roller inom organisationen

I detta avsnitt ska utfärdaren redogöra för de betrodda roller som existerar inom organisationen, vilket ansvar som följer av respektive roll och på vilket sätt dessa roller är bemannade.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K 2.4(a), K3.2

Svar 5.2.1 – Beskrivning av betrodda roller inom organisationen:

5.2.2 Åtgärder som kräver separation av arbetsuppgifter

Vissa särskilt säkerhetskritiska åtgärder kan fordra att flera personer i förening krävs för genomförandet (utöver det som anges under 6.2.1). Här ska utfärdaren i förekommande fall redogöra för vilka åtgärder som kräver sådana kontroller, vilka roller som involveras och på vilket sätt samt hur efterlevnad säkerställs.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.2, K4.1

Svar 5.2.2 – Beskrivning av åtgärder som kräver separation av arbetsuppgifter:

5.2.3 Identifiering av personer i betrodda roller

Personer i betrodda roller besitter som regel sådan fysisk- och/eller logisk behörighet till informationstillgångar och informationsbehandlingsresurser som medför att ett särskilt säkerhetskritiskt ansvar vilar på dem. I detta avsnitt ska utfärdaren beskriva vilka kontroller som tillämpas för att identifiera dessa personer vid (fysisk och logisk) åtkomst till sådana informationstillgångar.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.1, K4.1

Svar 5.2.3 – Beskrivning av identifiering av personer i betrodda roller:

5.3 Personalorienterad säkerhet

Följande avsnitt avses i första hand gälla personal i betrodda roller, men även övrig personal som i sitt arbete kan komma i kontakt med sådana informationstillgångar och system som används för att tillhandahålla tjänsten. Exempel innefattar säkerhetsansvariga, systemadministratörer, personal i registraturfunktion, handläggare och underhållspersonal.

5.3.1 Bakgrund och kvalifikationer

Utfärdaren ska beskriva de rutiner som tillämpas för att säkerställa att personal i betrodda roller samt de som i övrigt kan komma i kontakt med känsliga informationstillgångar och system, kan anses pålitlig och har den utbildning och de kvalifikationer som krävs för att fullgöra sina arbetsuppgifter på ett korrekt och säkert sätt.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.2

Svar 5.3.1 – Beskrivning av kontroll av bakgrund och kvalifikationer:

5.3.2 Utbildning av personal

Personal i betrodda roller kräver som regel specifik utbildning i de arbetsuppgifter de ska utföra. Utfärdaren ska beskriva hur denne bedriver utbildning av sådan personal, vid anställning och därefter regelbundet.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.2

Svar 5.3.2 – Beskrivning av utbildning av personal:

5.3.3 Krav vid utkontraktering av personal

Då personal som inte är anställd vid utfärdaren (och inte genomgått bakgrundskontroll och utbildning hos utfärdaren) ska utföra tillfälligt arbete där denne kan komma i kontakt med informationstillgångar och system, krävs som regel att dessa kontrolleras eller att det på annat sätt säkerställs att säkerheten upprätthålls. I detta avsnitt ska utfärdaren beskriva sådana kontroller denne tillämpar då kontrakterad personal utför sådant arbete.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.6, K3.2, K3.3

Svar 5.3.3 – Beskrivning av krav vid utkontraktering av personal:

5.4 Spårbarhet och loggning

Följande avsnitt avses omfatta all den information som krävs för att säkerställa uppföljning av säkerhetsrelaterade händelser, även innefattande den information som krävs för revision av ledningssystem, med mera.

5.4.1 Händelser som registreras i säkerhetslogg

Registrering av så kallad behandlingshistorik eller säkerhetslogg ska innefatta samtliga händelser som relaterar till livcykelhanteringen av e-legitimationer, såväl som personals åtkomst till känsliga informationstillgångar och system. Utfärdaren ska här redogöra för de grundprinciper som gäller för sådan registrering. Behandlingshistorik eller säkerhetslogg.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.7

Svar 5.4.1 – Beskrivning av händelser som registreras i säkerhetslogg:

5.4.2 Kontroll och uppföljning av säkerhetsrelaterade händelser

Utfärdaren ska beskriva under vilka premisser regelbunden och särskild kontroll av säkerhetsrelaterade händelser sker. Exempel kan innefatta stickprov av dokumentation som stödjer att utfärdandeprocessen fungerar som avsett, eller kontroller av vilken personal som sökt åtkomst till vilken information och när, samt i vilken mån de haft befogenhet att vidta dessa åtgärder.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.9, K3.3

Svar 5.4.2 – Beskrivning av kontroll och uppföljning av säkerhetsrelaterade händelser:

5.4.3 Skydd av spårbarhetsinformation

Information som registreras i säkerhetslogg eller bevaras för revisions- och uppföljningsändamål kan vara av både integritetskänslig och säkerhetskritisk karaktär. Utfärdaren ska beskriva de åtgärder som vidtagits för att säkerställa dessa informationstillgångars sekretess, deras integritet samt även spårbarheten vid åtkomst till dem.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K3.3, K4.1

Svar 5.4.3 – Beskrivning av skydd av spårbarhetsinformation:

5.4.4 Handlingars bevarande

Den spårbarhetsinformation som krävs för uppföljning ska bevaras i enlighet med bestämmelserna i Tillitskrav för Valfrihetssystem 2017 E-legitimering. Utfärdaren ska beskriva hur sådant bevarande säkerställs då informationen t.ex. flyttas ur systemen för att arkiveras. Detta ska innefatta beskrivning av hur det är säkerställt att informationen kan eftersökas, läsas tillbaka och tolkas under hela tiden för bevarande. Beskrivningarna ska även innefatta hur det är säkerställt att fysiska handlingar kan återsökas under samma förutsättningar.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.8

Svar 5.4.4 – Beskrivning av handlingars bevarande:

5.4.5 Gallring

Då tiden för bevarande förlöpt ska spårbarhetsinformationen gallras. Vid gallring ska sådan information utplånas på ett säkert sätt, så att den inte enkelt kan återskapas. Olika informationstyper kan också ha olika tid för bevarande. Utfärdaren ska redogöra för hur information gallras på ett sådant sätt att dessa krav är uppfyllda.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.8

Svar 5.4.5 – Beskrivning av gallring:

5.5 Operationella aspekter

5.5.1 Kontinuitetsplanering

Utfärdaren ska ha upprättat en kontinuitetsplan som säkerställer förmågan att återställa kritiska processer vid händelse av allvarliga incidenter eller kris. Denna kontinuitetsplan ska även regelbundet testas och övas. Utfärdaren ska redogöra för det övergripande innehållet i denna kontinuitetsplan, och med vilken frekvens den testas och övas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4, K6.9, K7.1

Svar 5.5.1 – Beskrivning av kontinuitetsplanering:

5.5.2 Incidenthantering

Incidenthanteringen är ett av de viktigaste verktygen att förebygga och att lindra konsekvenserna av säkerhetsbrott. I detta avsnitt ska utfärdaren redogöra för hur de interna rutinerna kring incidenthanteringen fungerar, till exempel innefattande hur incidenter och rotorsaker utreds, införande av konsekvensbegränsande och förebyggande åtgärder samt utvärdering och uppföljning.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4

Svar 5.5.2 – Beskrivning av incidenthanteringsprocessen:

5.5.3 Avveckling av tjänsten

En avveckling av tjänsten ska ske under kontrollerade former. Utfärdaren ska redogöra för de övergripande momenten i en sådan avvecklingsprocess, innefattande hur dess användare informeras och hur information som ska bevaras hålls tillgänglig.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K5.5

Svar 5.5.3 – Beskrivning av avveckling av tjänsten:

6. Teknisk säkerhet

6.1 Kryptografiska funktioner

Säkerheten i hanteringen och användningen av e-legitimationer beror till betydande del på starka kryptografiska funktioner. För att säkerställa denna styrka är det viktigt att de kontroller som omgärdar nyckelhanteringen är baserade på välkända och genomlysta funktioner och metoder. I de följande underavsnitten ska utfärdaren visa hur denne har säkerställt en hög säkerhet i kryptografiska funktioner och kring hanteringen av sådant känsligt kryptografiskt nyckelmaterial som används för att utfärda e-legitimationer, identifiera innehavare och ställa ut identitetsintyg.

6.1.1 Kryptografiska algoritmer och nyckeltyper

Grundläggande är att utfärdaren har identifierat vilka kryptografiska nycklar denne hanterar inom ramen för utfärdarverksamheten, och kategoriserat dessa. I detta avsnitt ska utfärdaren redogöra för de kryptografiska algoritmer och de kategorier, hierarkier och kedjor av kryptografiskt nyckelmaterial som säkerheten i utfärdarverksamheten kan komma att bero på.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.3

Svar 6.1.1 – Beskrivning av kryptografiska algoritmer och nyckeltyper:

6.1.2 Nycklars livscykel

I detta avsnitt ska utfärdaren redogöra för de olika administrativa livslängder som utfärdaren tilldelat olika kategorier av nycklar, det vill säga vilken utbytesfrekvens som ska gälla och vilka olika faser som existerar i nycklarnas livscykel.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.1.2 – Beskrivning av nycklars livscykel:

6.1.3 Omgivning och metodik för nyckelframställning

Det sätt på vilket krypteringsnycklar framställs kan vara avgörande för de kryptografiska säkerhetsfunktionernas styrka. I detta avsnitt ska utfärdaren beskriva det sätt och den omgivning som används för att framställa nycklar inom utfärdarverksamheten. Den källa och metod till slumptalsframställning, samt den metod som används för att säkerställa nyckelparametrars kvalitet ska även beskrivas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.3

Svar 6.1.3 – Beskrivning av omgivning och metodik för nyckelframställning:

6.2 Förvaring och skydd av privata nycklar

Stora delar av informationssäkerhetsskyddet utgår ifrån att utfärdarens privata nycklar hålls konfidentiella över förhållandevis lång tid. Detta fordrar rigorösa kontroller i nyckelhanteringen.

6.2.1 Flerpersonskontroll av privata nycklar

I enlighet med Tillitskrav för Valfrihetssystem 2017 E-legitimering ska konfidentiellt nyckelmaterial som utfärdaren hanterar i anslutning till e-legitimationer med tillitsnivå 3 och högre, stå under flerpersonkontroll. Med detta avses att sådana aktiveringsdata eller andra uppgifter som kan användas för att återskapa

och/eller börja använda sådana nycklar, ska kontrolleras av minst två personer i förening.

I detta avsnitt ska utfärdaren redogöra för hur kravet på flerpersonkontroll är uppfyllt och beskriva det skydd som också omgärdar aktiveringsdata.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.3

Svar 6.2.1 – Beskrivning av flerpersonskontroll av privata nycklar:

6.2.2 Säkerhetskopiering av privata nycklar

Vissa privata nycklar kan behöva säkerhetskopieras då de inte med enkelhet snabbt kan bytas vid en eventuell förlust. Utfärdare ska övergripande redogöra för vilka nycklar denne anser kräver säkerhetskopiering, och hur dessa säkerhetskopior görs och hur säkerhetskopiorna skyddas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.3

Svar 6.2.2 – Beskrivning av säkerhetskopiering av privata nycklar:

6.2.3 Utplåning av privata nycklar

I detta avsnitt ska utfärdaren övergripande redogöra för de procedurer som denne tillämpar för att utplåna känsligt nyckelmaterial ifrån t.ex. uttjänt lagringsmedia eller utrangerad utrustning.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.2.3 – Beskrivning av procedurer för utplåning av privata nycklar:

6.3 Säkerhet i drift- och utvecklingsmiljö

6.3.1 Systemsäkerhet

Utfärdare ska redogöra för de principer denne tillämpar för att upprätthålla den tekniska systemsäkerheten i de olika delsystemen, innefattande säkerhet i operativsystem, åtkomststyrning, införande av kritiska säkerhetsrättningar, med mera.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.3.1 – Beskrivning av principer för upprätthållande av systemsäkerhet:

6.3.2 Systemutveckling

Utfärdare som utvecklar egen programvara som används inom utfärdarverksamheten och är av betydelse för säkerheten, ska redogöra för de principer som råder för säkerställande av kvalitet och säkerhet i utvecklingsprocessen.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.4

Svar 6.3.2 – Beskrivning av kvalitetssäkringsrutiner i systemutvecklingsprocessen:

6.3.3 Systemunderhåll och styrning av ändringar i drift

I systemunderhåll ingår att regelbundet införa ny funktionalitet, ändringar och programrättningar i operativ- och tillämpningssystem. I detta avsnitt ska utfärdaren redogöra för principerna för hur sådana ändringar testas och införs i driftmiljön, och hur det är säkerställt att informationssäkerhetsskyddet upprätthålls i samband med sådana ändringar. Utfärdaren ska även redogöra för hur ofta servicetillfällen förekommer, hur de planeras och godkänns, avbrottstidens maximala längd, samt vilka åtgärder som vidtas om avbrott riskerar att vara längre än planerat.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.4

Svar 6.3.3 – Beskrivning av rutiner för styrning av ändringar i drift:

6.3.4 Styrmedel för nätverkskommunikation

Logiskt sektionerade nätverk med indelning i olika säkerhetszoner och filtrering av kommunikation däremellan är en generell metod för att hantera de hot och lindra de sårbarheter som uppstår vid kommunikation över öppna nätverk. Utfärdare ska på en principiell nivå redogöra för hur sådan sektionsindelning och filtrering är införd. Vidare ska sådana krypteringsåtgärder som vidtagits för att

förhindra insyn, manipulation och återuppspelning av kommunikation beskrivas. Även mekanismer som införts och förberedelser som vidtagits för att lindra effekterna av eventuella överbelastningsangrepp ska belysas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1, K4.2, K6.8, K7.1

Svar 6.3.4 – Beskrivning av styrmedel för nätverkskommunikation:

6.3.5 Spårbar tid

Korrekt tid är en avgörande faktor för säkerheten vid utfärdande och användning av e-legitimationer, utställande av identitetsintyg och registrering av händelser i behandlingshistorik (säkerhetslogg). Utfärdaren ska redogöra för de åtgärder man vidtagit för att säkerställa tillgången till korrekt och spårbar tid.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.3.5 – Beskrivning av tillgång till spårbar tid:

6.3.6 Säkerhetskopiering

I detta avsnitt ska utfärdaren beskriva vilka åtgärder som vidtagits för att förhindra dataförlust, samt hur förmågan att återställa information från säkerhetskopior inom erforderlig tid upprätthålls, t.ex. genom återläsningstester. Det ska även framgå principer för förvaring av säkerhetskopior och hur ofta återställning testas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.3.6 – Beskrivning av rutiner för säkerhetskopiering:

6.3.7 Övervakning

Utfärdare ska redogöra för principer kring hur övervakning av kritiska system görs, och med vilka fastställda prioriteringar och åtgärdstider upptäckta avvikelser hanteras.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 6.3.7 – Beskrivning av rutiner för övervakning:

7. Ansökan, identifiering och registrering

7.1 Ansökan och information om villkor

Utfärdaren ska beskriva hur ansökningsfarandet går till och hur det säkerställs att villkoren förknippade med tjänsten kommer den som söker e-legitimation till del innan denne ingår avtal med utfärdaren. Även förutsättningar för att förändra dessa villkor ska belysas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K5.1, K5.2, K5.6, K5.7

Svar 7.1a – Beskrivning av ansökningsförfarandet och information om villkor:

Svar 7.1b – Bifoga allmänna villkor:

Bekräfta att utfärdarens allmänna villkor finns bilagerad ansökan.	**Ja** ☐

7.2 Identifiering och registrering

7.2.1 Fastställande av sökandens identitet

Utfärdaren ska i denna del belysa hur identiteten på den som ansöker om e-legitimation fastställs, om det är fråga om ett distansförfarande eller om identifiering sker vid ett personligt besök.

Om distansförfarande används ska utfärdaren även beskriva det rättsligt eller ekonomiskt betydelsefulla förhållande som råder mellan den som ansöker om e-legitimation och utfärdaren, samt de metoder som används för att på ett säkert sätt identifiera sökanden på distans.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K5.8-K5.12

Svar 7.2.1 – Beskrivning av fastställande av sökandens identitet:

7.2.2 Registreringsförfarande

Utfärdaren ska beskriva hur lämnade uppgifter från den som ansöker om e-legitimation verifieras, vilka uppgifter som lämnas och registreras samt den metod och källa utfärdaren använder för att kontrollera uppgifter, samt rutiner för att hålla detta register aktuellt.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K5.8, K5.9, K5.13

Svar 7.2.2 – Beskrivning av registreringsförfarandet:

7.3 Utfärdande och spärr av e-legitimation

7.3.1 Utformning av tekniska hjälpmedel

I detta avsnitt ska utfärdaren beskriva utformningen av de tekniska hjälpmedel (e-legitimationshandling och eventuellt tillkommande tekniskt stöd) som denne tillhandahåller den som ansöker om e-legitimation.

Utfärdaren ska också beskriva vilka skyddsmekanismer som omgärdar aktiveringen av användares privata nyckelmaterial, innefattande hur kraven upprätthålls gällande kvalitet i personlig kod och skydd mot uttömmande sökning.

Vidare ska beskrivas hur, om och under vilka förutsättningar användares e-legitimationer kan komma att blockeras. Med blockering avses här i den mån e-legitimationen har sådant aktivt skydd som blockerar (tillfälligt spärrar) användningen om aktivering misslyckats eller efter det att det aktiva skyddet detekterat försök att röja nyckelmaterialet på annat sätt, t.ex. via sidokanaler eller manipulation.

Blockering kan dock även tänkas ske även på annat sätt, t.ex. genom att en del i aktiveringsförfarandet görs direkt mot utfärdaren, och att den elektroniska identiteten vid ett visst antal felaktiga aktiveringsförsök blockeras.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K6.1, K6.2, K6.3

Svar 7.3.1a – Beskrivning av utformning av tekniska hjälpmedel:

Svar 7.3.1b – Exempel på tekniska hjälpmedel:

Bekräfta att utfärdaren på begäran från E-legitimationsnämnden kan tillhandahålla exemplar av tekniska hjälpmedel för granskning i samband med ansökan.	**Ja** ☐

7.3.2 Skapande av e-legitimationshandling

Utfärdaren ska redogöra för hur innehavares privata nycklar skapas, lagras och skyddas då de tillhandahållits innehavaren.

I de fall då symmetriska kryptografiska funktioner används för identifiering av innehavare, ska även anges och hur dessa nycklars eller koders konfidentialitet skyddas i utfärdarens tekniska omgivning vid verifiering av sådana e-legitimationer.

Utfärdaren ska också beskriva vilka identitetsbegrepp (unika identifierare, löpnummer eller motsvarande) denne använder internt för kontroll och spärr av enskilda e-legitimationshandlingar.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.3, K6.2, K6.4, K6.5

Svar 7.3.2 – Beskrivning av skapande av e-legitimationshandling:

7.3.3 Tillhandahållande av e-legitimationshandling

Utfärdaren ska i detta avsnitt beskriva hur tillhandahållandet av e-legitimationshandlingen sker, om detta sker vid personligt besök eller på distans och hur det annars säkerställs att e-legitimationshandlingen tillhandahålls till rätt mottagare.

Om aktiveringsdata framställts som del i utgivningsprocessen behöver även detta distribueras till innehavaren på ett säkert sätt. Normalt tillhandahålls aktiveringsdatat skilt från e-legitimationshandlingen. Under denna process är det viktigt att aktiveringsdatats konfidentialitet skyddas. Utfärdaren ska mot bakgrund av vad denne angett i det föregående beträffande aktiveringsdata, beskriva de procedurer som används för att distribuera aktiveringsdatat till de avsedda mottagarna.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K6.2, K6.6, K6.7

Svar 7.3.3a – Beskrivning av process för tillhandahållande av e-legitimationshandling:

Svar 7.3.3b – Exempel på tillhandahållande av e-legitimationshandling:

Bekräfta att utfärdaren på begäran från E-legitimationsnämnden kan tillhandahålla exempel på sådan kommunikation som används i samband med tillhandahållande av e-legitimationshandling.	**Ja** ☐

7.4 Spärrtjänst

7.4.1 Rutin för begäran om spärr

Utfärdaren ska beskriva vilka sätt som står till buds för innehavare att spärra sin e-legitimation, och hur det är rimligt säkerställt att missbruk av spärrfunktionen inte kan förekomma.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K6.8, K6.9

Svar 7.4.1 – Beskrivning av rutin för begäran om spärr:

7.4.2 Befogenhet att begära spärr

Utfärdaren ska beskriva vilka andra, förutom innehavaren själv, som har befogenhet att begära spärr av en e-legitimationshandling och vilka kontroller som i så fall tillämpas.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K6.8, K6.9

Svar 7.4.2 – Beskrivning av befogenhet att begära spärr:

7.4.3 Behandlingstid vid begäran om spärr

Utfärdaren ska beskriva hur lång tid det maximalt ska ta från det att denne erhållit en spärrbegäran till dess att begäran är effektuerad och i kraft.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K6.8, K6.9

Svar 7.4.3 – Beskrivning av behandlingstid vid begäran om spärr:

8. Verifiering av elektronisk identitet och utställande av identitetsintyg

Utfärdaren ska i detta avsnitt, i tillämpliga delar, beskriva den eller de tjänster som tillhandahålls för verifiering av elektronisk identitet och utställande av identitetsintyg.

För det fall utfärdaren inte själv ansvarar för någon tjänst för utställande av identitetsintyg, ska utfärdaren under respektive punkt nedan istället beskriva hur kraven på tillgänglighet, skydd mot missbruk och obehörig åtkomst i samband med verifiering av elektronisk identitet säkerställs genom avtal med exempelvis Leverantör av eID-tjänst, eller genom annan teknisk lösning än sådan intygsgivningstjänst som i övrigt förutsätts inom en identitetsfederation för Svensk e-legitimation.

8.1 Intygsgivningstjänstens tillgänglighet

Beskrivningarna i denna del ska innefatta vilken utlovad tillgänglighet funktionen för utställande av identitetsintyg har, hur denna tillgänglighet mäts och följs upp, vad som ska betraktas som godtagbara svarstider samt vilka åtgärder som är vidtagna för att säkerställa upprätthållandet av denna servicegrad.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K7.1

Svar 8.1 – Beskrivning av intygsgivningstjänstens tillgänglighet:

8.2 Skydd mot missbruk av identitetsintyg och intygsgivningstjänst

Utfärdaren ska i detta avsnitt beskriva vilka åtgärder som vidtagits för att förhindra att identitetsintyg missbrukas av obehöriga. Denna redogörelse ska innefatta:

- säkerhetsåtgärder vidtagna för att förhindra eller försvåra för så kallat nätfiske och motsvarande bedrägliga metoder som syftar till att lura användaren att legitimera sig mot en falsk intygsgivningstjänst,
- säkerhetsåtgärder vidtagna för att förhindra eller försvåra avlyssning eller manipulation av kommunikation och intyg,
- lämnade intygs giltighetstid, samt
- de tidsbegränsningar av identifierade användarens anslutningar, varefter en ny identifiering av användaren krävs.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K7.1, K7.2, K7.3, K7.4

Svar 8.2 – Beskrivning av skydd mot missbruk av identitetsintyg och intygsgivningstjänst:

8.3 Skydd mot obehörig åtkomst

Den riskanalys utfärdaren regelbundet ska genomföra förväntas identifiera intygsgivningstjänsten som särskilt utsatt för risk, då denna i normalfallet har en hög exponeringsgrad samtidigt som säkerhetsberoendet till denna funktion är mycket stort. Särskilt rigorösa tekniska säkerhetskontroller och kvalitetssäkringsrutiner förväntas därför omgärda denna del.

Utfärdaren ska redogöra för vilka särskilda skyddsåtgärder denne vidtagit i intygsgivningsfunktionen, och som syftar till att:

- förhindra missbruk eller röjande av det känsliga kryptografiska nyckelmaterial som tjänsten kräver åtkomst till,
- förhindra kvalificerade och motiverade angripare från att göra intrång i intygsgivningstjänsten,
- försök till eller faktiskt sådant intrång, missbruk eller röjande av nyckelmaterial inte ska kunna undgå upptäckt.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K4.1

Svar 8.3 – Beskrivning av skydd mot obehörig åtkomst:

9. Revision

För att verifiera att införda kontroller fungerar och är effektiva ska utfärdaren genomföra internrevision av de delar av utfärdarverksamheten som omfattas av Tillitskrav för Valfrihetssystem 2017 E-legitimering. I den mån revision av ledningssystemet för informationssäkerhet sker separat från revision gentemot Tillitskrav för Valfrihetssystem 2017 E-legitimerings krav ska även aspekter kopplade till detta belysas i efterföljande avsnitt.

9.1 Revisionens periodicitet och omfattning

Utfärdare ska redogöra för den revisionsplan denne beslutat om, där det ska framgå med vilken periodicitet och med vilken omfattning varje revision ska göras. Redogörelsen ska även omfatta process för revisionsplanering samt beskrivning av revisionsrapportering, inklusive hantering av uppföljning av eventuella avvikelser.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.9

Svar 9.1a – Beskrivning av revisionens periodicitet och omfattning:

Svar 9.1b – Bekräftelse avseende revisionsplan och revisionsrapport:

Bekräfta att utfärdaren på begäran från E-legitimationsnämnden kan presentera revisionsplan samt revisionsrapport från senast genomförda revision.	**Ja** ☐

9.2 Revisorns kvalifikationer

Utfärdaren ska redogöra för vilka formella kompetenskrav som ställs på den huvudansvariga revisorn.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.9

Svar 9.2 – Beskrivning av revisorns kvalifikationer:

9.3 Revisorns förhållande till den granskade parten

Utfärdaren ska redogöra för det förhållande som råder mellan den ansvariga revisorn och ansvariga inom utfärdarverksamheten, i syfte att garantera revisorns oberoende gentemot utfärdarverksamheten.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.9

Svar 9.3 – Beskrivning av revisorns förhållande till den granskade parten:

9.4 Åtgärder vid upptäckt av brist

Utfärdaren ska redogöra för hur upptäckta brister kommuniceras och hur lämpliga förbättringsåtgärder utvecklas och införs.

Styrande krav i Tillitskrav för Valfrihetssystem 2017 E-legitimering: K2.4, K2.9

Svar 9.4 – Beskrivning av åtgärder vid upptäckt av brist: