ÄRENDENUMMER: 2019-278

Vägledning till uppfyllande av tillitsramverkets krav för kvalitetsmärket Svensk e-legitimation

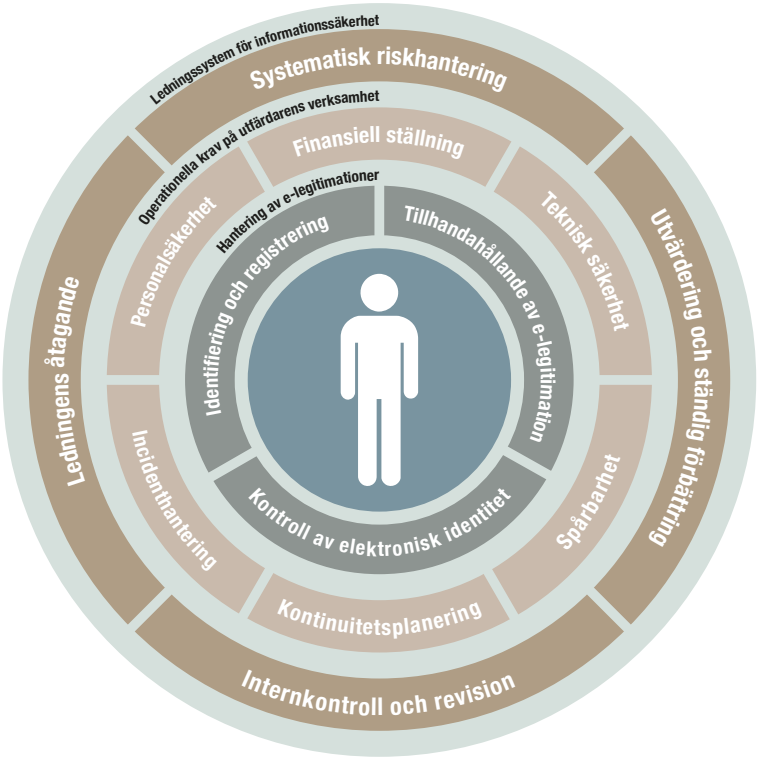
Version 2019-09-19

1. Inledning

Tillitsramverket för kvalitetsmärket Svensk e-legitimation syftar till att etablera gemensamma krav för utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation. Kraven, som vilar på internationella standarder och erkända och etablerade principer, 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 en person som tilldelas en elektronisk legitimationshandling verkligen är den han eller hon utgett sig för att vara.
Kraven formuleras enligt en allmänt vedertagen modell för elektronisk identifiering, där hanteringen av e-legitimationen delas in i tre olika faser;

1. Ansökan och fastställande av sökandens identitet;
2. Utfärdande och tillhandahållande av e-legitimationshandling; och
3. Verifiering av e-legitimation och utställande av identitetsintyg.

I var och en av dessa faser krävs särskilda åtgärder för att upprätthålla den angivna skyddsnivån för hanteringen av e-legitimationer. De områden inom vilka krav ställs redovisas översiktligt i följande figur.



Tillitsnivåerna är definierade utifrån en konsekvensbaserad modell för riskbedömning. Modellen är indelad i graderna begränsade, måttliga, betydande och allvarliga – det vill säga fyra nivåer. Valet av tillitsnivå för en

e-tjänst görs genom en avvägning utifrån sex riskområden och vad en felaktig legitimering skulle kunna föra med sig för negativa konsekvenser.

Tabellen ska läsas så att respektive tillitsnivå möter en viss riskprofil, där riskerna inom vart och ett av de angivna områdena inte får överstiga den angivna konsekvensgraden. Risker kan naturligtvis förekomma inom flera områden, och det är inte osannolikt att en felaktig identifiering kan leda till negativa konsekvenser inom flera områden. Det blir då det område inom vilket de svåraste konsekvenserna kan förekomma som blir styrande för vilken tillitsnivå som krävs. Förekomst av flera risker inom olika områden avses alltså som huvudregel inte räknas som kumulativa.
Konsekvensgraderna överensstämmer även med de nivåer som Myndigheten för samhällsskydd och beredskap (MSB) definierat i skriften *Modell för klassificering av information*. Till dessa nivåer har emellertid i riskbedömningsmodellen tillförts den lägre graden *begränsade* konsekvenser, i syfte att helt överensstämma med de internationella och vedertagna principer som råder inom området. Av samma anledning förekommer i modellen tillitsnivå 1 som svarar mot en elektronisk identifiering där användarens verkliga identitet inte är verifierad. Denna tillitsnivå har ingen motsvarighet i tillitsramverket, då den inte utgör en legitimation i verklig mening.
För kvalitetsmärket Svensk e-legitimation på tillitsnivå 3 är avsikten att den ska ge motsvarande skyddsnivå som den traditionella fysiska legitimationshandlingen, samtidigt som en sådan e-legitimation ska kunna tillhandahållas och användas på ett så effektivt sätt som möjligt. Det är också denna nivå av tillit som dagens e-legitimationer normalt uppfattas nå upp till.
Tillitsnivå 2, som något förenklat avses motsvara det skydd en kod förmedlad via reguljär postgång ger, ska kunna användas vid enklare ärenden där personlig kod i många fall redan idag används. Exempel på sådan enklare

identifiering är godkännande av deklaration via telefon eller mobilapplikation, ställa av eller på fordon, se sammandrag av trängselskattebeslut, et cetera.
För tillitsnivå 4 tillkommer ytterligare krav på skydd vid utgivning och hantering i övrigt, och avses svara mot de högsta skyddsbehoven. De centrala delarna av denna tillkommande kravställning är att utgivning eller förnyelse aldrig kan ske på distans, särskilt stringenta krav på utfärdarens internkontroll samt krav på fysiskt skydd av e-legitimationshandlingen (t.ex. koddosa eller aktivt kort).
De svenska tillitsnivåerna 2, 3 och 4 svarar mot eIDAS tillitsnivåer *låg*, *väsentlig* och *hög*.

Målgrupp och syfte

Denna skrift syftar till att utgöra den vägledning som både leverantörer och Myndigheten för digital förvaltnings (DIGG) granskningsgrupp har till stöd för att avgöra kravuppfyllnad från tid till annan. I vägledningen ges utrymme för att på en mer detaljerad nivå beskriva syfte och innebörd av respektive bestämmelse i tillitsramverket, samt ge exempel på hur den avsedda skyddsnivån kan uppnås. Vägledningen belyser också tekniska säkerhetsaspekter som är av sådan karaktär att de kan tänkas ändras förhållandevis ofta eller med kort varsel.
Det bör därför noteras att vägledningen är ett levande dokument som förväntas uppdateras i takt med teknikutveckling, omvärldskrav och förändrade risknivåer.

2. Organisation och styrning

Övergripande krav på verksamheten

K2.1 Utfärdare av e-legitimation med kvalitetsmärket 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 e-legitimation med kvalitetsmärket 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 e-legitimation med kvalitetsmärket Svensk e-legitimation.

K2.3 Utfärdare av e-legitimation med kvalitetsmärket 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.

Bestämmelserna i denna del syftar till att säkerställa att utfärdare har en stabil ekonomisk och finansiell ställning som är tillräcklig för att DIGG, förlitande parter och innehavare av e-legitimation med kvalitetsmärket

Svensk e-legitimation ska kunna fästa tillit till verksamhetens stabilitet och kontinuitet, samt att utfärdaren kan hållas ansvarig vid eventuella upptäckta brister.
Gällande kraven på erforderliga försäkringar i K2.1, så avses sådana försäkringar som är nödvändiga för att säkerställa verksamhetens fortlevnad och kontinuitet vid extraordinära händelser. Om utfärdarens finansiella ställning är sådan att försäkringar inte behövs för att täcka skador som kan tänkas uppkomma (t.ex. genom plötsliga händelser eller att utfärdaren har befunnits skadeståndsskyldig), kan alltså kravet på försäkringar lämnas utan avseende. Bestämmelsen K2.2 innebär att leverantören, redan en granskningsaktivitet inleds, ska kunna visa på komplett kravuppfyllnad. Det ska vara möjligt att via revisionsspår följa att samtliga kontroller är införda och är effektiva. I en nyetablerad verksamhet kan det naturligtvis vara så att inga kunder i verklig mening finns anslutna till tjänsten. Då ska tjänstens kravuppfyllnad åtminstone kunna verifieras via ett rimligt antal pilotanvändare som fungerat i tillräckligt lång tid för att revisionsspår till respektive kontroll ska ha uppstått.
Kravet i K2.3 avser alltså inte reglera utfärdarens eventuella skadeståndsansvar, utan enbart utfärdarens förmåga att bära risken för sådan skadeståndsskyldighet.

Informationssäkerhet

K2.4 Utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation ska för de delar av verksamheten som berörs i tillitsramverket 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 med kvalitetsmärket Svensk 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 med kvalitetsmärket 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 e-legitimation med kvalitetsmärket 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 e-legitimation med kvalitetsmärket Svensk 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 med kvalitetsmärket ska regelbundet utvärdera informationssäkerhetsskyddet och införa förbättringsåtgärder i ledningssystemet och säkerhetskontroller.

K2.5 Ledningssystemets omfattning och mognadsgrad

Nivå 4: Ledningssystemet för informationssäkerhet ska följa SS-ISO/IEC 27001:2014 eller därmed jämställbara internationella versioner av standarden, och inom avgränsningen för detta inkludera samtliga krav som ställs på utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation.

Kraven i K2.4 tar fasta på styrning, kontroll och uppföljning av informationssäkerhetsarbetet. Till stöd för detta bör ledningssystemstandarden ISO/IEC 27001 användas, men aktörer som implementerat likvärdiga principer för ledning och styrning av informationssäkerhetsarbetet, och som fyller bestämmelsens syfte, kan också godtas. Centralt för kravuppfyllnad är att ledningen gett bevis på sitt åtagande för att upprätta, införa, driva, övervaka, granska, underhålla och förbättra ledningssystemet, att processerna för varje steg är dokumenterade och planerade, samt att erforderliga resurser för att genomföra detta är tillsatta.
Ledningssystemets omfattning och tillämplighet ska vara dokumenterad och beslutad av ledningen genom ett *uttalande om tillämplighet* (*statement of applicability*) eller motsvarande dokument. Särskilt ska de ovan uppräknade punkterna innefattas inom ramen för ledningssystemet och dess kontroller.
Processen för riskanalys ska vara dokumenterad och tillämpad, och ska bygga på en riskanalysmetodik som ger konsistenta, korrekta och jämförbara resultat. Processen ska innefatta att också utforma, införa och följa upp risklindrande åtgärder, samt utverkande av riskägarens godkännande av kvarvarande risk. Resultatet av sådana riskanalyser ska bevaras för att möjliggöra uppföljning och internrevision.
För aktörer som levererar tjänster enligt tillitsnivå 4 ska ledningssystemet fullt ut leva upp till kraven i ledningssystemstandarden SS-ISO/IEC 27001:2014 eller motsvarande internationella versioner av standarderna. Kravuppfyllnad på denna nivå kan styrkas genom certifiering av ledningssystemet, genomförd av ackrediterad revisor. Om alternativa standarder eller principer tillämpas ska en analys av överensstämmelse

mellan standarderna vara genomförd, för att klargöra att inga väsentliga avvikelser förekommer.

Villkor för underleverantörer

K2.6 En utfärdare av e-legitimation med kvalitetsmärket 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.

Även om utfärdare lägger ut utförandet av vissa delar på en eller flera underleverantörer, så ansvarar utfärdaren för dessa som för egen verksamhet. Det avses innefatta samtliga krav som följer av anslutningsavtalet, bland annat DIGG bereds samma möjlighet till insyn i underleverantörs verksamhet som i den egna.
Bestämmelsen K2.6 syftar dock till att i första hand klargöra dessa eventuella underleverantörsförhållanden. Vilka underleverantörer som ansvarar för vilka delar ska bland annat belysas för att DIGG ska kunna bedöma om det kan finnas några sårbarhetsaspekter i användandet av en leverantör, möjligen genom att flera andra utfärdare använder samma underleverantör för utförandet av en likartad tjänst.

Spårbarhet, gallring och handlingars bevarande

K2.7 Utfärdare av e-legitimation med kvalitetsmärket 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, dokumentation och övriga uppgifter som styrker efterlevnaden av de krav som ställs på utfärdare av e-legitimation med kvalitetsmärket Svensk 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 ur integritetssynpunkt och har stöd i lag eller annan författning.

Bestämmelserna i denna del syftar till att säkerställa spårbarhet i utfärdarens verksamhet samt möjlighet till uppföljning av kravuppfyllnad.

Spårbarheten är även viktig för möjlighet till uppföljning av eventuella incidenter.
Kravet i K2.7(c) bör läsas så att det innefattar att registrera och bevara spår från alla från sådana händelser som kan vara av relevans för uppföljning. Det innefattar särskilt att de tekniska system utfärdaren använder för att leverera funktionaliteten registrerar sådana händelser i en säkerhetslogg. I termen bevara bör också inläsas att den information som ska bevaras skyddas mot förvanskning och obehörig insyn.
Att information ska kunna tas fram i läsbar form under hela dess arkiveringstid innebär att information som lagras elektroniskt, ska lagras i sådant format och på sådant lagringsmedia, att det är rimligt säkerställt att den utrustning och programvara som krävs för att återsöka och återläsa informationen finns tillgänglig 10 år efter att informationen en gång lagrades i mediet. Kravet omfattar även uppgifter som lagrats i traditionell form på papper.

Granskning och uppföljning

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

Utfärdare ska upprätta en revisionsplan som sträcker sig över cirka 3 år och omfattar hela det avgränsade området som anges i K2.9. Särskilt kritiska säkerhetskontroller bör identifieras i denna revisionsplan, och vara föremål för återkommande granskning varje år.
Revisionen bör i normalfallet utföras av en oberoende intern kontrollfunktion, där oberoende innebär att denne inte är involverad i den löpande driften och förvaltningen av den tillhandahållna tjänsten. I mindre verksamheter kan det av resursskäl vara svårt att vidmakthålla en sådan förmåga inom organisationen, varför det kan vara försvarbart att låta en (oberoende) externt anlitad funktion utföra den regelbundna granskningen. I många fall kan den huvudansvarige revisorn behöva tekniskt stöd för att verifiera efterlevnad av tillitsramverkets alla delar. Även sådan teknisk stödfunktion anses kräva ett oberoende för att kunna göra en objektiv och skärskådande granskning.

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.

Alla verksamhetsställen som inhyser utrustning eller informationsbärande media där känsliga uppgifter behandlas eller lagras (tillfälligt eller mer permanent) anses kräva ett omfattande och heltäckande fysiskt skydd för att förhindra informationsförlust eller röjande av sådana känsliga uppgifter till obehöriga.
Det fysiska (mekaniska) skyddet ska vara så pass fördröjande att det reaktiva skyddet (t.ex. skalskydd och försåtsskydd) kan verka genom att påkalla uppmärksamhet från bevakningsbolag, polis, etc., som i sin tur hinner avvärja intrånget. En mer avlägsen driftanläggning kan därför anses kräva ett starkare mekaniskt skydd, jämfört med en driftanläggning där väktare finns till hands dygnet runt.
Det fysiska skyddet bör inordnas i lager av stegvis högre säkerhetsgrad. Enligt detta resonemang bör utrymmen för utrustning som lagrar t.ex. kryptografiskt nyckelmaterial placeras i sådana inre lager som åtnjuter den högsta graden av skydd, och dit endast den personal har tillträde som oundgängligen behöver det för att kunna fullgöra sina arbetsuppgifter
De normer som utarbetats av Svenska Stöldskyddsföreningen (SSF), kan utnyttjas av utfärdare för att dimensionera mekaniskt inbrottsskydd och inbrottslarm för skyddade utrymmen. Det mekaniska inbrottsskyddet bör då som regel uppfylla SSF 200 skyddsklass 2, och ha ett larmskydd som uppfyller SSF 130 larmklass 2.

K3.2 Innan en person antar någon av de roller som identifierats i enlighet med K2.4K2.4(a), och som är av särskild betydelse för säkerheten, ska utfärdaren av e-legitimation med kvalitetsmärket 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 tillfredsställande, korrekt och säkert sätt utföra de arbetsuppgifter som följer av rollen.

Utfärdare ska särskilt identifiera de roller som har möjlighet att åsidosätta säkerhetskontroller som innebär att falska elektroniska legitimationshandlingar eller identitetsintyg kan utfärdas. Personer som antar en sådan roll ska ha genomgått bakgrundskontroll. Det är dock inte fråga om registerkontroll enligt säkerhetsskyddsförordningen, varför utdrag ur belastningsregistret inte heller bör vara en del av bakgrundskontrollen.
Utfärdaren förväntas inrätta en egen process för bakgrundskontroll med lämplighetsprövning som kan innefatta verifiering av akademiska meriter, tidigare anställningar, kontakt av både angivna och icke-angivna referenspersoner, samt göra en ekonomisk riskbedömning av personen.
Delar av prövningen kan behöva upprepas med vissa intervall, vilket även bör framgå av den process man dokumenterar. Personal som sedan länge varit anställd hos utfärdaren och visat sig pålitlig behöver inte genomgå

förnyad bakgrundskontroll, utöver den del som eventuellt regelbundet upprepas enligt det föregående.

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.

De uppgifter som ska samlas in och bevaras i enlighet med K2.7 innefattar behandlingshistorik som registreras i säkerhetslogg från de aktuella systemen. Uppgifterna kan också vara av integritetskänslig karaktär. Säkerhetsloggen ska kunna användas för att genomföra regelbunden och systematisk uppföljning och kontroll, i syfte att säkerställa att otillåten åtkomst till system och information inte förekommit.

Utfärdare ska därför säkerställa att den personal som har tillgång till den tekniska systemmiljön inte har tillgång till säkerhetsloggen, och att det alltså i denna del finns en separation av arbetsuppgifter.

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.

För tillitsnivå 3 och 4 ställs särskilt rigorösa krav kring separation av arbetsuppgifter i verksamheten. Inte i något led ska en enskild individ ensam kunna kringgå, upphäva eller annars åsidosätta säkerhetskontrollerna på ett sådant sätt att denne kan tillskansa sig en e-legitimationshandling (inklusive aktiveringskod) i en annan persons namn.
Detta innefattar att ordna rutiner, processer och den tekniska infrastrukturen på ett sådant sätt att missbruk av kritiska komponenter inte kan förekomma utan att flera personer agerar i samförstånd. Särskilt kritiska delar utgörs naturligtvis av tillhandahållandet av e-legitimationshandlingen, där särskilda bestämmelser gäller i enlighet med K6.6 – K6.7. Kravet omfattar dock även möjlighet till missbruk av det systemstöd som omgärdar utfärdarverksamheten. Kritiska komponenter utgörs vanligen av nyckelmaterial som krävs för kommunikation mot utfärdarsystem, utfärdarsystemet i sig samt de lagringssystem och databaser som utfärdarsystemet nyttjar.

4. Teknisk säkerhet

K4.1 Utfärdare av e-legitimation med kvalitetsmärket 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.

Tekniska styrmedel och kontroller ska tillämpas för att säkerställa integritet, sekretesskydd, tillgänglighet och spårbarhet i de system och i den information som systemen behandlar. Kontrollernas effektivitet ska regelbundet utvärderas som del i förbättringsarbetet.
Förutom de tvingande åtgärder som anges i K4.2-K4.4, ska utfärdaren utforma och införa de skyddsåtgärder denne anser vara lämpliga och tillräckliga mot bakgrund av riskanalysen och de uppsatta riskacceptanskriterierna. Principer som bör tillämpas är djupledsförsvar och överlappande säkerhetsåtgärder. Detta innefattar bl.a. krypteringsåtgärder, styrmedel för nätverkskommunikation i flera nivåer och restriktiv åtkomstkontroll till systemresurser och informationstillgångar.

Riskanalysen förväntas i förekommande fall även identifiera identitetsintygsfunktionen (avsnitt 8 i tillitsramverket) som särskilt utsatt för risk, då denna i normalfallet har en hög exponeringsgrad samtidigt som säkerhetsberoendet till denna är mycket stort. Särskilt rigorösa tekniska säkerhetskontroller och kvalitetssäkringsrutiner förväntas därför omgärda denna del, som alltså även omfattas av kraven i K4.1, om sådan identitetsintygsfunktion tillhandahålls av utfärdaren.

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

Säkerhetskritisk kommunikation till-, från- eller mellan fysiskt skyddade utrymmen kräver skydd mot avlyssning och förvanskning. Vanligen är det effektivare att tillämpa starka kryptografiska metoder för att skydda sådan kommunikation, snarare än att fysiskt skydda anslutningarna längs hela deras sträckning. Skydd av kommunikation avses kunna tillämpas både som skydd av meddelanden eller som skydd endast under transport (transportskydd). Det krävs dock alltid att de kommunicerande parternas identitet är ömsesidigt säkerställd. Autentiseringsmekanismen och hanteringen av de uppgifter som ligger till grund för autentiseringen måste säkerhetsmässigt motsvara minst samma skyddsnivå som de e-legitimationer som systemet hanterar.

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

Med kryptografiskt nyckelmaterial avses här sådant nyckelmaterial som används för att utfärda e-legitimationer, autentisera användare samt utfärda identitetsintyg enligt K8.1. Nyckelmaterial som till exempel används i nätverksutrustning och för skydd av kommunikation avses inte omfattas av kraven.
Sådant nyckelmaterial som omfattas av kraven i K4.3, ska skyddas genom användande av kryptografisk hårdvarumodul som erbjuder såväl logiskt som fysiskt skydd. Hårdvarumodulens säkerhetsfunktioner ska vara trovärdiga, innebärande att de ska vara baserade på välkända standarder och principer, samt vara genomlysta av erkänt och fristående granskningsorgan. I det är det lämpligt att använda produkter som är certifierade enligt t.ex. Common Criteria (ISO/IEC15408)[1], ISO/IEC 19790:2006 eller FIPS 140-2 (nivå 3 eller högre).
Åtkomst till hårdvarumodulerna och den tekniska och fysiska omgivning där de finns installerade ska begränsas till de personer vars arbetsuppgifter kräver det. För nivå 3 och uppåt ska aktivering av nyckelmaterialet ske genom minst två personer i förening.
I vissa särskilda fall kan det vara motiverat att låta göra de kryptografiska operationerna utanför säkerhetsmodulens skyddade omgivning. Detta kan vara aktuellt för lösningar som bygger på engångskoder, och där det saknas stöd i hårdvarumodulen för att verifiera sådana engångskoder. I sådana fall ska nyckelmaterialet då det inte används lagras krypterat, och säkerhetsmodulen användas för att tillgängliggöra detta nyckelmaterial i

[1] Vid produktcertifiering enligt Common Criteria (ISO/IEC15408) avses att detta ska göras gentemot en för ändamålet utformad skyddsprofil (PP), t.ex. CWA 14167-2, av ett certifieringsorgan erkänt inom Common Criteria Recognition Arrangement (CCRA) och/eller Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA).

klartext just i den stund då det behövs, för att sedan på ett säkert sätt låta utplåna uppgifterna från minnet.

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

Bestämmelsen omfattar de ingående IT-systemens hela livscykel, från utveckling eller anskaffning, till konfiguration, drift, ändring och avveckling. Samtliga dessa delar ska vila på en formell dokumenterad grund. IT-systemet och dess omgivning ska övervakas för att på ett tidigt stadium kunna upptäcka avvikelser och anomalier. Processer ska inrättas som säkerställer kontinuerlig omvärldsbevakning och att omedelbara preventiva och reaktiva åtgärder kan vidtas som svar på förändrade risknivåer eller uppkomna incidenter.

5. Ansökan, identifiering och registrering

Information om villkor

K5.1 Utfärdare av e-legitimation med kvalitetsmärket 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 e-legitimation med kvalitetsmärket Svensk e-legitimation ska tydligt hänvisa till villkoren och utforma rutinerna så att villkoren kommer sökanden tillhanda innan denne ingår avtal med utfärdaren.

Utfärdare ska hålla avtal, villkor och anknytande uppgifter enkelt tillgängliga för allmänheten att ta del av, lämpligen via utfärdarens webbplats.
Det är också viktigt att tjänstens villkor kommer sökanden tillhanda innan denne accepterar att använda tjänsten. Detta förfarande kan utformas på olika sätt beroende på hur ansökningsproceduren i övrigt är utformad. Regeln ska inte anses kräva en brevväxling eller namnunderskrift, dock bör det vid ett minimum ske genom ett aktivt acceptansförfarande, t.ex. en kryssruta vid begäran/ansökan om att få en e-legitimation. Regeln gäller även vid ändring av villkoren.

K5.3 Utfärdare av e-legitimation med kvalitetsmärket 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 utgivning, spärr och avveckling,

(c) villkor förknippade med den tillhandahållna tjänsten, innefattande användarens skyldigheter att skydda sin elektroniska identitet, 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 utfärdardeklarationen, villkor eller andra förutsättningar för den tillhandahållna tjänsten.

Utgångspunkten för en utfärdardeklaration bör vara att en utfärdare på en övergripande nivå ska beskriva de tjänster som denne tillhandahåller för en intresserad allmänhet, men ska samtidigt inte beskriva förhållanden på en sådan detaljnivå att dokumentet riskerar röja affärshemligheter eller andra delar som kan anses utgöra en säkerhetsrisk.

K5.4 **Nivå 3 och 4:** Utfärdare av e-legitimation med kvalitetsmärket 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.

På begäran av en avtalspart som förlitar sig på av utfärdaren tillhandahållna tjänster ska en utfärdare av Svensk e-legitimation kunna redogöra för ägarstrukturer och principer för organisationens bolagsstyrning.
I en sådan redogörelse bör bl.a. innefattas:

- organisationsstruktur, enheter, affärsområden, dotterbolag, utlokaliserade verksamheter och intressen i samriskbolag,
- koppling mellan ersättning till styrelseledamöter, ledande befattningshavare och chefer och organisationens resultat,
- om och i så fall hur den s.k. försiktighetsprincipen tillämpas, samt
- en beskrivning av de rutiner som tillämpas inom styrelsen för att säkerställa att inga intressekonflikter uppstår.

K5.5 En utfärdare av e-legitimation med kvalitetsmärket Svensk 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.

Den skyldighet som följer av anslutningsavtalet och punkterna K2.7 och K2.8 i tillitsramverket, gäller även efter att anslutningen upphört. Av det följer att denna information ska hållas tillgänglig och ska kunna tas fram i läsbar form minst 10 år från det att informationen skapades.

Ansökan

K5.6 En e-legitimation med kvalitetsmärket 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 komma att 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 e-legitimation med kvalitetsmärket Svensk e-legitimation ska knytas till personnummer eller samordningsnummer, samt de uppgifter som i övrigt är nödvändiga för att utfärdaren av en e-legitimation med kvalitetsmärket Svensk e-legitimation ska kunna tillhandahålla sådan e-legitimation.

Ansökningsförfarandet kan komma att se olika ut beroende på tillitsnivå och om ansökan sker på distans eller vid personligt besök. Det är vanligt att ansökan sker i formen av en begäran från användarens sida att erhålla en e-legitimation, snarare än att ett ansökningsformulär fylls i med sökandes uppgifter som sedan lämnas till utfärdaren.
Bestämmelsen syftar till att utfärdande av e-legitimation ska göras på användarens initiativ. Användaren ska göras uppmärksam på att en e-legitimation tillhandahålls denne, på vilka villkor detta sker och vilket ansvar som kommer komma att vila på användaren.
Syftet är att motverka situationer där användare per automatik tilldelas en e-legitimation, kanske utan att situationen står helt klar för användaren att så skett. En sådan situation skulle kunna vara om användaren upplever att denne t.ex. har ett kundkort av tämligen begränsat värde i handen, men att detta också är en legitimationshandling. Samma situation skulle kunna gälla en mobiltelefon, en koddosa, eller något annat. Det är viktigt att det även i användarens ögon tydliggörs om en e-legitimation kopplas på detta sätt.
Att regeln anger att det ska ske i skriftlig form är för att underlätta uppföljning. Det står dock klart att syftet med regeln är uppfyllt även vid ett förfarande där användaren på begäran presenteras villkoren i skrift, och där

denne (vid ett minimum) godtar villkor och bekräftar dennes uppgifter via ett acceptförfarande.
I vissa situationer, t.ex. om e-legitimationer utfärdas till personer med funktionshinder, kan dock ansökan i verbal form vara acceptabel om hela konversationen spelas in och bevaras. Detta kan dock behöva förenas med ytterligare krav, varför det hanteras som undantag som ska bedömas från fall till fall.
Utgivning som syftar till att ersätta till exempel en spärrad e-legitimation, eller för att tillhandahålla en ny teknisk lösning, avses inte kräva ett sådant ansökningsförfarande, utan kan genomföras på utfärdarens initiativ.

Fastställande av sökandens identitet

K5.8 Utfärdare av e-legitimation med kvalitetsmärket 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.

Det ska säkerställas att de uppgifter som utgivningen av e-legitimationen grundas på överensstämmer med uppgifter registrerade i ett officiellt register. Om utgivning sker i en befintlig kundrelation, då dessa uppgifter inhämtats vid ett tidigare tillfälle, så ska uppgifternas aktualitet verifieras mot ett officiellt register. Uppgifter anses vara aktuella om de är inhämtade i enlighet med K5.13. Som officiellt register räknas bland annat SPAR, men motsvarande tjänst från t.ex. ett kreditupplysningsinstitut anses även uppfylla kraven.

K5.10 Identifiering av sökanden vid personligt besök

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

Kravet på ursprungsidentifiering på likvärdigt sätt som vid utfärdande av en fullgod identitetshandling innebär att identifieringen genomförs med stöd av en dokumenterad process och av särskilt utbildad personal i betrodd ställning inom utfärdarens organisation. Det förväntas också att identitetskontrollen i samband med utgivningen av e-legitimationen grundas i att sökanden redan har en fullgod identitetshandling med vilken denne kan styrka sin identitet. Som fullgod identitetshandling räknas svenskt körkort, svenskt pass i vinröd bok, SIS-märkt ID-kort (av DNV certifierat tjänste- och ID-kort), nationellt ID-kort samt Skatteverkets ID-kort.
De olika bestämmelser som tillämpas för utgivning av ID-kort till personer som saknar fullgod identitetshandling bör alltså i normalfallet inte tillämpas

för utgivning av e-legitimation. Saknas fullgod identitetshandling bör det därför tillsvidare förutsättas att sökanden skaffar sådan, innan utgivning av e-legitimation kan ske.
Det bör i detta sammanhang också särskilt noteras att den legitimationskontroll som förväntas följa vid utlämnande av rekommenderat brev, inte anses uppfylla kraven för utgivning av fullgod identitetshandling. I detta ämne skrev Id-kortsutredningen i sitt betänkande (SOU 2007:100) *Id-kort för folkbokförda i Sverige* följande: *"Det är vanligt att andra företag tillhandahåller Posten utlämningsställen för privatpersoner, som t.ex. mataffärer. Dessa är emellertid knappast lämpliga som utfärdandeplatser för id-kort."*.
Identifiering genom rekommenderat brev kan dock användas som del i att upprätta en sådan distansrelation som avses i K5.11 nivå 3, där det rekommenderade brevet kombineras med tillkommande kontroller för att säkerställa trovärdigheten i identifieringen, vilket alltså förutsätts läggas till grund för upprättandet av den relation som rör ekonomiskt eller rättsligt betydelsefulla mellanhavanden som avses i nämnda bestämmelse.

K5.11 Identifiering av sökanden på distans

Nivå 2: Utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation som identifierar sökanden på distans, ska identifiera sökanden genom att tillhandahålla e-legitimationshandlingen i enlighet med K6.6 Nivå 2.

Nivå 3: Utfärdare av e-legitimation med kvalitetsmärket 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.

För att kunna ge ut e-legitimationer på nivå 3 på distans, krävs att utfärdaren själv står en betydande rättslig eller ekonomisk risk kopplad till distansrelationen. Detta innebär i normalfallet att utfärdaren tillhandahåller en e-tjänst gentemot sökanden, där konsekvenserna för utfärdaren vid en felaktig identifiering kan komma att leda till betydande skador. Konsekvensgraderna vid en felaktig identifiering ska motsvara de som anges för tillitsnivå 3 i figur 1.

Figur 1 - Konsekvensgrader per tillitsnivå

Bestämmelsen K5.11 gör det alltså möjligt för vissa aktörer att ge ut e-legitimation på nivå 3 på distans, via t.ex. bank på Internet, utan att kraven på identifiering genom fullgod identitetshandling enligt K5.10 med nödvändighet varit uppfyllda vid den ursprungliga identifieringen av sökanden.
Det kan konstateras (SOU 2007:100, s. 41) att det förekommer att t.ex. en bank som har en relation med en utländsk kund, då denne har ett svenskt personnummer, som grund för identifieringen godtar vissa utländska pass. För sådana situationer bör en särskilt restriktiv bedömning göras av den ekonomiskt eller rättsligt betydelsefulla relationen. Särskild vikt måste också fästas vid att i sådana situationer upprätthålla kraven i K6.4, och alltså säkerställa att sammanblandning mellan två personer inte kan förekomma. Om sådana rutiner tillämpas bör dessa rutiner också redovisas i samband med utfärdarens ansökan.

K5.12 Identifiering genom annan e-legitimation med kvalitetsmärket Svensk e-legitimation

Nivå 2 och 3: En utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation får, utöver vad som angetts i K5.11 Nivå 3, även identifiera sökanden på distans genom annan e-legitimation med kvalitetsmärket Svensk e-legitimation på minst tillitsnivå 3, om denne utan avtalsrättsliga hinder kan lägga sådan identifiering till grund för utfärdande av en ny e-legitimation.

Nivå 4: Ej tillämpligt.

En utfärdare som kan identifiera sökanden på distans genom annan e-legitimation med kvalitetsmärket Svensk e-legitimation av minst tillitsnivå 3,

får utfärda en ny e-legitimation baserad på denna identifiering. Detta under förutsättning att eventuella förlitandeavtal tecknade med utgivaren av den ursprungliga e-legitimationen inte förhindrar sådan identitetsväxling. Bestämmelsen medger också att en utfärdare, som annars inte skulle omfattas av det distansförfarande som beskrivs i K5.11 Nivå 3, på distans förnya en av denne tidigare utgiven e-legitimation.
Regeln är inte tillämplig på nivå 4, då identifiering av sökanden på denna nivå alltid ska ske vid personligt besök.

Registrering

K5.13 Utfärdare av e-legitimation med kvalitetsmärket 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.

Det förväntas att utfärdare håller grundläggande personuppgifter knutna till anslutna innehavare i eget register för att kunna fullfölja de förpliktelser som följer av tillitsramverket. Detta register ska hållas aktuellt och bör uppdateras med förändringar från officiellt register varje helgfri vardag. Identitetsintyg som lämnas enligt K7.1 ska grundas i dessa uppgifter, snarare än eventuella uppgifter lagrade i själva e-legitimationshandlingen. Om personuppgifter lagras i e-legitimationshandlingen, bör även dessa hållas aktuella. Vid förändring bör sådana uppgifter förnyas inom 30 dagar. Om inte så skett bör e-legitimationshandlingen spärras.
Utfärdaren är normalt personuppgiftsansvarig för de uppgifter som samlas in och lagras i registret, samt för de i övrigt tillkommande uppgifter som behandlas och kan knytas till fysiska personer. Sådan behandling måste följa bestämmelserna i personuppgiftslagen (1998:204). Generellt kan sägas att de rättsliga förpliktelser som följer av personuppgiftslagen innebär att en utfärdare som behandlar personuppgifter ska, baserat på riskerna som är förknippade med behandlingen, göra en samlad bedömning av riskerna som behandlingen medför och införa en väl avvägd säkerhetsnivå. Vidare ska endast de personuppgifter samlas in som är nödvändiga för ändamålet, och sparas endast så länge som de behövs.

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.

Det finns tre huvudkategorier av så kallade autentiseringsfaktorer; *"något man vet"* (i praktiken koder), *"något man är"* (biometriska egenskaper) eller *"något man har"* (t.ex. en dator, koddosa, mobiltelefon eller aktivt kort).
Med *koder* avses lösenord, lösenfraser, sifferkombinationer eller annan informationsmängd som inte är knuten till en särskild utrustning eller programvara. Det innebär att innehavaren av sådan e-legitimation ska identifiera sig genom *"något man vet"*.
Innehav eller kontroll över en enhet, utrustning, programvara eller i övrigt någon lagrad datastruktur, dvs. *"något man har"*, är som grundregel inte tillräckligt om endast en autentiseringsfaktor används på grund av risken för plötslig förlust av kontroll över denna del.

- Exempel: Ett s.k. blixt-SMS *("flash SMS"*) till en mobiltelefon är för svagt skydd om det inte kombineras med kod, då SMS-meddelandet enkelt kan avläsas och kvitteras av någon som för tillfället förfogar över mobiltelefonen (ofta utan kännedom om kod för skärmlås, beroende på telefonmodell).

Biometri är inte tillämpligt för identifiering av personer på distans av orsaker som följer av biometrins underliggande egenskaper; inte minst det faktum att biometriska egenskaper inte kan anses vara hemliga. Den grundläggande autentiseringsfunktionen för biometri är förmågan att avläsa biometri från en levande människa genom utrustning som är i direkt kontakt med personen i fråga, och där denna utrustning är tillräckligt säker och tillförlitlig i både att läsa av den biometriska egenskapen och i att avgöra om intrycket är äkta (det vill säga att det härstammar från en människa).
Biometrilösningar kan därför vara ett alternativ eller komplement till aktiveringskod, men kan inte användas som enda autentiseringsfaktor på distans.
För samtliga tillitsnivåer för kvalitetsmärket Svensk e-legitimation krävs flerfaktorsautentisering. Utgångspunkten bör vara att *"koder"* kombineras med innehav av (fysisk kontroll över) en lagrad datastruktur, men andra lösningar kan godtas då säkerheten i övrigt upprätthålls genom andra kompletterande kontroller.
För tillitsnivå 4 ska personlig fysisk säkerhetsmodul användas. En sådan enhet skyddar de kritiska nyckelparametrarna från såväl logiska som fysiska försök att röja dem. Vanligen är det fråga om ett så kallat aktivt kort, men motsvarade funktionalitet kan integreras i till exempel telefoner, klockor och accessoarer. Den personliga säkerhetsmodulen lagrar nyckelmaterialet och utför de kryptografiska operationerna på ett sådant sätt att de kritiska

nyckelparametrarna aldrig lämnar säkerhetsmodulen. Det är lämpligt att sådana enheter har genomgått ett certifieringsförfarande enligt Common Criteria (ISO/IEC15408) gentemot en för ändamålet relevant skyddsprofil.

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

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

Bestämmelsen innebär att komplexitetskraven på den personliga koden måste utformas så att resurserna som krävs för att röja den står i proportion till e-legitimationens övriga säkerhetsegenskaper, innebärande att denna del inte ska vara en svagare länk än någon annan del i kedjan av säkerhetskontroller.
Detta kan åstadkommas på flertalet olika sätt, till exempel:

- I de fall en personlig säkerhetsmodul används, att denna blockeras efter ett visst antal felaktiga aktiveringsförsök, där antalet tillåtna försök står i proportion till aktiveringskodens komplexitet.
- I de fall andra tvåfaktorslösningar än personlig säkerhetsmodul används:
    - Att aktiveringen av e-legitimationshandlingen tar stor maskinkapacitet i anspråk, det vill säga att processen att tillgängliggöra nyckelmaterialet går till så att ett stort antal operationer krävs för att pröva om rätt kod angivits, och att det därmed (i normalfallet) tar orimligt lång tid att genomföra en uttömmande sökning efter rätt kod.
    - Att den personliga kodens komplexitet i termer av längd samt kombination av versaler, gemener, siffror och specialtecken medför att uttömmande sökning blir mycket omfattande resursmässigt att genomföra.
    - Att en del i aktiveringsförfarandet görs direkt mot utfärdaren, och att denne därmed kan spärra den elektroniska identiteten efter ett visst antal felaktiga försök.

E-legitimationshandlingar som uppfyller kraven för tillitsnivå 3 men som inte baseras på en personlig säkerhetsmodul av det slag som nämnts tidigare ska implementera kopieringsskydd för att ytterligare försvåra för utomstående att röja nyckelmaterialet. Detta kan åstadkommas genom att inkludera uppgifter knutna till hårdvaran som del av den underliggande aktiveringskoden. Utöver detta kan man också använda operativsystemfunktioner som förhindrar främmande processer från att läsa det krypterade nyckelmaterialet.

E-legitimationshandlingar som endast ska uppfylla kraven för tillitsnivå 2 får kunna kopieras eller flyttas mellan enheter, då detta i vissa fall kan vara en önskvärd egenskap.
I fråga om en enskild teknisk utformning uppfyller kraven i tillitsramverket ska en samlad bedömning göras, där hänsyn tas till samtliga ovan nämnda aspekter och väga dessa mot de hot som existerar på respektive tillitsnivå.

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.

Denna bestämmelse syftar till att säkerställa att det ska vara enkelt för användaren att byta personlig kod om denne misstänker att den blivit röjd. Ett specialfall av kravuppfyllnad är istället för att användaren på egen hand byter personlig kod, att samma effekt åstadkoms genom att begära spärr av e-legitimationshandlingen och att innehavaren tillhandahålls en ny e-legitimation med ny personlig kod. Detta alternativ får dock inte medföra påtagligt krångel eller ytterligare kostnader för användaren, för att inte riskera att användare avhåller sig från att spärra e-legitimationer vars aktiveringskod kanske blivit röjd.

K6.4 Utfärdare av e-legitimation med kvalitetsmärket 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.

Kravet innebär att varje enskild e-legitimationshandling ska tilldelas en unik identifierare, och att denna ska kopplas entydigt till en fysisk person. Det betyder också att fiktiva personnummer eller samordningsnummer inte får förekomma, och att det heller inte får förekomma situationer där en sammanblandning av två e-legitimationshandlingars identifierare (el. motsv.) är möjlig.

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.

Giltighetstiden för utgivna e-legitimationer ska begränsas till att gälla i maximalt 5 år. Det är emellertid rimligt att begränsa giltighetstiden ytterligare, särskilt för de typer av e-legitimationer vars nycklar eller koder

över tid löper större risk att röjas till obehöriga. Detta gäller i första hand enfaktorsautentisering med personlig kod samt e-legitimationshandlingar som inte baseras på en personlig säkerhetsmodul. Dessa typer av e-legitimationshandlingar bör förnyas genom att grunden för identifieringen (koder, nyckelmaterial) byts ut på regelbunden basis.
Även e-legitimationer som baseras på personlig säkerhetsmodul ska dock begränsas i giltighetstid, men får förlängas genom ett återverifieringsförfarande i vilket användaren bekräftar för utfärdaren att denne fortfarande har den personliga säkerhetsmodulen under sin kontroll (inom giltighetstiden). Syftet är att säkerhetsmoduler som kommit på avigvägar tids nog spärras och därmed avregistreras.

Tillhandahållande av e-legitimationshandling

K6.6 Tillhandahållande på distans

Nivå 2: En utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation ska tillhandahålla e-legitimationshandlingen på ett sätt som bekräftar kontaktuppgifter förda i officiellt register.

Nivå 3: En utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation som tillhandahåller e-legitimation via elektroniskt förfarande som är förenligt med K5.11 Nivå 3 eller K5.12 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: ej tillämpligt.

K6.7 Tillhandahållande vid personligt besök

En utfärdare av e-legitimation med kvalitetsmärket 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.

Tillhandahållandet av e-legitimationshandlingen är en särskilt kritisk fas i utgivningsprocessen. Bestämmelserna i denna del syftar till att förhindra eller försvåra identitetsstöld. Allt eftersom spridningen och användningen av e-legitimationer ökar, kan också riskerna för identitetsstöld förväntas öka. Konsekvenserna för den drabbade är ofta påfrestande och långdragna.

Tillhandahållandesätt som involverar två säkerhetsmässigt separata kanaler är en möjliggörare för flera säkerhetshöjande kontroller. Genom att grunda en del av tillhandahållandet i uppgifter som registreras eller verifieras oberoende av registraturen, och som därvid inte kan förändras eller kontrolleras av en person i denna funktion, minskas det säkerhetsmässiga beroendet till enstaka personer inom registraturfunktionen. Syftet är att i första hand lindra:

- personalrelaterade risker i registraturfunktionen, där en person under hot eller av andra orsaker försöker erhålla en e-legitimation i en annan persons namn, och
- risker som härrör till brister i identifieringen av sökanden; till exempel genom förfalskade ID-handlingar vid personligt besök, eller på distans genom andra typer av bedrägliga metoder, bland annat innefattande nätfiske, missbruk av annans elektroniska ID-handling, intrång eller manipulation av IT-system, med mera.

Används utgivningskontor eller andra utlämningsställen i ett utgivningsförfarande som baseras på personligt besök, kan kravet på tillhandhållande genom två separata kanaler åstadkommas genom en separation av arbetsuppgifter i registraturfunktionen.
Sker utgivningen automatiserat och helt på distans, uppstår inte personalrelaterade risker på samma sätt. Vid distansutgivningsförfarandet är det istället de mer IT-relaterade riskerna som behöver hanteras. Då en sådan helt automatiserad metod ofta innebär att såväl e-legitimationshandling som personlig kod tillhandahålls samtidigt, ska istället en bekräftelse sändas via en alternativ och säkerhetsmässigt separat kanal. Det ger den enskilde ett väsentligt bättre utgångsläge i att upptäcka försök till identitetsstöld, och denne kan snabbt vidta åtgärder för att begränsa skadeverkan av sådana handlingar.
Grundläggande är alltså att inte basera hela tillhandahållandet på samma kommunikationskanal eller på en person i registraturen. Om till exempel tillhandahållandet vid personligt besök eller elektroniskt på distans, även involverar traditionellt brev direkt från utfärdarfunktionen till folkbokföringsadressen, det vill säga till den adress som finns registrerad i officiellt register, kan återkopplingen göras helt oberoende av registraturfunktionen och därvid uppfylla kraven för tillhandahållandet.
I vissa situationer kanske det inte är praktiskt möjligt att skicka brev till personens folkbokföringsadress. Sådana situationer skulle bland annat kunna tänkas uppkomma vid utfärdande av e-legitimationer till utlandssvenskar, där alltså svensk folkbokföringsadress saknas, eller inom särskilda yrkesgrupper där tjänsten fordrar att personen vistas på annan plats under längre tid.
I sådana fall kan alternativa kontaktuppgifter användas under förutsättning att hela utfärdandeprocessen kan genomföras med likvärdig säkerhet. Det kan till exempel uppnås genom inhämtning av alternativa kontaktuppgifter intygade av personens arbetsgivare, uppdragsgivare eller motsvarande. Det förutsätts då att inhämtning eller verifiering av sådana uppgifter sker på ett

sätt som gör att det inte uppstår ett säkerhetsmässigt beroende till enstaka personer inom utfärdarorganisationen eller registraturen. För personer med skyddad identitet kan bekräftelser förmedlas till personen via Skatteverkets postförmedlingstjänst, både inom Sverige och utomlands.
Det är också möjligt att skicka bekräftelser elektroniskt, vilket många gånger kan vara en fördel då de når den enskilde snabbt och inte sällan ger en högre säkerhet än en traditionell brevlåda. Det krävs då att denna alternativa elektroniska kanal grundas i uppgifter som registrerats och verifierats oberoende av tillhandahållandet av e-legitimationen. Grundläggande är att denna kommunikationskanal inte har ett säkerhetsmässigt beroende till den e-legitimation som ska ges ut. Det får alltså inte vara möjligt att med hjälp av e-legitimationen ta kontroll över eller ändra den alternativa kommunikationskanalen vid utgivningstillfället. Även om det är möjligt att uppdatera sådana kontaktuppgifter via den kanal som tillhandahållande av e-legitimationshandlingen sker genom, kan utfärdare säkerställa att den elektroniska bekräftelsen även sänds till de kontaktuppgifter som funnit registrerade en viss tid innan utgivningen sker. På så sätt är det rimligt säkerställt att bekräftelsen når fram till personen ifråga, även om en bedragare vid utgivningstillfället försöker manipulera den alternativa kommunikationskanalen. Det förutsätts också att den alternativa kommunikationskanalen är verifierad på något sätt, så att det är rimligt säkerställt att endast mottagaren kan ta del av information som sänds denna väg, till exempel genom att denna kanal används regelbundet även för andra ändamål av väsentlig betydelse.
För tillhandahållande på nivå 2 gäller att återkoppling från ansökningsprocessen ska göras på samma sätt som för övriga nivåer, och enligt samma krav. Skillnaden återfinns i att identifieringen enligt K5.11 kan ske genom återkopplingskanalen. Ansökan på distans kan alltså genomföras utan identifiering av sökanden. Med hjälp av information som erhålls dels vid ansökningstillfället, dels vid återkopplingen, kan sökanden sedan tillhandahållas e-legitimationshandlingen. Därvid grundas utgivningsprocessen även på nivå 2 på två skilda kanaler, om än att ansökan sker genom en icke-verifierad kanal.
Återkopplingskanalen kan även användas för att ytterligare uppmärksamma innehavaren om att utgivning skett, och därvid minska risken för att denne inte är fullt införstådd med situationen. Det kan därför också vara lämpligt, där så är möjligt, att i återkopplingen sammanfatta ansvar och skyldigheter som följer av innehavet av e-legitimationen.

Spärrtjänst

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

K6.9 Utfärdare av e-legitimation med kvalitetsmärket 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.

Utfärdare ska tillhandahålla en spärrtjänst där användaren dygnet runt kan spärra sin e-legitimation. Spärrtjänsten måste skyddas mot missbruk, så att det är rimligt säkerställt att den som begär spärr är behörig att göra sådan spärrbegäran. Identifiering av den som begär spärr kan till exempel göras genom tidigare angivet mobiltelefonnummer (SMS) eller via e-post.
En spärrbegäran ska i normalfallet expedieras och effektueras omedelbart. Under vissa omständigheter, då det inte går att identifiera den som begär spärr på ett tillförlitligt sätt, kan det emellertid vara nödvändigt att tillfälligt blockera e-legitimationen i avvaktan på en trovärdig verifiering.
För att säkerställa att innehavare kan spärra sina e-legitimationer då så krävs, ska utfärdare också ha ändamålsenligt beredskap för att hantera överbelastningsangrepp i de delar som rör spärrtjänsten.

7. Kontroll av innehavares elektroniska identiteter

Detta avsnitt i tillitsramverket behandlar den tekniska process, ofta benämnd autentisering, genom vilken en innehavare av en e-legitimation uppger och bevisar sin identitet.

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

Kraven i K7.1 tar fasta på att autentiseringsprocessen som nyttjas när en e-legitimation används ska innefatta sådana kontroller som dels säkerställer att e-legitimationen ifråga är äkta, dels att den inte är spärrad eller att dess giltighetstid har löpt ut.

K7.2 Utfärdare av e-legitimation med kvalitetsmärket Svensk e-legitimation ska säkerställa att tekniska säkerhetskontroller införts vid kontroll av elektronisk identitet så att det är osannolikt att utomstående genom gissning, avlyssning, återuppspelning eller manipulation av kommunikation kan forcera skyddsmekanismerna.

Kraven i K7.2 innebär att användarnas kommunikation vid autentiseringstillfället ska skyddas kryptografiskt. I de fall autentiseringen sker mot en intygutgivningstjänst enligt avsnitt 8 innefattar dessa krav även att tjänsten ska kunna identifieras av användaren på ett säkert sätt. Det ska i möjligaste mån vara uppenbart för användaren att denne kommunicerar

med utfärdaren av den e-legitimation denne innehar, och i detta ska de medel som står till buds användas. Detta bör innefatta användande av s.k. *Extended Validation*-certifikat som resulterar i att utfärdarens identitet visas i användarens webbläsare, samt övriga tillgängliga funktioner som syftar till att förebygga och förhindra att användaren förleds att identifiera sig mot fel part.

8. Utställande av identitetsintyg

Utfärdare av e-legitimation med kvalitetsmärket 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 e-legitimation med kvalitetsmärket 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.

För att säkerställa att innehavare kan använda sina e-legitimationer då de behövs, ska utfärdare också ha ändamålsenlig beredskap för att hantera stunder av exceptionell belastning och försök till överbelastningsangrepp i de delar som rör intygsutgivningstjänsten. Kravet i K8.1 innefattar även att intygsutgivningstjänsten inför utställande av ett identitetintyg med positivt resultat ska ha genomfört en sådan tillförlitlig autentisering i enlighet med avsnitt 7.
För utställande av identitetsintyg på nivå 4 krävs även att identitetsintygen innefattar en referens som går att härleda till en kryptografisk nyckel som utfärdaren vid tidigare tillfälle verifierat att innehavaren har kontroll över. Vanligen är denna nyckel samma nyckel som används för att upprätta transportskyddet, vilket dock inte med nödvändighet måste vara samma nyckelmaterial som används för att autentisera användaren i intygsgivningsfunktionen.
Syftet med skyddet är att förhindra att en mellanhand som förmår snappa upp ett identitetintyg obehörigen ska kunna använda detta. Denna variant av identitetsintyg benämns ibland HoK-intyg (*"Holder-of-Key"*).

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.

DIGG publicerar från tid till annan genom det tekniska ramverket de format och övriga förutsättningar som råder för utformningen av identitetsintyg, samt ombesörjer den distribution av de kryptografiska nycklar som krävs för verifiering av äkthetsskydd (av begäran om intyg samt de intyg som ställs ut) och för kryptering av identitetintygen. Utfärdarens egna konfidentiella nyckelmaterial ska hanteras och skyddas i enlighet med K4.3.

K8.3 Utfärdare av e-legitimation med kvalitetsmärket 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.

Den maximala tid under vilken användaren tillåts göra *single-sign-on* ska begränsas i enlighet med de förskrifter som DIGG från tid till annan publicerar i det tekniska ramverket.

BILAGA A - DISTANSUTGIVNING AV E-LEGITIMATION MED KVALITETSMÄRKET SVENSK E-LEGITIMATION

1. Inledning

För att en legitimationshandling ska vara användbar måste det finnas ett brett förtroende för handlingen bland de som ska förlita sig på den. Förtroendet grundas bland annat i att både utfärdandeprocessen, tillhandahållandet och legitimationshandlingen som sådan är utformad på ett tillräckligt säkert sätt, och att de överenskomna regler som omfattar dessa delar följs av de som ger ut sådana legitimationshandlingar.

Reglerna för utgivning av traditionella legitimationshandlingar av privata aktörer har sina rötter i standarden för de s.k. SIS-märkta ID-korten. Det SIS-märkta ID-kortet är inte i någon del författningsreglerat, utan bestämmelserna utformas i samråd med en certifieringskommitté där branschföreträdare ingår. Dessa innefattar DNV, Statens kriminaltekniska laboratorium, Svenskt Näringsliv, Posten AB, Svenska Bankföreningen, Finansinspektionen, SIS och Rikspolisstyrelsen. Genom dessa branschgemensamma regler åtnjuter det SIS-märkta ID-kortet ett brett förtroende inom hela samhället. Ambitionsnivån för kvalitetsmärket Svensk e-legitimation är densamma. E-legitimationshandlingar av tillitsnivå 3 avses uppfylla motsvarande grad av skydd som den traditionella legitimationshandlingen, samtidigt som sådana elektroniska legitimationshandlingar ska kunna tillhandahållas och användas på ett så effektivt sätt som möjligt.

2. Tillitsramverkets bestämmelser

Tillitsramverkets bestämmelser för utgivning av e-legitimationshandlingar på tillitsnivå 3 tar sin utgångspunkt i de principer som gäller för utgivning av traditionella legitimationshandlingar. Bestämmelserna i denna del kräver fysisk

representation där utfärdaren identifierar sökanden och tillhandhåller legitimationen vid personligt besök.
Utmärkande för den traditionella ID-handlingen är att en sådan innefattar ett tydligt välliknande foto av innehavaren, och att legitimering med sådan ID-handling sker vid ett personligt möte då det krävs att den som presenterar legitimationshandlingen också liknar detta foto. Förutsättningarna vid användning av en elektronisk ID-handling skiljer sig i denna del från den traditionella.
Någon som obehörigen kommer över en e-legitimation kan använda denna utan sådana restriktioner, och utan fysisk närvaro. Vid missbruk av en e-legitimation kan det vara mycket svårt att spåra förövaren. Riskerna förknippade med obehörigt användande av en elektronisk ID-handling kan därvid anses fordra särskilda säkerhetsåtgärder i tillhandahållandet av sådan till sökanden, jämfört med den traditionella ID-handlingen. Därför måste det ställas mycket stringenta krav i denna del för att e-legitimationen ska uppnå en motsvarande grad av skydd som en fysisk legitimation. Kraven på ursprungsidentifiering av sökanden vid utfärdande av e-legitimation bör dock kunna vara jämbördiga med de som ställs vid utfärdande av traditionella ID-handlingar.

3. Säker legitimationskontroll

Utgångspunkten är att en e-legitimation med kvalitetsmärket Svensk e-legitimation av tillitsnivå 3 ska tillhandahållas vid personligt besök, på samma sätt och under samma förutsättningar som en traditionell legitimation. Detta innefattar att legitimationskontroll och tillhandahållande av e-legitimationshandling genomförs av personal i betrodd ställning inom organisationen, vilket som regel fordrar att utfärdaren har egen fysisk representation på de platser man avser utfärda e-legitimationer.
Utfärdaren ska alltså, genom egna medarbetare som visat sig pålitliga och har den utbildning och utrustning som krävs för att fullgöra uppgifterna på ett tillfredsställande och säkert sätt, identifiera sökanden och tillhandahålla e-legitimationshandlingen.
En bedömning av om en person visat sig pålitlig bör göras på grundval av den bakgrundskontroll som utfärdaren förväntas genomföra i enlighet med K3.2 i tillitsramverket, men också baseras på den generella utbildningsnivå och den ställning inom verksamheten som medarbetaren har. Det är knappast lämpligt att nyanställda eller tillfällig personal på egen hand fullgör de uppgifter som är förknippade med utgivning av e-legitimationer, även om de skulle ha fått vad som kan anses vara tillräcklig utbildning i fullgörandet av de arbetsmoment som krävs vid utfärdande av legitimationshandlingar. Det är inte heller lämpligt att personal som i övrigt saknar kvalificerande meriter, och därför annars endast utför enklare sysslor inom verksamheten, hanterar utgivning av e-legitimationer.
En utfärdare som identifierar sökande och tillhandahåller e-legitimationer i egen regi, förväntas därför göra detta med hjälp av egen personal med kvalificerad utbildning, och som i relation till det ansvar som vilar på denne erhåller skälig ersättning.

I denna del ska särskilt understrykas att den hantering av rekommenderat brev för privatpersoner som vanligen tillhandahålls av andra företag än Posten, t.ex. mataffärer, knappast är lämpliga för utfärdande av legitimationshandlingar. Detta inte minst mot bakgrund av de faktiska incidenter som inträffat i hanteringen av rekommenderade brev vid sådana utlämningsställen.
En sådan hantering med rekommenderat brev kan dock vara en del i ett distansutgivningsförfarande, som tillsammans med andra kontroller kan anses uppnå en motsvarande grad av skydd som tillhandahållande vid personligt besök. Denna bilaga syftar till att belysa vad som bör gälla vid ett distansutgivningsförfarande, för att kraven på säker identifiering och säkert tillhandahållande ska kunna anses vara bibehållet.

4. Utfärdande via ombud

Det är naturligtvis tänkbart att säker identifiering och tillhandahållande av e-legitimation kan utföras av ett ombud för utfärdaren. Samma krav enligt K3.2 ställs då på ombudets personal som ska tillhandahålla denna funktion, som för den egna personalen. Ansvaret ska också regleras i avtal mellan ombudet och utfärdaren, och eventuella underleverantörsförhållanden ska tydliggöras i enlighet med K2.6. Utfärdare ansvarar dock för ombuden som för den egna verksamheten.
Utfärdande under sådana premisser bör alltså inte anses utgöra distansutgivning.

5. Distansutgivning

Vid införandet av e-legitimation som elektroniskt legitimeringssätt angavs att utfärdaren ska identifiera sökanden vid personligt besök, på likvärdigt sätt som vid en ansökan om en SIS-märkt legitimationshandling. Samtidigt infördes emellertid en regel om att en sökande som, på angivet sätt, redan har identifierats vid ett personligt besök för att få använda bank på Internet eller någon liknande tjänst *för ekonomiskt eller rättsligt betydelsefulla mellanhavanden*, istället får identifieras genom denna tjänst.
Dessa bestämmelser för distansutgivning syftar till att underlätta utgivning av e-legitimation på så kallad mjuk bärare, och att detta skulle kunna ske elektroniskt och på distans, företrädesvis via sökandens Internetbank. Det möjliggör kostnadsbesparingar, både genom att sökanden direkt i e-tjänsten kan tillhandahållas det användarstöd som krävs vid installationen och i nedladdningen av e-legitimation och programvara, men också för att effektivisera utgivningen genom ett självserviceförfarande från sökandens sida.
En sådan förenklad rutin skulle emellertid inte få användas om det kan antas att den avsedda e-tjänsten inte förmår identifiera sökanden på ett tillräckligt säkert sätt. Tillåtligheten kräver alltså också att sökanden ska kunna identifieras på distans på ett säkert sätt, åtminstone med en säkerhetsnivå likvärdig med den e-legitimation som ges ut.
Övriga säkerhetsaspekter anses omhändertagna genom att leverantören erbjuder utgivning som del i en annan tjänst, vars huvudsakliga syfte innebär att leverantören står en betydande ekonomisk eller rättslig risk i samband med denna.
Resonemanget grundas alltså i att leverantören förväntas ha vidtagit de

säkerhetsåtgärder som krävs för att hantera den egna risken förknippad med tjänsten, och att dessa bör kunna anses tillräckliga även för utgivning av e-legitimationer.
Det är även vanligt att banker som helt saknar fysisk representation ger ut e-legitimationer. Dessa kan då anses ha uppfyllt kraven på rättsligt eller ekonomiskt betydelsefulla mellanhavanden genom att ha uppnått kundkännedom då kunden kontinuerligt använder en eller flera tjänster som tillhandahålls av banken, snarare än att det skett ett fysiskt möte då kunden legitimerat sig på likvärdigt sätt som vid ansökan om SIS-märkt ID-handling. Ofta är ett eller flera rekommenderade brev ett led i upprättandet av den ursprungliga kundrelationen, men där utgivning i så fall inte ska ske förrän banken och kunden har en sådan rättsligt eller ekonomiskt betydelsefull relation som avses i avtalstexten. Det avses fordra att kunden brukar bankens tjänster under viss tid, vanligen i storleksordningen 6 månader.
Där även andra aktörer utanför finanssektorn utfärdar och tillhandahåller e-legitimationstjänster gäller samma principer. Bestämmelserna kan emellertid komma att kräva en vidare tolkning än vad som ursprungligen avsågs, dock utan att målsättningen bör ändras; att utgivning av e-legitimation ska ske med samma nivå av säkerhet och tillit som en traditionell legitimationshandling.

6. Utfärdandeprocessen

Utfärdandeprocessen i de delar som rör distansförhållandet kan brytas ner i två huvudkomponenter:

- fastställande av sökandens identitet,
- tillhandahållande av e-legitimationshandling.

Den samlade skyddsgraden kan sägas vara produkten av säkerheten i dessa två steg. Fastställande av sökandens identitet kan samtidigt betraktas utifrån både säkerheten i den ursprungliga identifieringen och den kundkännedom om sökanden som utfärdaren uppnått över tid, där dessa två delar kan kompensera för varandra.

Exempel: Utfärdande via Internetbank

I det typfall för vilket bestämmelserna för distansutfärdande en gång utformades, dvs. bankkunder med tillgång till Internetbank, förutsätts kundens identitet ha fastställts då kundrelationen upprättas genom legitimering vid personligt besök med fullgod legitimationshandling. I efterföljande tid har banken sedan uppnått det som kallas kundkännedom, t.ex. genom att kundens lön regelbundet sätts in på ett konto i banken, och kanske att ett bankkort knutits till kontot med vilket kunden betalar sina utgifter. Därigenom upprätthålls en pågående relation mellan banken och kunden. Detta är också de grunder som bankerna själva använder för att utfärda de s.k. SIS-märkta ID-korten.
I tillägg till detta har banken dessutom tillhandahållit kunden någon form av elektronisk identifieringsmekanism, t.ex. ett aktivt kort eller dosa för engångslösenord, med vilken kunden kan identifieras på ett säkert sätt i Internetbanken. Tillhandahållandet sker då genom användning av denna säkra identifieringsmekanism.

I detta fall har alltså **ursprungsidentifiering** skett genom legitimationskontroll av hos utfärdaren betrodd personal, och som tilldelat sökanden en **säker elektronisk ID-handling** som utfärdaren kan använda för att på distans och på ett säkert sätt identifiera sökanden. I efterföljande tid har banken uppnått **kundkännedom**, varvid en e-legitimation kan tillhandahållas på nämnda sätt.
Förfarandet bör anses förenligt med tillitsramverkets syfte att upprätthålla tillräcklig säkerhet i processen för distansutgivning, och från säkerhetssynpunkt kunna betraktas som likvärdig med ansökan och utgivning av en traditionell legitimationshandling.

Exempel: Utfärdande via arbetsgivare

En tillämpning av bestämmelserna bör även kunna göras vid det fall identifiering och tillhandahållande sker genom en arbetsgivares försorg. En sådan arbetsgivare skulle nödvändigtvis inte behöva agera formellt ombud enligt avsnitt 4, utan kan istället genom sin ställning bidra till att stärka säkerheten i utgivningsprocessen till den nivå som krävs.
Då arbetsgivarens organisation används som en del i utgivningsprocessen, förutsätts initiativet till utgivningen tas av arbetsgivaren som en del i att tillhandahålla medarbetaren en e-legitimation denne ska använda i tjänsten. Här anses rekvisitet **rättsligt eller ekonomiskt betydelsefulla mellanhavanden** vara uppfyllt genom arbetsgivarens relation med sökanden. Den person vid arbetsgivaren som beställer e-legitimationen förutsätts vara behörig att företräda beställaren i den aktuella rollen, det förutsätts vidare att utfärdaren kontrollerar dessa omständigheter så att den försändelse som riktas till arbetsgivaren kommer rätt person till handa.
Dock, då arbetsgivaren inte är att anse som en del av utfärdarens verksamhet och inte heller agerar ombud för denne, krävs kompenserande kontroller för att säkerställa att inte arbetsgivaren obehörigen i annans namn beställer och missbrukar en sådan e-legitimation. Det förutsätts vidare att utfärdaren och arbetsgivaren har upprättat avtal, där de allmänna villkoren förknippade med tjänsten regleras, vilken ersättning som ska utgå vid utfärdande och vilka personer inom arbetsgivarens organisation som är behöriga att beställa sådana e-legitimationer. Utfärdaren bör ha kontroller som säkerställer att beställningen är behörigen undertecknad av de som lägger varje beställning.
Tillhandahållandet av sådan e-legitimation kan ske genom att sökanden förses med två olika försändelser; en försändelse sänds som rekommenderat brev till sökandens folkbokföringsadress, och en försändelse sänds till den som behörigen undertecknat ansökan för beställarens räkning. Denne företrädare för beställaren ska personligen efter att ha säkerställt sökandens identitet, överlämna den obrutna försändelsen till sökanden.
Det rekommenderade brevet som skickas direkt till sökanden ska skickas med mottagningskvittens, och kvittensen av detta mottagande får anses utgöra tillräckliga kontroller för att en person ska kunna upptäcka om sådan e-legitimation beställts obehörigen i dennes namn.

I detta fall har alltså **ursprungsidentifiering** skett dels genom legitimationskontroll av behöriga företrädare för arbetsgivaren, dels av utlämningsstället för det rekommenderade brevet, varvid **uppgifter i dessa två försändelser** kombineras för att på ett säkert sätt på distans identifiera sökanden. Arbetsgivaren anses ha uppnått motsvarande **kundkännedom** genom ett anställningsförhållande eller motsvarande, där arbetsgivaren också betalar ersättning till sökanden. Utfärdande kan sedan ske via den upprättade distansrelationen med utfärdaren på angivet sätt. Även detta förfarande bör kunna anses vara förenligt med tillitsramverkets syfte att upprätthålla tillräcklig säkerhet i processen för distansutgivning.

Exempel: Utfärdande grundad på elektronisk identifiering

Det är också tänkbart att en utfärdare kan utnyttja sina egna eller en annan parts mekanismer för säker elektronisk identifiering för distansutgivning. Det kan dock förekomma affärsmässiga begränsningar i ett sådant förfarande. Det är naturligt att affärsdrivande utgivare inte tillåter att annan utgivare slår mynt av den distansrelation de upprättat med respektive e-legitimationsinnehavare. Det kan dock förekomma andra elektroniska ID-handlingar som inte är behäftade med sådana restriktioner, eller att sådan utgivning grundad i en elektronisk identifiering möjliggörs genom ett särskilt avtal.
En förutsättning är naturligtvis att den ursprungliga elektroniska ID-handlingen givits ut på ett sätt som är förenligt med tillitsramverkets syften.
Exempel skulle kunna innefatta de så kallade **tjänstekort** som används av personal inom vissa myndigheter. Dessa har inte sällan förmåga till elektronisk identifiering på distans. Vid ett sådant förfarande anses kraven på **ursprungsidentifiering** och **kundkännedom** uppfyllt genom den ursprungliga utgivarens försorg.
Tillhandahållandet av en e-legitimation ska emellertid alltid innefatta tillkommande kontroller som möjliggör för en person att upptäcka och agera på obehörig utgivning. Det kan t.ex. ske genom att personlig kod för att aktivera e-legitimationen skickas ut med reguljärt brev till folkbokföringsadressen.

7. Otillräckliga grunder för distansutgivning

Som tidigare angetts bör rekommenderat brev ställt till privatperson som enda identifieringsgrund inte anses vara tillräckligt för distansutgivning av e-legitimation. Inte heller bör uppgifter från fakturor eller liknande försändelser användas som grund för att att identifiera sökanden. Sådana förfaranden är visserligen vanliga i många andra länder, företrädesvis inom den s.k. anglosfären. I dessa länder finns därför en inarbetad kultur att säkert förvara och förstöra sådana handlingar. I Sverige med den starka offentlighetsprincip som råder, finns ingen sådan kultur. Fakturor, kontoutdrag och liknande handlingar slängs ofta med hushållssopor eller i pappersåtervinning, och det är ofta också enkelt att få ut fakturakopior från olika leverantörer. Ett sådant förfarande skulle därför medföra betydande risker för identitetsstölder, varför sådana uppgifter inte ska användas som grund för identifiering och distansutgivning av e-legitimation.
Slutligen bör inte heller enstaka kreditkortstransaktioner av ringa värde kunna anses utgöra tillräcklig grund för att identifiera sökanden vid distansutgivning.

Kreditkort ges ofta ut via reguljär postgång, där kreditkortsföretagen har interna kontroller för att upptäcka transaktioner som kan tyda på att kreditkortet hamnat i felaktiga händer. Det är också vanligt att kreditkortsuppgifter röjs genom dataintrång. En enstaka sådan transaktion kan därför inte anses vara tillräcklig grund för identifiering av sökanden, och måste således kompletteras på mer än ett sätt. I det tidigare angivna exemplet med mobiltelefonoperatör som agerar utgivare, kombineras verifiering av kreditkortets ägare med en ursprungsidentifiering av butikspersonal och den tröghet som etablerande av kundkännedom innebär.