Analys och hantering av rapport från MSB - Analys av informationssäkerheten i Svensk e-legitimation

Innehållsförteckning

1 Inledning och syfte

Handlingsplanen är framtagen av E-legitimationsnämndens kansli. Den utgör ett underlag för vilka åtgärder och aktiviteter som bör initieras med anledning av de rekommendationer avseende informationssäkerheten i Svensk e-legitimation som finns i MSB rapport.

Handlingsplanen fastställdes av E-legitimationsnämnden vid nämndmötet den 20 februari 2015.

1.1 Bakgrund

E-legitimationsnämnden ska stödja och samordna elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster. Detta görs genom att tillhandahålla anslutning till en samverkan runt tjänster - federationen för Svensk e-legitimation. Samverkan avser aktörer inom offentlig förvaltning och aktörer som levererar legitimeringstjänster. Det innebär bland annat att administrera valfrihetssystemet för elektronisk identifiering och att upphandla en signeringstjänst. Den senare genom att nämnden tagit fram en normativ specifikation för en underskriftstjänst som en del av ramavtalet ”*E-förvaltningsstödjande tjänster 2010”*.

MSB har på begäran från tre myndigheter genomfört en analys av Svensk e-legitimation. De tre myndigheterna är Arbetsförmedlingen, CSN och Försäkringskassan. Analysen har resulterat i en rapport som innehåller ett antal rekommendationer om vad som behöver göras för att förstärka lösningen Svensk e-legitimation ur ett säkerhetsperspektiv. Rapporten blev klar den 20 oktober 2014. En fyrsidig sammanställning av analysen publicerades på MSB:s webbplats. Hela rapporten hemligstämplades enligt 18 kap. 8 § och 18 kap. 13 § offentlighets- och sekretesslagen (2009:400).

E-legitimationsnämnden och de tre myndigheterna som lämnade in begäran till MSB har fått den fullständiga rapporten.

Denna handlingsplan beskriver förslag till angreppssätt av de rekommendationer som finns i MSB:s rapport. En förutsättning för det fortsatta arbetet är att det blir en konstruktiv och bred dialog runt det som rekommendationerna står för.

Rekommendationernas innehåll kan delas in i olika grupper av frågor nämligen:

- Frågor som nämnden bör hantera t ex krav på regelverk och den centrala infrastrukturen.
- Frågor som gäller alla som tillhandahåller tjänster som exponeras över Internet.
- Frågor som har sin utgångspunkt i behov hos offentlig förvaltning.
- Frågor som är viktiga för leverantörer i federationen.

Andra perspektiv som är viktiga att belysa är:

- När i tid krävs att rekommendationen hanteras t ex kan få påverkan på den utveckling som pågår.
- Finns det olika planeringsperspektiv för hantering av rekommendationerna – omedelbart, inom visst antal år, på lite längre sikt.
- Vilka effekter ska uppnås på sikt med utgångspunkt i rekommendationerna.

Arbetet med att ta fram denna handlingsplan har föregåtts av möten med de som genomfört analysen i syfte att förstå rekommendationerna.

Nämndens kansli har också haft möten med ett antal myndigheter för att få deras syn på rekommendationerna.

Upplägget för denna handlingsplan är enligt följande:

- Alla rekommendationerna finns med inklusive den bakgrundsbeskrivning, som MSB har gett, vilken lett fram till rekommendationen.
- För varje rekommendation finns det en inledande analys som beskriver utgångspunkter och kravarbete med området t ex ”*Central infrastruktur*” och vad som bör göras utifrån rekommendationen.
- Slutligen finns förslag till fortsatt hantering av det som rekommendationen står för.

Några av de frågor som bör vara med i det fortsatta arbetet med rekommendationerna är:

- Vem kan hantera rekommendationen?
- När måste rekommendationen hanteras i sin helhet eller delvis?
- Vilken effekt ska nås om rekommendationen genomförs till sin helhet eller delvis?
- Hur påverkas befintlig lösning av rekommendationen?

1.2 Målet med arbetet

Arbetet med handlingsplanen är av stor betydelse för tilltron till lösningen Svensk e-legitimation. För det fortsatta arbetet är det betydelsefullt hur lösningen Svensk e-legitimation utvecklas. Det är viktigt att ett antal mål formuleras som kan vara utgångspunkten för det fortsatta arbetet.

Effektmålen för arbetet är:

1) Användare ska ha en god helhetsupplevelse avseende tjänster, som använder Svensk e-legitimation.
   Mäts genom enkäter till användare där den första enkäten sänds ut i slutet på andra halvåret 2016 och därefter vartannat år.
2) Informationssäkerheten ska vara högt prioriterad inom offentlig förvaltning.

Mäts genom att antalet inträffade säkerhetsincidenter i den offentliga federationen för Svensk e-legitimation har minskat med x % för varje år med start från och 1 januari 2017.

3) Alla som tillhandahåller tjänster enligt Svensk e-legitimation ska ha ett riskbaserat angreppssätt vid utveckling och förändring av tjänst.
Mäts genom att antalet inträffade säkerhetsincidenter där tjänster enligt Svensk e-legitimation används, har minskat med y % för varje år med start från och 1 januari 2017.

2 Analys och förslag avseende rekommendationer

2.1 Övergripande rekommendationer

2.1.1 Analys och förslag till hantering rekommendation 1

1. MSB rekommenderar att det tillförs ytterligare strategisk teknisk kompetens till E-legitimationsnämnden. Antingen direkt till nämnden eller genom stöd från myndigheter med teknisk informationssäkerhetskunskap.

Bakgrund till rekommendationen (MSB)
Ett system av denna typ kräver långsiktig strategisk teknisk kompetens, då det ständigt kommer att vara under utveckling och utsättas för nya hot och risker som uppdagas i befintliga lösningar. E-legitimationsnämndens kansli består idag av fyra personer som ska arbeta med alla aspekter av Svensk e-legitimation.
En kompetens som bör förstärkas är egen strategisk teknisk kompetens, alternativt kan denna kompetens tillföras från annan myndighet. En viktig del av denna kompetens är informationssäkerhetskunskap. Mot bakgrund av detta anser MSB att E-legitimationsnämnden bör tillföras ytterligare strategisk teknisk kompetens för att utföra dessa arbetsuppgifter.

Nämndens analys
Det finns några grundläggande effekter som ska uppnås med utvecklingen av identitetsfederationen för Svensk e-legitimation. Lösningen ska underlätta för offentlig förvaltning att utveckla e-tjänster genom att standardisera kommunikationen mellan de aktörer som behövs för att genomföra en legitimering alternativt en underskrift i en e-tjänst. Frågorna är av olika karaktär allt från juridik, verksamhet, affärsfrågor till tekniska frågor. Att tillhandahålla och förvalta en identitetsfederation ställer höga krav på kompetens inom många områden. Federationen ska bidra till ökad säkerhet och tillgänglighet till offentlig förvaltnings e-tjänster. Men det ska också bidra till att offentlig förvaltning får en effektivare utvecklingsverksamhet. Syftet är att e-tjänsten alltid ska få ett standardiserat intyg och därmed ska det underlätta och effektivisera utvecklingen.

Målet är att arbetet på e-tjänstesidan runt anpassning av den egna miljön till nya e-legitimationslösningar kan komma att minska när anslutningen till Svensk e-legitimation kommit en bit på väg dvs. när standardiseringen slagit igenom fullt ut.

Kompetensen och erfarenheten av den infrastruktur som Svensk e-legitimation bygger på är inte särskilt utbredd inom offentlig förvaltning idag. Den kompetens som framförallt krävs är dels

informationssäkerhet men också runt SAML som mycket av arkitekturen bygger på. Kompetensen finns inom offentlig förvaltning och specifikt inom vissa expertmyndigheter.

Nämnden och Förvaltningsforum i samverkan blir en nyckelspelare för att hantera rekommendationen. Det är denna gruppering som kan definiera den kompetens som krävs samt identifiera var denna finns. Specialistkompetens inom informationssäkerhet finns bl.a. hos de myndigheter som genomfört analysen och som kommit med rekommendationen.

Uppbyggnaden av kompetensen bör ske inom hela offentlig förvaltning. Fokus för tillhandahållare av e-tjänster bör vara att utveckla e-tjänster som är säkra och som bygger på riskbaserad behovsanalys. Fokus för nämnden bör vara hög kunskap om den valda arkitekturens alla delar, förmåga att arbeta riskbaserat samt utvecklingen inom standardisering av identifiering och underskrift.

Hantering rekommendation 1
Nämndens kansli ska tillföras resurs med djup kompetens inom informationssäkerhetsområdet. Arbetet inom Förvaltningsforum ska ha som målsättning att den samlade kompetensen inom offentlig förvaltning avseende standardiserade lösningar inom IT-säkerhetsområdet ska öka. Detta kan ske genom att en undergrupp till forumet skapas med syfte att stärka den samlade kompetensen.
Nämnden ska arbeta för att en formaliserad samverkan med MSB kan etableras.

2.1.2 Analys och förslag till hantering rekommendation 2

2. MSB rekommenderar att det genomförs en genomgång av hela systemet ur ett informationssäkerhetsperspektiv när den tekniska lösningen har etablerat sig i dess olika delar, dvs. när systemet är i drift.
Vidare rekommenderar MSB att en genomgång av hela systemet ur ett informationssäkerhetsperspektiv vid större förändringar eller med lämplig regelbundenhet.

Bakgrund till rekommendationen (MSB)

Denna analys har genomförts i ett skede där Svensk e-legitimation på många vis varit under utveckling, exempelvis saknas legitimeringstjänster. Det är därför viktigt att det genomförs en genomgång av hela systemet ur ett informationssäkerhetsperspektiv när den tekniska lösningen har etablerat sig i dess olika delar, dvs. när systemet är i drift.
Det är också av vikt att vid större förändringar framöver genomföra övergripande säkerhetsanalys av hela systemet för att säkerställa att nya svagheter inte oavsiktligt införs.

Nämndens analys

Alla typer av tjänster inom Svensk e-legitimation finns ännu inte i drift. Ingen leverantör av eID-tjänst hade ansökt om att ansluta sig och processen för att ansluta tillhandahållare av e-tjänst hade ännu inte prövats. Vid tidpunkten för analysen som MSB genomfört fanns inga legitimeringstjänster eller e-tjänster anslutna till federationen. Då fanns de centrala tjänsterna i drift dvs. de tjänster som nämnden kravställt och godkänt.

Lösningen är därför i sin helhet från ett operativt perspektiv ännu inte genomgånget och analyserat utifrån ett helhetsperspektiv av en extern och oberoende part. Det är viktigt att

lösningen granskas och analyseras när systemet innehåller alla dess tjänstetyper. Vad som ska granskas och hur bör analyseras vidare. Det fortsatta arbetet är beroende av andra åtgärder som görs för att öka säkerheten i lösningen. Beroende på vilka åtgärder som vidtas kan det få påverkan på redan anslutna tjänster. Det bör tas med i beaktande vid framtagningen av en åtgärdsplan för analys av hela systemet. Denna rekommendation har hög prioritet på grund av eventuell påverkan på redan anslutna tjänster samt pågående utveckling av tjänster.

Det är viktigt att lösningen i sin helhet är analyserad och genomgången och där delar utifrån ett riskbaserat synsätt hanterat de risker med de högsta riksvärdena. Svensk e-legitimation är en infrastruktur med många anslutna aktörer och ingående komponenter som kräver ett metodiskt och kontinuerligt arbete utifrån ett informationssäkerhetsperspektiv och att det finns en medvetenhet om risker och riskåtgärder. De senare behöver kontinuerligt analyseras och utvärderas.

Hantering rekommendation 2
Rekommendationen ska hanteras i sin helhet när alla typer av tjänster finns anslutna till den offentliga federationen.
Nämnden ska i samverkan med Förvaltningsforum gå igenom den åtgärdslista som togs fram i samband med den riskanalys som genomfördes inom nämnden under 2012 och 2013. Det ska vara startpunkt för en förnyad riskanalys.
Nämnden ska planera för att en förnyad riskanalys genomförs under första kvartalet 2015 och med deltagande från Förvaltningsforum. Åtgärdslistan från denna riskanalys ska utgöra utgångspunkt för en förnyad säkerhetsanalys. Denna förnyade säkerhetsanalys ska vara genomförd senast 1 april 2016.
Nämnden ska som styrande princip ha att det alltid ska göras en riskbaserad säkerhetsanalys vid större förändringar inom systemet.

2.1.3 Analys och förslag till hantering rekommendation 3

3. E-legitimationsnämnden bör överväga kravställning som innebär att de handlingar som ska skrivas under går att presentera på ett tillförlitligt sätt för användaren.

Bakgrund till rekommendationen (MSB)

Det finns en tydlig problematik i de flesta E-legitimationssystem, där användarna har svårt att särskilja autentisering och signering. Ett annat problem är att användare ofta misstar E-legitimationen för en inloggningsmetod snarare än en ID-handling. Detta illustreras bl.a. i den användarbarhetsstudie som genomförts på uppdrag av E-legitimationsnämnden.

Nämndens analys

Det är angeläget att avsikten med interaktionen där användaren ska skriva under en handling blir tydlig. Regelverket för Svensk e-legitimation kravställer att förlitande parts namn ska visas för användaren både vid inloggning och vid underskrift i legitimeringstjänsten. Användaren ska också få information om det är en inloggning eller om det är en underskrift som sker i legitimeringstjänsten. Det är viktigt att användaren förstår när det är en inloggning alternativt när en underskrift görs.
Det finns en vägledning för hur användargränssnitt ska se ut. Syftet med vägledningen är att

utvecklare av användargränssnitt ska få stöd i hur interaktionen med användaren kan och bör se ut. Alla som utvecklar tjänster, som har interaktion med användare, måste ha förståelse för detta behov.

Genom att ge användaren tillräcklig information om vad som krävs av denna minskar också risken att användaren blir lurad att genomföra en felaktig åtgärd. Vad som är tillräcklig information och möjlig information kan enbart e-tjänsten bedöma när det gäller information om vad användaren skriver under. Nämnden kan tillhandahålla en infrastruktur som medger ett säkert medskick av information till legitimeringstjänsten som kan visa upp det för användaren i underskriftssituationen. Det innebär att legitimeringstjänsten måste kunna hantera information som ska presenteras för användaren.

E-tjänstens möjlighet att leverera information som är specifik för just den handling som ska skrivas under är inte oproblematisk att formulera och tillhandahålla utifrån framförallt ett integritetsperspektiv.
Regelverket för Svensk e-legitimation måste också anpassas så att det blir möjligt att säkert leverera information om den handling som ska skrivas under.
Legitimeringstjänsternas förmåga att hantera och visa specifik information för användaren måste redas ut.
Det är underskriftstjänsten som måste kunna ta emot och leverera vidare till legitimeringstjänsten den information som e-tjänsten anger.
Ambitionen måste vara att användaren ges möjlighet att förstå vad underskriften innebär och att den genomförs på ett säkert sätt.

Hantering rekommendation 3
Nämnden ska ta fram förslag till hur en teknisk lösning kan se ut som ger stöd till att användaren kan se vad som skrivs under. I förslaget ska det tydligt framgå på vilket sätt lösningen påverkar olika tjänster. Förankring av förslaget ska göras så brett som möjligt för att på det sätt få en bred acceptans för förslaget. Detta arbete ska vara klart senast 1 januari 2016.
Nämnden ska i samverkan med Förvaltningsforum ta fram vägledning och tips för hur e-tjänsteägare kan arbeta med frågor runt legala förutsättningar för vad som får visas vid underskrift av handlingar.
Nämnden ska i samverkan med Förvaltningsforum ta fram en plan för detta arbete. Planen ska finnas framme senast 1 oktober 2015.

2.1.4 Analys och förslag till hantering rekommendation 4

4. De myndigheter som erbjuder e-tjänster som ska använda Svensk e-legitimation bör genomföra en grundlig behovsanalys innan tjänsten tas i bruk. Analysen bör bland annat innefatta riskanalys av de tjänster som exponeras samt informationsklassificering av de informationstillgångar som ingår. Resultatet av denna analys bör vara vägledande i myndighetens beslut, bland annat om val av LoA nivå för e-legitimering, behov av sidokanaler mm.

Bakgrund till rekommendationen (MSB)
I en federationslösning är aktörerna beroende av att alla ingående aktörer håller en god säkerhetsnivå, därför är det centralt att alla de myndigheter som erbjuder e-tjänster och som ska

använda Svensk e-legitimation genomför en grundlig behovsanalys. Analysen bör bl.a. innefatta riskanalys av de tjänster som exponeras samt informationsklassificering av de informationstillgångar som ingår.
Myndigheter är vidare ansvariga för att säkerställa att deras egna system håller god säkerhet, och har ansvar för att själva bedöma behov av LoA nivå för legitimering, och behov av ytterligare säkerhetsåtgärder som exempelvis sidokanaler, beroende på sin informationsklassificering. Sidokanaler används för att t.ex. informera om att en förändring har skett av en uppgift som rör den enskilde. En sådan sidokanal kan vara sms eller mail.

Nämndens analys

En utgångspunkt för att tillhandahålla tjänster över Internet är att tillhandahållaren av e-tjänst har god kunskap om de risker och de krav som det egna regelverket ställer på hur information får hanteras och exponeras.
Varje aktör med tjänster som exponeras över Internet måste ha god kunskap inom informationssäkerhetsområdet och de krav som ställs samt också kunna införa de åtgärder som krävs för att minimera riskerna.

Rekommendationen påverkar alla som ska delta i identitetsfederationen för Svensk e-legitimation. För utfärdare av e-legitimation och leverantörer av eID-tjänst ställs tydliga krav på detta. Dels i form av uppfyllnad av regelverket för viss tillitsnivå men också krav på informationssäkerheten och dess uppfyllnad.
För aktörer inom offentlig förvaltning t ex. kommuner, landsting och statliga myndigheter, finns tydliga krav på informationssäkerhet inklusive klassificering av information. För de e-tjänster som hanterar information ska en behovsanalys göras för att beslut ska kunna tas avseende krav på vilken tillitsnivå som krävs för att e-tjänsten ska kunna tillåta att information visas och hanteras. Uppfyllnaden av kraven på en viss legitimeringstjänst ska motsvara de krav som e-tjänsten ställer för att tillgängliggöra efterfrågad information.

I regelverket för Svensk e-legitimation finns dessa krav formulerade. Vid den annonsering av tjänster som sker inom valfrihetssystemet sker annonsering av tjänster med viss tillitsnivå t ex LoA 3.
Att ha god informationssäkerhet och genomfört informationsklassificering av den egna informationen är en förutsättning för att kunna tillhandahålla säkra tjänster som är exponerade över Internet.

Hantering rekommendation 4
Tillitsramverket för Svensk e-legitimation är en central del i beslut runt tillitsnivåer av informationen.
Nämnden ska ta fram en vägledning med rekommendationer som ger stöd till kommuner, landsting och statliga myndigheter, i beslut runt krav på tillitsnivåer i elektroniska tjänster. Arbetet ska ske i samverkan med Förvaltningsforum. Vägledningen ska finnas tillgänglig i sin första utgåva, senast 1 januari 2016.
Nämnden ska i samverkan med Förvaltningsforum driva på att det tas fram en vägledning för informationsklassificering av den information som ska tillgängliggöras via tjänster. Fokus ska vara på utveckling av nya tjänster. Vägledningen ska finnas tillgänglig i en första utgåva senast 30 juni 2016.

2.2 Regler och avtal för Svensk e-legitimation

2.2.1 Analys och förslag till hantering rekommendation 5

E-legitimationsnämnden bör överväga att:

5. Definiera minimikrav på säkerhet i de skrivningar som ger utrymme för tolkningar och subjektiva bedömningar, exempelvis i de fall där texten hänvisar till ospecificerad ”god branschpraxis”.

Bakgrund till rekommendationen (MSB)

I vissa fall är den dokumentation som finns för Svensk e-legitimation tvetydig vilket riskerar att leda till skillnader i implementation hos aktörerna i federationen, med konsekvensen att uppnådda säkerheten i federationen dimensioneras av den mest sårbara implementationen.

Ett tydligt exempel på detta är där regelverket föreskriver att federationsoperatören och eID-leverantörer

”ska utföra sina uppgifter på ett fackmannamässigt sätt och i enlighet med Regelverket, gällande lagar och andra författningar, myndighetsbeslut och inom relevant område förekommande god branschpraxis.”

Att föreskriva att arbetet ska utföras fackmannamässigt och enligt förekommande god branschpraxis utan att exemplifiera vad som avses med detta, lämnar en stor tolkningsmån till respektive aktör. Om kravet utökas alternativt förtydligas med referenser till standarder (t ex [ISO27002] och dokumenterad branschpraxis (t.ex. OWASP Testing Guide [QWASP TG] blir kravet mycket tydligare och det blir lättare att påvisa efterlevnad av kravet. Det är värt att notera att vissa standarder, t.ex. ISO 27002, anger rekommendationer i form av bör-krav. Användning av en sådan standard behöver då kompletteras med tillägg för att säkerställa implementationen av standarden hos aktören.

Att för lågt ställda och otydliga krav kan orsaka problem har identifierats i den leverantörsdokumentation och de penetrationstestrapporter som levererats till E-legitimationsnämnden från leverantören av de centrala tjänsterna, men även genom den dialog som under analysen förts med leverantören av de centrala tjänsterna.

Nämndens analys

Utgångspunkten vid framtagning av kraven på aktörerna inom Svensk e-legitimation (Regelverket) har varit att dessa ska vara teknikneutrala och så långt möjligt peka på standardiserade lösningar. Om det av olika skäl inte har varit möjligt att peka ut en eller flera standarder så har kraven formulerats på så att syftet och vad som ska uppnås är tydligt. Ett skäl till att inte ställa krav på en bestämd standard är i de fall leverantörerna har visat att de arbetar utifrån olika standarder. Att gå alltför långt i hur kraven formuleras i form av att peka på en specifik standard eller ramverk kan därmed innebära att kraven är svåra att uppfylla för leverantören. Utgångspunkten måste vara att om det finns skallkrav ska dessa formuleras tydligt. I övrigt ska det finnas visst utrymme i hur olika aktörer väljer att realisera ett krav. Det är i granskningen av varje levererande aktör inklusive dess tjänst som uppfyllnaden av ett visst krav kan dömas av.

Det är också avvägning av hur kraven kan ställas i ett skede när det ska ske en övergång från dagens lösning till en mer standardiserad lösning.

Det är dock angeläget, att det vid den granskning som sker av levererande aktörer och dess tjänster, att realiseringen av kravet blir normgivande.

I det granskningsarbete som ska ske inför godkännande finns alltid en miniminivå på krav definierad.

Att alltför snabbt sätta en miniminivå för högt innebär risker att ingen kan komma upp till den satta nivån.
När det gäller kravställningen av den centrala infrastrukturen fanns en kravställning på viss minimininivå.
En strävan måste vara att kraven ska peka på standarder vilket också ska visa på viss miniminivå.
Men arbetet med att verifiera att kravet är uppfyllt måste kvarstå.

Hantering rekommendation 5
Den kravställning som finns i regelverket för Svensk e-legitimation kvarstår.
Nämnden ska tydliggöra i Regelverket och dess vägledningar vad som ska vara uppfyllt för att få godkänt vid en granskning. Arbetet ska vara genomfört senast 1 januari 2016.
Granskningsprocessen och dess kravdokument (Regelverket) ska publiceras senast 1 augusti 2015. En genomgång av granskningsprocessens innehåll ska ske i Förvaltningsforum senast 31 december 2015.

2.2.2 Analys och förslag till hantering rekommendation 6

E-legitimationsnämnden bör överväga att:

6. Ta fram en plan för framtida utveckling av Svensk e-legitimation där relevanta kommentarer från aktörer (alla i federationen ingående parter) och andra intressenter (som exempelvis leverantörer av underskriftstjänster eller potentiella medlemmar av federationen) har beaktats.

Bakgrund till rekommendation (MSB)

I Svensk e-legitimation kommer olika aktörer som t ex e-tjänster, eID-tjänster och identitetsutfärdare att ha ett stort ansvar för säkerheten i deras respektive delar av systemet. Aktörerna kan fritt förbättre säkerheten inom sin respektive del så länge det fortfarande är inoperabelt enligt specifikationerna för Svensk e-legitimation.
Normal vidareutveckling och utökning av säkerhetsmekanismer genom förändringar i regelverk och tekniskt ramverk måste presenteras för anslutna aktörer tidigast 180 dagar innan ändringen kan träda i kraft [ELN-500] om det inte gäller ”allvarliga säkerhetsskäl” (vilket MSB tolkar som akuta säkerhetsproblem) eller om samtliga aktörer är överens om en tidigare tidpunkt ([ELN-500], avsnitt 3.4.2. och 3.4.5).
Ingen arkitektur och inget ramverk är statiskt. Nya behov kommer kontinuerligt att uppstå, baserat på användningsfall (exempelvis att använda e-legitimation för mobiltelefoner) men även baserat på teknikutvecklingen och på nya hot som uppkommer. Dessa behov kommer att behöva hanteras, en del skyndsamt, och en del (exempelvis mer fundamentala och genomgripande förändringar) kommer att kräva längre framförhållning. Texten är något förkortad!

Nämndens analys

En viktig grund för en väl fungerande samverkan mellan ett stort antal aktörer är att det finns en gemensam bild av vad man vill med samverkan. I den aktuella samverkan där alla använder samma infrastruktur är det en överlevnadsfråga att det finns en gemensam vilja åt vilket håll infrastrukturen ska utvecklas. Så arbetet med att ta fram gemensamma utvecklingsplaner är en självklar del i det gemensamma arbetet tillsammans.
Den självklara platsen för att arbeta fram utvecklingsplaner är Förvaltningsforum där alla

anslutna aktörer finns representerade.
Samverkan i Förvaltningsforum är i sitt startskede och arbetet med att formera sig pågår. Att ta fram en gemensam plan för utveckling blir en viktig aktivitet för forumet.
En tydlig utstakad plan för hur federationen ska utvecklas vad avser dess infrastruktur är ett viktigt arbete för att säkra att alla aktörerna ges möjlighet att arbeta med kommande förändringar.

Hantering rekommendation 6
Nämnden ska i samverkan med Förvaltningsforum ta fram en utvecklingsplan. Planen ska ha både ett kortsiktigt såväl som ett mera långsiktigt perspektiv. Planen ska föregås av en omvärlds- och behovsanalys som ska utgöra grunden för planens innehåll. En första version av utvecklingsplanen ska finnas framme senast 1 december 2015.

2.2.3 Analys och förslag till hantering rekommendation 7

E-legitimationsnämnden bör överväga att:
7. På begäran utöka den information som skickas till förlitande parter (exempelvis e-tjänsteleverantörer) med riskinformation vid behov. Detta för att förlitande parter ska kunna göra relevanta riskbedömningar och enklare kunna upptäcka olika typer av attacker.

Bakgrund till rekommendationen (MSB)
Begreppet ”riskinformation” avser i det här fallet den extra information som de ingående parterna (främst tjänsteleverantörerna) kan använda för att beräkna graden av risk för missbruk för en transaktion. Informationen kan omfatta version och leverantör av webbläsarklienten, förekomst av virus- och intrångsskydd på användarens dator mm.
Fördelen med att utbyta riskinformation är att vissa typer av attacker kan avstyras eller upptäckas, t ex. när flera förfrågningar om identitetsintyg inkommer för samma användare från olika länder med kort mellanrum.
Det finns inget tekniskt hinder att lägga till riskinformation i Svensk e-legitimation. Mot bakgrund av detta rekommenderar MSB att E-legitimationsnämnden inför löpande dialog med berörda federationsaktörer där dessa kan, på grundval av genomförda riskanalyser (se avsnitt Riskanalys ovan), ange vilket behov de har av riskinformation.

Nämndens analys
Att exponera tjänster över Internet innebär ökade risker i förhållande till att tjänster enbart finns inom ett slutet känt område. Kunskapen om aktiviteter och beteenden som förekommer inom Internet finns spridd på många olika aktörer. Alla inom federationen för Svensk e-legitimation kan dra nytta av denna kunskap. Här är det viktigt att denna kunskap delas mellan aktörer inom federationen samt att den hanteras och bedöms utifrån ett riskbaserat synsätt.
Hantering av riskinformation är ett relativt nytt område där det krävs gemensamt synsätt på t ex vilka risker som vem kan hantera och vad som kan göras när nya risker uppstår osv. Det krävs ett gemensamt arbete för att hantera den kunskap som finns samt att hitta arbetssätt för att hantera den riskinformation som finns tillgänglig.
Beroende på hur lösningar för delning av riskinformation utformas kan det få större eller mindre påverkan på tjänsterna i federationen.
Utgångspunkten för federationen måste vara att det inom samverkan finns en hög kunskap om de

risker som finns och som bör hanteras, samt att det finns ett gemensamt arbetssätt för hur riskinformation ska hanteras.

Hantering rekommendation 7
Nämnden ska i samverkan med Förvaltningsforum påbörja ett arbete som ska ge ökad kunskap om och förståelse för användningen av riskinformation. Arbetet kan även innehålla försöksverksamhet med klassificering av riskinformation och riskbedömningar. Arbetet ska påbörjas senast 1 januari 2016.

2.2.4 Analys och förslag till hantering rekommendation 8

E-legitimationsnämnden bör överväga att:
8. Ta fram tydliga rekommendationer till e-tjänst- och underskriftsleverantörer avseende utformning av användargränssnitt för att ge användarna liknande upplevelser vid inloggning respektive signering.

Bakgrund till rekommendationen (MSB)
Det finns en tydlig problematik i de flesta E-legitimationssystem där användarna har svårt att särskilja autentisering och signering samt att användare ofta misstar e-legitimationen för en inloggningsmetod snarare än en ID-handling. Detta illusteras i den användbarhetsstudie som genomförts på uppdrag av E-legitimationsnämnden.
I regelverkets användargränssnittsbilaga [ELN-0507], stycke 3.3, finns krav på att eID-tjänsten tydligt ska presentera syftet med identitetsintyget, men utöver detta krav finns inga ytterligare detaljerade krav på hur användargränssnitt för olika tjänster ska utformas.
I och med att det inte finns detaljerade krav i regelverket på hur användargränssnitt ska utformas, t ex. hur handlingen som ska skrivas under presenteras för användaren, är det sannolikt att gränssnittet ser olika ut i olika e-tjänster vilket i sin tur ger minskad tydlighet och sämre upplevd användbarhet sett över samtliga e-tjänster, detta påverkar också säkerheten i systemet.
Tydliga rekommendationer till e-tjänst- och underskriftsleverantörer avseende utformning av användargränssnitt, t ex genom en guide för hur användargränssnitten utformas är därför viktigt för att likrikta systemet. På så sätt uppnås en tydligare användbarhet i systemet och en ökad säkerhet.

Nämndens analys
Rekommendationen avser det stöd som ges till användaren som ska legitimera sig alternativt skriva under en handling. Med den lösning som federationen för Svensk e-legitimation ger innebär det att det finns möjligheter för alla ingående aktörer att skapa gränssnitt som ser likadana ut oavsett vilken aktörs tjänst det är fråga om. Regelverkets krav avseende användargränssnitt innehåller ett antal skall-krav. Dessa är bland annat att det ska vara synligt för användaren vem dvs. organisation, som begärt en legitimering alternativt en underskrift i legitimeringstjänsten. Det finns också krav på att följa standard inom användbarhetsområdet.
Det finns en vägledning (Vägledning för användargränssnitt) som nämnden tagit fram i samverkan med ett antal myndigheter och utfärdare som ger stöd till respektive aktör i deras utformning av användargränssnittet. Men det är upp till varje aktör att följa de rekommendationer som finns beskrivna i vägledningen. Med aktör avses eID-leverantören, tillhandahållaren av e-tjänsten och nämnden som leverantör av Anvisningstjänsten. Underskriftstjänsten har inget gränssnitt mot användaren.
Ett genomförande av denna rekommendation kan ske omedelbart vid anslutning till Svensk e-

legitimation. Och det kan gälla för alla ingående aktörer.
Om alla aktörer inom federationen antar och realiserar det som rekommendationen står för kan det innebära likformning av användargränssnittet vilket kan ge en stor förbättring för användaren.

Hantering rekommendation 8
Vägledningen för användargränssnitt för Svensk e-legitimation ska användas i utvecklingen av elektroniska tjänster inom Svensk e-legitimation.
Nämnden ska i samverkan Förvaltningsforum genomföra ett arbete runt vägledningen med syftet att kommunicera dess innehåll och det ska leda till att vägledningen används vid både utveckling och vidareutveckling av elektroniska tjänster. Arbetet ska starta senast 1augusti 2015.
Nämnden ska i samverkan med Förvaltningsforum fortsätta arbetet med att vidareutveckla vägledningen så att den blir ett stöd till de som utvecklar elektroniska tjänster.

2.2.5 Analys och förslag till hantering rekommendation 9

E-legitimationsnämnden bör verka för att:
9. Det tas fram riktlinjer för oavvislighet, dvs. vad som ska loggas och hur loggar ska hanteras hos berörda parter i Svensk e-legitimation.

Bakgrund till rekommendationen (MSB)
Signering inom Svensk e-legitimation bygger på att en e-tjänst skickar en förfrågan till en signeringstjänst där användarens signatur skapas.
För att kunna skapa signaturen krävs först att användaren har autentiserat sig mot tjänsten.
I praktiken innebär det att användaren inte signerar en handling utan ger underskriftstjänsten en fullmakt att skriva under handlingen i användarens namn, dock utan att underskriftstjänsten fått reda på vad som skrivs under eller kan visa för användaren vad som skrivs under.
Genom det underskriftsförfarande som görs, dvs. att användaren delegerar till e-tjänsten att genomföra en underskrift med hjälp av en underskriftstjänst, så förlorar användaren kontrollen över det som signeras. Detta förfarande innebär potentiellt att en stor uppsättning attacker är möjliga att genomföra där attackeraren kan åstadkomma en falsk underskrift i en användares namn. En falsk underskrift kan innebära både ekonomisk skada för användaren, t ex. genomförande av finansiella transaktioner eller ändring av utbetalningskonto för socialförsäkringar, men även annan skada som avregistrering av ett företag eller en ändring i vald barnomsorg.
Man bör ta höjd för möjligheten att antalet fall där en användare förnekar att det var han/hon som genomförde en underskrift kommer att öka.
För att säkerställa oavvislighet i underskrifter måste loggning och hantering av loggar i e-tjänst såväl som underskriftstjänst vara mycket väl genomtänkt så att dessa möter de krav som ställs för att hålla i t.ex. en domstolsförhandling.
Mot denna bakgrund bör E-legitimationsnämnden därför verka för att ta fram riktlinjer för vad som ska loggas och hur loggar ska hanteras hos berörda parter i Svensk e-legitimation.

Nämndens analys
Underskriftstjänsten tillhandahålls via avrop från ett ramavtal som Kammarkollegiet ansvarar för med nämnden som ansvarig för den normativa specifikationen. Specifikationen innehåller krav på loggning av det som sker i underskriftstjänsten. När underskriftstjänsten är klar lämnas allt resultat tillbaka till e-tjänsten. I resultatet ingår även den logginformation som producerats av

underskriftstjänsten. Det är upp till e-tjänsten att sätta ihop den underskrivna handlingen och arkivera detta tillsammans med alla loggar inklusive den som producerats av underskriftstjänsten.

Riksarkivet är en viktig aktör när det gäller genomförandet av rekommendationen. Myndigheten har ansvar för att stötta offentlig förvaltning i dessa frågor. Det finns riktlinjer och vägledningar för detta arbete. Varje myndighet har ett ansvar att följa dessa.

Genom att ha oavvislighet som grundkrav med sig i utvecklingen av e-tjänster som innehåller underskrift, skapas grunden för ett flöde som går att återskapa när så krävs.

Hantering rekommendation 9
Nämnden ska i samverkan med Förvaltningsforum dela med sig av sina erfarenheter runt hur oavvislighet i underskrivna handlingar kan uppnås. Ett gemensamt arbete i frågan där också Riksarkivet bjuds in ska genomföras senast 1 december 2015.

2.2.6 Analys och förslag till hantering rekommendation 10

E-legitimationsnämnden bör överväga att:
10. Det tas fram riktlinjer för att DoS/DDoS-problematiken hanteras i samtliga lager som hanterar informationsflödet och dess underliggande system: internetaccess, nätverk, applikationslogik, databaser med flera.

Bakgrund till rekommendationen (MSB)

MSB kan konstatera att de aktörer som har e-tjänster och eID-tjänster, själva är ansvariga för att hantera överbelastningshotet för respektive tjänst.
I kravställningen för centrala infrastrukturen framgår, bilaga 3 – Säkerhetstjänster kap 3.3.3 stycke tre följande ang. DDoS-skydd att:
”*Systemet ska skyddas mot belastningsattacker (DDoS). Företrädesvis görs detta i Internetoperatörens domäner*.”
Frågan om DoS och DDoS är dock mycket mer komplex än så och kan inte enbart hanteras hos internetoperatören. Många implementationer och applikationer går att angripa utan att internetoperatören får en indikation på att ett angrepp pågår. Många avancerade angrepp går ut på att efterlikna ”normal” trafik och aktivitet så mycket som möjligt. Exempelvis profilerar en kvalificerad angripare först sitt mål och angriper de funktioner som kräver tid av de olika logiska lagren; presentationslager, logik och backend/databaslager. När dessa punkter är identifierade angrips de vidare.
Det är därför viktigt att DoS/DDoS-problematiken hos alla berörda aktörer hanteras i samtliga lager som hanterar informationsflödet och dess underliggande system: Interaccess, nätverk, applikationslogik, databaser m.fl. Ett av de mer framstående ramverken för säker utveckling som berör ämnet är OWASP Developer Guide.
Genom att ta fram riktlinjer för hur överbelastningsproblematiken kan hanteras inom ramen för Svensk e-legitimation kan E-legitimationsnämnden bidra till att öka säkerheten i systemet.

Nämndens analys

Det måste vara ett skall-krav att alla anslutna aktörer inom federationen kan hantera olika typer av överbelastningsattacker. Det innebär också att de tjänster som nämnden tillhandahåller måste leva upp till samma krav.
Kraven på tillgänglighet på aktörerna inom federationen uttrycks i form av SLA-krav.

MSB med flera myndigheter har god kunskap inom området. Dessa ger också vägledning hur attacker kan minimeras och begränsas.
Utgångspunkten måste vara att alla aktörer inom federationen har tillräcklig kunskap för att värdera den egna organisationens förmåga att hantera överbelastningsattacker.

Hantering rekommendation 10
Nämnden ska säkerställa att de centrala tjänsterna har förmågan att hantera överbelastningsattacker. Det ska vara genomfört senast 1 september 2015. Aktiviteten har koppling till åtgärder för rekommendation 20.
Nämnden tillsammans med Förvaltningsforum ska i samverkan med MSB, ta fram riktlinjer för hur överbelastningsattacker ska hanteras inom federationen. Riktlinjerna ska i sin första version finnas framme senast 1 januari 2016.

2.2.7 Analys och förslag till hantering rekommendation 11

E-legitimationsnämnden bör överväga att:
11. Det finns en regelbunden och tydligare granskning och kontroll, som bör följa en strukturerad metodik. Det som framöver kan övervägas är att, efter systemet är fullt driftsatt, införa tillsyn av systemet i alla dess delar.

Bakgrund till rekommendationen (MSB)
I och med att E-legitimationsnämnden tar fram regelverket samt är den centrala avtalsparten för federationen så vilar ett stort ansvar för federationens säkerhet på E-legitimationsnämnden.
Det finns inget direkt avtalsförhållande mellan E-legitimationsnämnden och leverantörerna av underskriftstjänster. I specifikationen för underskriftstjänster finns inte heller något reglerat om att E-legitimationsnämnden har rättighet att utöva tillsyn av leverantören. Tillsammans innebär detta att dessa tjänster ligger utanför E-legitimationsnämndens kontroll. I dagsläget finns ingen motsvarande information om attributtjänster men det är rimligt att anta att avtalsförhållanden runt dessa kommer att likna de runt underskriftstjänsterna vilket innebär att även dessa faller utanför E-legitimationsnämndens kontroll.
Det finns i praktiken ingen part som har ett helhetsansvar för Svensk e-legitimation i och med att tjänster avtalas och upphandlas av olika parter. E-legitimationsnämnden har dock ett långtgående ansvar att se till att regelverket och tekniska specifikationer är rimliga och korrekta. Däremot har E-legitimationsnämnden ingen juridisk bindande rätt att reglera alla inblandade aktörer då det varken finns någon lag som sanktionerar detta eller något direkt avtalsförhållande mellan E-legitimationsnämnden och vissa aktörer. Dessutom är endast svaga möjligheter runt tillsyn av aktörer inskrivna i regelverket vilket innebär att säkerhetsproblem hos olika aktörer kan döljas, antingen avsiktligt eller oavsiktligt, för E-legitimationsnämnden. Exempelvis regleras tillsyn av leverantör av eID-tjänst i regelverket [ELN-0500], kap 10.1: där det specificeras att 3:e part kan genomföra tillsyn men det måste finnas sakliga skäl att misstänka oegentligheter och minst 14 dagars skriftlig förvarning måste ges innan tillsyn.
Periodisk tillsyn genomförd av oberoende 3:e part är ett mycket viktigt instrument för att säkerställa att aktörer i federationen upprätthåller minimikraven på säkerhet både tekniskt och operationellt inte bara vid anslutningstillfället utan även kontinuerligt över tid. Annars finns det risk för att felaktigheter introduceras, exempelvis vid omkonstruktion, felrättning mm.

Nämndens analys
Begreppet *Tillsyn* används i texten under rubriken **Bakgrund till rekommendationen**. I E-legitimationsnämnden uppdrag ingår ingen tillsynsroll. Om vi däremot likställer begreppet med *kontroll och revision* så ingår det i nämndens uppdrag att följa upp anslutna aktörer och då framförallt leverantör och dess tjänst utifrån i kravuppfyllnad enligt Regelverket.

Underskriftstjänsten finns att avropa från ett ramavtal som Kammarkollegiet äger. Det medför att det finns ett avtal mellan Kammarkollegiet och underskriftsleverantören som reglerar uppfyllnaden av ramavtalet. Den normativa specifikationen som innehåller specifika krav på underskriftstjänsten är en del av ramavtalet. Det innebär att om det finns sakligt skäl att misstänka att leverantören inte uppfyller avtalet kan Ramavtalsägaren ta beslut att genomföra en revision. När det gäller eID-leverantörer finns det reglerat att leverantören själv ska göra internrevisioner och arbeta riskbaserat. Om det finns sakligt skäl att misstänka att leverantören inte uppfyller avtalet kan nämnden göra en revision.
Alla aktörer som är anslutna till federationen med tjänster har ett ansvar att leva upp till det som avtalet kräver. Här är granskningsprocessen och leveransgodkännande ett viktigt instrument för att få hög kvalitet i det som levereras.

Hantering rekommendation 11
Nämnden ska ha en regelbunden dialog med ramavtalsägaren avseende status och uppfyllnaden av den normativa specifikationen för Underskriftstjänsten. Dialogen ska påbörjas senast 1 mars 2015.
Nämnden ska tillhandahålla en mall inklusive beskrivning till aktörerna inom federationen, för hur rapportering av händelser (incidenter) ska gå till. Mallen plus beskrivning ska finnas framme senast 1 mars 2015.
På Förvaltningsforums möten ska det finnas en stående punkt avseende rapportering av händelser som gett störningar i federationen. Ska genomföras senast 1 april 2015.

2.3 Kryptoalgoritmer

2.3.1 Analys och förslag till hantering rekommendation 12, 13 och 14

12. En rutin bör införas för att löpande hantera svagheter i algoritmer rörande krypteringslösningar.
13. Kryptoalgoritmer bör brytas ut till ett eget kravdokument som kan versionshanteras separat.
14. E-legitimationsnämnden bör överväga att stöd för SHA-1 tas bort ur dokumentationen.

Bakgrund till rekommendationen (MSB)
Svagheter identifieras löpande i krypteringslösningar. En del svagheter kommer att vara akuta, medan en del är av karaktären att de föranleder att lösningar av olika skäl kommer att behöva bytas ut inom överskådlig tid. Det är av vikt att kontinuerligt hantera denna säkerhetsfråga, förslagsvis genom att samla krypteringslösningar i ett separat dokument (rutin) som versionshanteras separat, och löpande ses över med avseende på förändringar i standarder och baserat på omvärldsanalys. Detta är även kopplat till rekommendationen kring utvecklingsplan, i en utvecklingsplan kan det t.ex. specificeras när (i framtiden) en viss algoritm inte längre ska stödjas vilket gör att aktörerna har möjlighet att förbereda sig för ett byte.
I 2013-10-30 Tjänstespecifikation Underskriftstjänst som del av Svensk e-legitimation version 1.0

avsnitt 4.5 kravställs vilka signeringsalgoritmer underskriftstjänsten ska stödja. Bland annat krävställs att stöd för RSA med SHA-1. SHA-1 snarast bör tas bort ur dokumentet eftersom det enligt NIST Special Publication 800-131A [SP 800-131A] går att utläsa att SHA-1 inte rekommenderas för användning till signaturgenerering enligt nämnd specifikation.

Nämndens analys

Hög kunskap om kryptoalgoritmer och dess status över tid är en grundförutsättning för att tjänsterna inom samverkan för Svensk e-legitimation ska hålla en hög säkerhet. Det gäller i högsta grad även för underskriftstjänsten som kan avropas och användas i många aktörers tjänster. För att kunna vidmakthålla en hög kunskap krävs regelbunden och återkommande genomgång av området. Behovet av kryptolösningar finns inom många tjänster i dag. Både sådana tjänster som exponeras över Internet men även interna tjänster. Svagheter i de kryptolösningar som används inom federationens tjänster måste därför identifieras och hanteras löpande. Förändringar i kryptolösningar ställer krav på hantering och eventuell anpassning av de tjänster som använder lösningarna.
Alla aktörer som är en del av samverkan i federationen har ansvar för tjänsterna de tillhandahåller. Nämnden har ett ansvar som federationsoperatör att driva arbetet med att ha rätt säkerhet på de kryptolösningar inklusive algoritmer som används inom federationen och då specifikt för de tjänster som nämnden tillhandahåller.
Den genomförda analysen som MSB genomfört har identifierat en kryptoalgoritm (SHA-1) som inte ska användas efter 2013. Underskriftstjänsten som tillhandahålls via ramavtalet ”*E-förvaltningsstödjande tjänster 2010”* ger inte stöd för användning av SHA-1. Dokumentationen är uppdaterad och de tjänster som finns tillgängliga för avrop ger inte möjlighet för användning av SHA-1.
Alla aktörer som ansluter tjänster till Svensk e-legitimation bör se över vilka kryptolösningar som finns i de egna tjänsterna.

Ambitionen för samverkan inom Svensk e-legitimation ska vara att den samlade kunskapen runt kryptolösningar och deras utveckling ska vara hög samt att det ska finnas planer för hur övergången från utgående lösningar ska se ut.

Hantering rekommendation 12, 13 och 14
Nämnden är ansvarig för att det finns ett kravdokument för kryptoalgoritmer. Kravdokumentet ska finnas senast 1 augusti 2015.
Nämnden ska ta fram en rutin för hantering av svagheter i kryptolösningar som används inom federationen. Förvaltningsforum ska kunna lämna synpunkter på rutinen. Rutinen ska finnas framme senast 1 september 2015.
Hänvisning till SHA-1 i den normativa specifikationen för underskriftstjänst är borttagen.

2.4 SAML scenarier

2.4.1 Analys och förslag till hantering rekommendation 15

15. FRA har identifierat ett antal tänkbara angreppsscenarior, som har extrapolerats från den tillgängliga dokumentationen. MSB rekommenderar att E-legitimationsnämnden genomför en analys och vidtar åtgärder för att hantera de identifierade riskerna.

Bakgrund till rekommendationen (MSB)

Genom granskning av dokumentationen har ett antal potentiella särbarhetsaspekter och scenarier noterats ur ett säkerhetsperspektiv. Dessa bör analyseras ur ett angriparperspektiv för att se vilka möjliga konsekvenser de kan leda till, och hur de i så fall på bästa sätt kan avhjälpas. Texten är något förkortad!

Nämndens analys

Det finns ett antal beskrivna scenarier som kan utgöra hot mot federationen för Svensk e-legitimation. Scenarierna är olika till sin karaktär och kräver därför olika lösningar för att minimera risken för att de ska inträffa. Åtgärderna kan bestå av allt från ytterligare regler i Tekniskt ramverk till beskrivning i vägledningar avseende vilka kontroller som olika tjänster måste göra.
Inledningsvis bör nämnden gå igenom regelverket och förstärka där så krävs. Det bör göras snarast möjligt innan utvecklingen av tjänster kommer i gång på bred front. Det är angeläget att ett gemensamt arbete startar som ger ökad kunskap om rätt sätt att utveckla tjänster som ska ingå i federationen. Ambitionen ska vara att federationen för Svensk e-legitimation är en samverkan som bygger på hög säkerhet i tjänsterna och med stor kunskap hos aktörerna av hur det kan uppnås.

Hantering rekommendation 15
Nämnden ska ta fram förslag till hur Tekniskt ramverk kan vidareutvecklas så att risken för att scenarierna inträffar kan minimeras. Förslaget ska finnas framme senast 1 april 2015.
Nämnden ska ta fram vägledning till stöd för utvecklare för att minimera risken för att felaktig implementering i tjänsterna görs.
Nämnden ska i samverkan med Förvaltningsforum genomföra en workshop där scenarierna tillsammans med föreslagna ändringar presenteras. Syftet med workshopen är att verifiera att förslagen är tillräckliga för att minimera riskerna för att scenarierna ska inträffa. Workshopen ska genomföras senast 1 maj 2015.

2.5 SAML kravställning

2.5.1 Analys och förslag till hantering rekommendation 16 - 19

16. – 19. Fyra rekommendationer är kopplade till SAML och den valda implementationen av SAML i Svensk e-legitimation. Dessa rekommendationer har till syfte att stärka säkerheten i systemet som helhet, då SAML är det gemensamma protokoll som ska användas av aktörerna.

Bakgrund till rekommendationen (MSB)

Ett antal specifika rekommendationer kopplade till SAML och den valda implementationen av SAML behandlas här. SAML aspekter har även behandlas i föregående rekommendationskapitel, dock utan specifika åtgärdsförslag. Texten är något förkortad!

Nämndens analys

Det är fyra stycken rekommendationer som finns inom området. Dessa fyra är direkta förslag till hur regelverket ska se ut. Det är viktigt att fortsatt analys görs av innehållet i rekommendationerna. Utgångspunkten för regelverket är att ge stöd för interoperabilitet och möjlighet till att använda färdiga lösningar.
Nämnden bör fortsätta arbetet med innehållet i rekommendationerna. Arbetet bör göras så snart möjligt eftersom resultatet kan påverka de tjänster som utvecklas. Resultatet bör diskuteras

tillsammans med de som utvecklar tjänster. En av rekommendationerna är en feltolkning av hur regelverket ser ut.
Målsättningen för utvecklingsarbetet av tjänster inom federationen bör vara att dessa ska bygga på interoperabilitet mellan tjänster, att det så långt möjligt går att använda standardprogramvara där så är möjligt och att nivån på säkerheten sätts utifrån ett riskbaserat arbetssätt.

Hantering rekommendation 16 - 19
Nämnden ska fortsätta analysen av innehållet i rekommendationerna och komma med förslag på hantering av dessa.
Förslagen ska ingå i det underlag som hanteras i workshopen enligt rekommendation 15 ovan.

2.6 Central infrastruktur

2.6.1 Analys och förslag till hantering rekommendation 20

20. E-legitimationsnämnden bör överväga att låta en oberoende tredje part genomföra en heltäckande säkerhetsgranskning (arkitektur, implementation, hårdvara, mjukvara (både egenutvecklad och COTS) av de centrala tjänsterna i Svensk e-legitimation bl. a. Metadatatjänsten.

Bakgrund till rekommendationen (MSB)
Analysen av den centrala infrastrukturen har inom ramen för detta uppdrag genomförts genom dokumentgranskning, diskussioner med arkitekter för Metadatatjänsten, och läsning av testrapporter i olika revisioner, samt ett platsbesök. En konsekvens av detta är att delar av de observationer som gjorts är subjektiva till sin karaktär.
En oberoende tredje part bör genomföra en heltäckande säkerhetsgranskning eftersom en sådan granskning av den centrala infrastrukturen innebär att tekniska och operativa svagheter i implementationen kan identifieras och åtgärdas, och för att identifiera eventuella brister i kravställningen (dvs. om krav saknats eller varit för lågt ställda).

Nedan följer några utvalda typexempel på noterade aspekter som föranleder denna rekommendation:

- De penetrationstester och säkerhetsanalyser som har genomförts av leverantör och av E-legitimationsnämnden har enbart fokuserat på utvalda delar.
- I Kravställningen (Federationstjänster Bilaga 3 – Säkerhetskrav) lämnas det till leverantören att avgöra vad som är en fastställd rutin för en informationsklassning. Att göra så utan att ange en grundläggande lägstanivå är riskfyllt.
- Kravet på lösenord ”*Det ska finnas regler för utformning, byte och hantering av lösenord*” lämnar mycket öppet för tolkning i och med att det inte anger en lägstanivå, exempelvis på lösenordslängd.
- Noteringar har gjorts rörande val av säkerhetsarkitektur där förbättringar är möjliga. Men, då dessa observationer baseras på diskussioner kan inte alltför långtgående slutsatser dras annat än att en oberoende tredje part bör ges möjlighet att genomföra en fullständig säkerhetsgranskning för att kunna komma med eventuella rekommendationer.

Nämndens analys
De centrala tjänsterna avropades från ramavtalet ”*E-förvaltningsstödjande tjänster2010* ”.

Grundidén med ramavtalet är att avrop ska avse *tjänster* och inte produkter. Det innebär att ingen detaljerad kravställning ska ske på exakt programvara eller liknande. När det gäller godkännandet av specifik tjänst är det nödvändigt att förstå och förvissa sig om att tjänsten uppfyller kraven som ställts.
Det är alldeles riktigt att när det gäller säkerhetsanalyser inkl. penetrationstester så har inga analyser genomförts med extern tredje part i dagsläget.
Resultatet från nämndens riskanalys har identifierat att detta är en risk som ska åtgärdas.
Den centrala infrastrukturen är en mycket viktig del i federationen som måste hålla hög kvalitet och säkerhetsnivå. Den är en förutsättning för tilliten till federationen för Svensk e-legitimation. Det bör därför ske regelbundna säkerhetsanlyser av hela eller delar av den centrala infrastrukturen.

Hantering rekommendation 20
Nämnden ska ta initiativ till att det görs en säkerhetsanalys av den centrala infrastrukturen där analysens omfattning ska bygga på ett riskbaserat synsätt. Analysen ska genomföras av extern part senast 1 september 2015.
Uppdragsbeskrivning för analysen och resultatet ska presenteras för Förvaltningsforum.

2.6.2 Analys och förslag till hantering rekommendation 21

21. E-legitimationsnämnden bör säkerställa att det finns en väldefinierad och publicerad process för godkännande, verifiering och driftsättning.

Bakgrund till rekommendationen (MSB)

I den avtalsmässiga lösning som valts för den centrala infrastrukturen överlåts mycket av hur lösningen ska se ut till tillhandahållaren av den centrala infrastrukturen. Dock specificeras att E-legitimationsnämnden ska godkänna en lösning innan den driftsätts.
Dokumentation om hur ett sådant godkännandeförfarande ser ut saknas dock. Risken med detta är att processen kommer att se olika ut från fall till fall.
Att publicera hur förfarandet ska gå till ökar transparensen och tilltron till systemet.
Vidare framgår

> ”*Genomförande av förändringar i systemets programvara ska strikt kontrolleras, godkännas och testas genom att använda formella processer för detta*.”

I texten framgår det ej vilken typ av tester det rör sig om, men förändringar i miljön bör även säkerhetstestas då det är vanligt att sårbarheter förs in i systemen vid denna typ av förändringar.

Nämndens analys

Den centrala infrastrukturen är en viktig del i federationen för Svensk e-legitimation. Alla förändringar som sker av den kan, om det görs på ett felaktigt sätt, få stor påverkan på hela federationen. Leveransgodkännandet av förändringar som sker i den centrala infrastrukturen är därför en viktig del för att behålla hög kvalitet och säkerhet i den centrala infrastrukturen.
Det finns en framtagen process för godkännande av både tjänsterna och de processer som ska stödja tjänsterna. Genom att förbättra, förtydliga och också publicera hur leveransprovning går till kan ökad säkerhet och transperens uppnås.
Vetskapen om hur förändringar i den centrala infrastrukturen beslutas och genomförs samt hur godkännandet går till ökar kunskapen och tilliten till lösningen.

Hantering rekommendation 21
Nämnden ska publicera processen för godkännande av tjänsterna som nämnden tillhandahåller t ex centrala tjänster och underskriftstjänst. Publiceringen ska ske senast 1 maj 2015.
Nämnden ska presentera processen i Förvaltningsforum med syfte att förbättra och förankra denna. Ska vara genomfört senast 1 maj 2015.

2.6.3 Analys och förslag till hantering rekommendation 22

22. E-legitimationsnämndens kravställning på den centrala infrastrukturen bör i högre grad peka på standarder och ”best practices” inom informationsområdet. Utgångspunkten för detta är de iakttagelser av implementationen som gjorts.

Bakgrund till rekommendationen (MSB)
Kraven på den centrala infrastrukturen bör i större utsträckning peka på standarder och praxis inom säkerhetsområdet, antingen i form av direkta krav eller som referens för att sätta nivån på förväntat säkerhetsarbete. Exempel på dokumentation att peka på:

- Övriga dokument inom ISO 27000-familjen
- NIST-dokument, t ex. [SP 800-53r4] och [SP 800-63-2],
- ”Fundamental Practices for Secure Software Development “ [Safecode],
- OWASP Testing Guide/Developer Guide [OWASP TG]

För de fall där man väljer att inte peka på konkreta standarder och praxis som de listade ovan bör man i stället utöka kravmassan med explicita krav med motsvarande innehåll, så att det säkerställs att det finns kravställning på alla relevanta områden. Texten är något förkortad!

Nämndens analys
Den centrala infrastrukturen är kravställd via avrop på ramavtalet ”*E-förvaltningsstödjande tjänster2010”*, godkänd och levererad i en första version. Vidareutvecklingen av den centrala infrastrukturen kommer att fortgå allteftersom anslutning och användningen av tjänsterna ökar. Den centrala infrastrukturen består av Anvisningstjänst, Metadatatjänst och en webbplats som innehåller information om tjänsterna inom Svensk e-legitimation. Arbetet med att vidareutveckla och förbättra tjänsterna fortgår alltjämt. Det är viktigt att användningen av tjänsterna kommer igång. Det behövs mera erfarenhet av hur tjänsterna fungerar när det finns flera olika aktörers tjänster anslutna.
Utgångspunkten för allt arbete är att de centrala tjänsterna håller hög kvalitet, att det är tydligt vilka krav som ligger till grund för tjänsterna och att de tillhandahålls i en säker och stabil driftmiljö. Kunskapen om standarder och säkerhetsramverk bör förstärkas hos de aktörer som ansluts till Svensk e-legitimation inklusive hos nämnden.
Den fortsatta kravställningen av den centrala infrastrukturen ska bygga på standarder och kända säkerhetsramverk så långt det är möjligt.

Hantering rekommendation 22
Nämnden ska i samverkan med Förvaltningsforum ta initiativ till aktiviteter som ökar kunskapen om tillämpning av standarder och användning av säkerhetsramverk. Arbetet ska påbörjas senast 1 december 2015.