Eva Ekenberg
010-574 87 25

Regeringsuppdrag
Fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv

Eva Ekenberg
010-574 87 25

Innehållsförteckning

Eva Ekenberg
010-574 87 25

Eva Ekenberg
010-574 87 25

1 Sammanfattning och slutsatser

Utifrån genomförda analyser i samband med regeringsuppdraget bedömer E-legitimationsnämnden att säkerheten i Svensk e-legitimation uppfyller det samlade behovet som finns hos offentlig sektors aktörer för de publika e-tjänsterna. Nämnden konstaterar vidare att det är viktigt att arbetet fortsätter med vidareutveckling av kravställningen för att ännu bättre möta behoven och eliminera riskerna. Nya behov av säkerhetsåtgärder behöver fångas upp tidigt och analyseras för att kunna införas på ett säkert sätt i Svensk e-legitimation. Det är viktigt att arbetet blir kontinuerligt och kan utvecklas i samverkan med alla parter inom Svensk e-legitimation. Hur expertmyndigheters kompetens kan tillföras är också en viktig del i det fortsatta arbetet.

2 Bakgrund, aktörer, begrepp och översikt över Svensk e-legitimation

En av de viktigaste förutsättningarna för effektiva och framgångsrika digitala tjänster är att det finns väl fungerande tjänster för elektronisk identifiering, signering och validering. Med hjälp av en e-legitimation kan en användare av elektroniska tjänster både bevisa sin identitet och med elektronisk signatur bekräfta lämnade uppgifter. Regeringen har förstärkt samordningen av användningen av e-legitimationer i den offentliga sektorn genom att den 1 januari 2011 inrätta E-legitimationsnämnden.

E-legitimationsnämnden har i uppdrag att stödja och samordna elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster. Med offentlig förvaltning avses kommuner, landsting och statliga myndigheter, fortsättningen benämnda myndigheter.

Regeringens uppdrag till e-legitimationsnämnden bygger på att den offentliga sektorn fortsatt ska kunna nyttja konkurrerande marknadslösningar på e-legitimationsområdet. Nuvarande avtal löper ut vid halvårsskiftet 2016. För att möta behovet därefter har E-legitimationsnämnden utformat en infrastruktur för e-legitimationer, benämnd Svensk e-legitimation. Infrastrukturen bygger på ett valfrihetssystem, som ger den enskilde rätt att välja leverantör av e-legitimation bland de leverantörer som E-legitimationsnämnden har godkänt.

Visionen är att:

- Svensk e-legitimation ska göra det enkelt och säkert för medborgare och anställda att använda e-tjänster i offentlig förvaltning och privat sektor

Eva Ekenberg
010-574 87 25

- Svensk e-legitimation har ett högt förtroende och är utvecklingsbar

Målen är att:

- Bidra till utveckling och användning av flera e-tjänster i samhället
- Det finns flera utfärdare av Svensk e-legitimation
- Svensk e-legitimation är tillgänglig från 1 juli 2014
- Villkoren är transparenta, förutsägbara och kostnadseffektiva
- Övergången från dagens lösning till Svensk e-legitimation är smidig

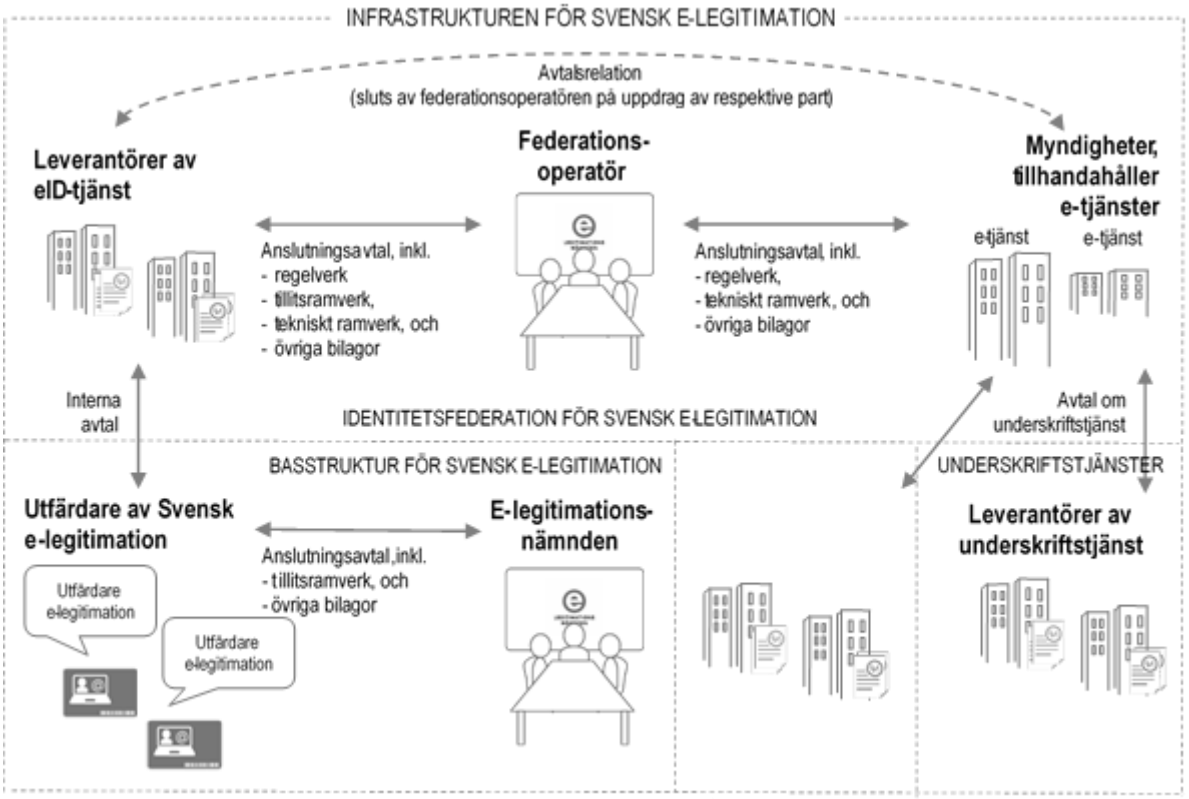
Idag finns i Sverige drygt 7 miljoner e-legitimationer, vilket är en hög penetrationsgrad internationellt sett. E-legitimationer används ca 250 miljoner gånger per år i offentliga e-tjänster av olika slag.

E-legitimationsnämnden tillhandahåller en infrastruktur för elektronisk identifiering, en så kallad identitetsfederation för svensk offentlig sektor. Denna består av det regelverk som nämnden har tagit fram och som bland annat innehåller bestämmelser om tillitsnivåer för e-legitimationer, servicenivåer för i federationen ingående tjänster, skadeståndsbestämmelser och avtalsreglerad möjlighet för E-legitimationsnämnden att utföra kontroll och vid behov stänga av tjänster eller aktörer. Federationen innehåller även vissa centrala tjänster, som metadatatjänst och anvisningstjänst. Myndigheter har möjlighet att avropa underskriftstjänst utifrån den kravspecifikation som E-legitimationsnämnden tillsammans med Kammarkollegiet tagit fram.

I praktiken fungerar valfrihetssystemet så att myndigheterna ger E-legitimationsnämnden i uppdrag att administrera sina valfrihetssystem. E-legitimationsnämnden annonserar efter tjänster för elektronisk identifiering och leverantörer som ansöker om att få delta och som uppfyller kraven ska godkännas. Avtal tecknas därefter mellan myndigheten och leverantören genom E-legitimationsnämndens försorg.

Eva Ekenberg
010-574 87 25

2.1 Översikt över Svensk e-legitimation



Roller och relationer inom Infrastrukturen för Svensk e-legitimation

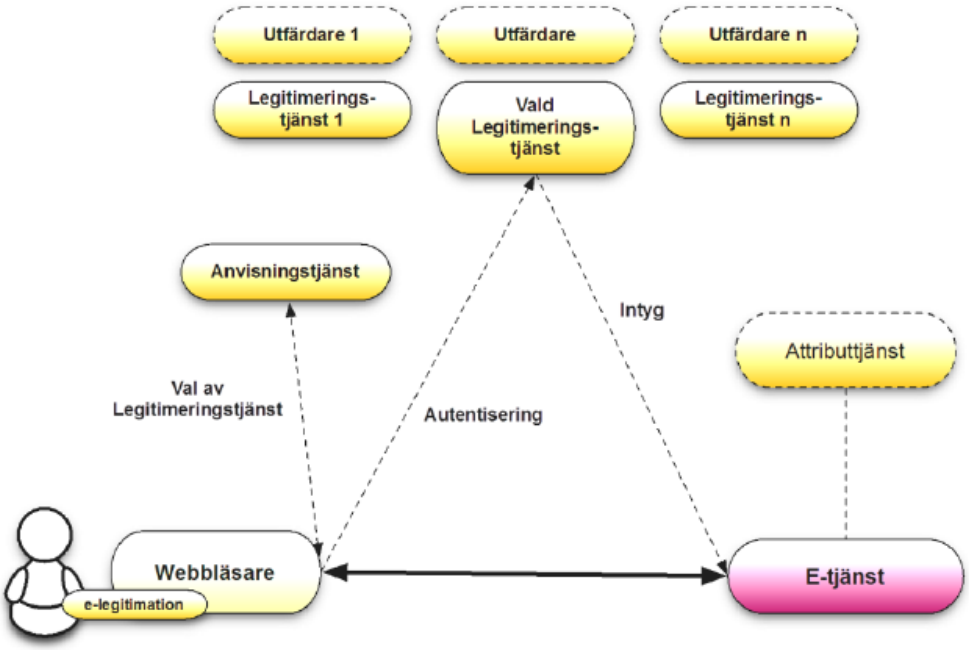
2.1.1 Aktörer och roller

Aktörer, roller och berörda inom infrastrukturen för Svensk e-legitimation i identitetsfederationen för offentlig sektor är följande:

- Myndigheter, kommuner och landsting i svensk offentlig förvaltning som har e-tjänster för allmänheten där det finns behov av elektronisk identifiering eller elektronisk underskrift.
- Leverantörer av eID-tjänst som levererar elektroniska identitetsintyg om innehavaren av en e-legitimation.
- Utfärdare av e-legitimationer, företag som förser enskilda personer med e-legitimationer. En utfärdare kan själv vara leverantör av eID-tjänsten eller ha avtal med ett annat företag.
- E-legitimationsnämnden administrerar infrastrukturen, håller register, utformar och administrerar avtal och regelverk och har rollen som federationsoperatör för den offentliga sektorns identitetsfederation.
- Enskilda personer som använder sina e-legitimationer för att identifiera sig eller skriva under när de använder en e-tjänst i svensk offentlig sektor.

Eva Ekenberg
010-574 87 25

En legitimering går till på följande sätt:



Användaren är inne på en myndighets, kommuns eller landstings e-tjänst. Anvisningstjänsten bidrar med att hjälpa användaren att välja sin variant av Svensk e-legitimation och därmed dirigeras till rätt eID-tjänst. När användaren ska legitimera sig eller genomföra en underskrift går begäran om autentisering från användaren till den eID-tjänst som användarens e-legitimation tillhör.

eID-tjänsten kontrollerar användarens e-legitimation och skickar ett identitetsintyg till myndighetens e-tjänst, där användaren därefter kan komma vidare med sitt ärende.

2.1.2 Styrande dokument

De styrande dokumenten och avtalsstrukturen skapar en sammanhängande infrastruktur och är samlade i federationens regelverk. I avtal förbinder sig aktörerna att följa regelverket som gäller inom federationen. Regelverket gäller även för de utfärdare som är knutna till eID-leverantörer inom federationen.

I regelverket ingår tillitsramverket och det tekniska ramverket. Genom att regelverket anger krav som styr säkerheten i systemet och alla inblandade aktörer förbinder sig att

Eva Ekenberg
010-574 87 25

följa regelverket skapar federationen tillit till systemet. Tillitsramverket ställer krav på utfärdare av e-legitimationer och alla aktörer är bundna av avtal, där tillitsramverket och det tekniska ramverket ingår i avtalets bilagor.

I tillitsramverket regleras säkerheten i utfärdandet av e-legitimationen och utfärdandet av identitetsintyget genom att det här definieras krav på teknisk och operationell säkerhet hos utfärdaren och på kontroll av att en person som tilldelas en elektronisk identitet verkligen är den han eller hon utger sig för att vara. Det kan finnas flera olika tillitsnivåer, graderade nivå 1 till 4. För närvarande har E-legitimationsnämnden annonserat valfrihetssystem för svensk offentlig sektors identitetsfederation för tillitsnivå 3.

Alla som utfärdar identitetsintyg måste visa att hela den process som ligger till grund för utfärdandet uppfyller kraven i den aktuella tillitsnivån, vilket innefattar krav på

- skapandet av identitetsintyget
- utfärdandeprocessen med verifiering av identiteten
- e-legitimationen och dess användning
- utfärdaren av e-legitimation

Det tekniska ramverket beskriver de tekniska specifikationerna som ska gälla för aktörerna.

Anslutningsavtal finns för utfärdare, leverantörer av eID-tjänster och för den offentliga sektorns tillhandahållare av e-tjänster. Genom anslutningsavtalen knyts aktörerna till regelverket och utfäster sig att följa detta.

- Offentliga sektorns tillhandahållare av e-tjänster förbinder sig att följa reglerna i regelverket och får begära och ta emot identitetsintyg i anslutning till sina e-tjänster
- Leverantör av eID-tjänst förbinder sig att följa reglerna i regelverket och leverera identitetsintyg
- Utfärdare förbinder sig i sitt anslutningsavtal att följa reglerna i tillitsramverket
- E-legitimationsnämnden förvaltar identitetsfederationen för offentlig sektor, administrerar anslutningsavtal och tillhandahåller metadataregister

Avtalsrelationer ska i valfrihetssystemet upprättas direkt mellan de myndigheter, kommuner och landsting som tillhandahåller e-tjänster och samtliga leverantörer av eID-tjänster. I praktiken löses detta genom att myndigheterna uppdrar åt E-legitimationsnämnden att för deras räkning ingå avtal med befintliga och tillkommande leverantörer av eID-tjänst.

Anslutna aktörer har rätt att använda federationens kännetecken på sina webbplatser.

Eva Ekenberg
010-574 87 25

2.1.3 De centrala tjänsterna

De centrala tjänsterna metadatatjänst och anvisningstjänst är upphandlade av E-legitimationsnämnden och i leveransavtal ställs krav och villkor på leverantören. Metadatatjänsten är en viktig centralpunkt i infrastrukturen och tjänsten är upphandlad med säkerhetsskyddsavtal.

Underskriftstjänsten är en möjlighet för myndigheter, kommuner och landsting som tillhandahåller e-tjänster att avropa på Kammarkollegiets ramavtal *E-förvaltnings-stödjande tjänster 2010*. I regelverket finns en normativ specifikation över underskriftstjänsten som säkerställer att den är tydligt definierad och kravställd. E-legitimationsnämnden har i samverkan med Kammarkollegiet funktionsprovat underskriftstjänsterna.

E-legitimationsnämnden för ett register över aktörer i federationen, metadataregistret, med de aktörer i offentlig sektor som tillhandahåller e-tjänster och leverantörerna av eID. I registret finns information om identitetsfederationens medlemmar och de nycklar som krävs för säker kommunikation och informationsutväxling mellan tjänster. Där finns också annan information som är viktig för samverkan mellan tjänster, till exempel internetadresser, information om tillitsnivåer, tjänstekategorier och användargränssnitts-information. Registret är elektroniskt signerat.

Identitetsfederationen förutsätter att eID-tjänster och tillhandahållare av e-tjänster litar på varandra. Därmed kan de verifiera de signaturer som används i kommunikationen dem emellan genom att de litar på varandras signeringscertifikat.

Anvisningstjänsten är en central tjänst som hjälper e-tjänsterna att ge användarna stöd för hur dessa väljer sin e-legitimation och därmed legitimeringssätt.

De e-tjänster som kräver underskrift behöver inte anpassas efter olika användares e-legitimationer för att skapa underskrift, utan e-tjänsten kan överlåta detta till en underskriftstjänst. I denna kan användare med stöd av Svensk e-legitimation ges möjlighet att underteckna elektroniska handlingar.

3 Offentlig sektors behov av användning av e-legitimationer i digitala tjänster

Offentlig sektors behov av e-legitimationer har uttryckts i många dokument som lett fram till bildandet av E-legitimationsnämnden och Svensk e-legitimation. Exempel ges nedan från E-delegationen, Regeringen och Sveriges Kommuner och Landsting. Vidare presenteras dagens användning av e-legitimationer och de behov som några myndigheter gett uttryck för på E-legitimationsnämndens förfrågan.

Eva Ekenberg
010-574 87 25

3.1 Offentlig sektors behov

3.1.1 E-delegationens avsiktsförklaring

E-delegationen har i början av 2014 formulerat en avsiktsförklaring där de 16 statliga myndigheter som är delegationens medlemmar uttalar sin avsikt att teckna avtal om medverkan i den identitetsfederation för offentlig sektor som E-legitimationsnämnden ansvarar för och där SKL uttalar att de har för avsikt att rekommendera sina medlemmar att teckna avtal.

3.1.2 Regeringens proposition 2012/13:123

Regeringen skriver i Proposition 2012/13:123, Myndigheters tillgång till tjänster för elektronisk identifiering: ”Det har dock hela tiden funnits ett tryck på att utveckla säkra lösningar för elektronisk identifiering och elektroniska signaturer. Skälet till detta är att det i många ärenden finns behov av säker identifiering, krav på underskrift och krav på skydd för den personliga integriteten. En förutsättning för en effektiv och säker e-förvaltning är att alla som behöver använda e-tjänster har tillgång till enkla och säkra metoder för elektronisk legitimering. Med en elektronisk legitimation (e-legitimation) kan en användare styrka sin identitet. Den som driver e-tjänsten kontrollerar genom en tjänst för elektronisk identifiering (eID-tjänst) att den e-legitimation som används är giltig.”

…
”E-legitimationer fyller en viktig funktion inom e-förvaltningen. Möjligheten till säker elektronisk identifiering medför framför allt att det går att på ett enkelt och tillförlitligt sätt hantera ärenden enklare och billigare. Innehavaren kan med sin e-legitimation bevisa sin identitet vid inloggning till en myndighets e-tjänst. Det gör det möjligt för myndigheten att visa information som finns hos myndigheten och som rör individen i fråga, men som andra inte ska ha tillgång till. En säker identifiering innebär också att myndigheten kan fastställa vem som har lämnat uppgifter i e-tjänsten. Med hjälp av elektroniska signaturer kan användarna även bekräfta lämnade uppgifter.

E-legitimationer bidrar till att medborgaren enkelt och säkert kan sköta sina ärenden hos myndigheterna. E-legitimationer används exempelvis vid ansökan om bidrag, vid deklarationer och vid ansökan om förskoleplats. I stället för att papper skickas fram och tillbaka med post gör e-legitimationer och e-tjänster att det blir enklare, billigare och snabbare att kontakta myndigheterna och hantera sina ärenden. Dessutom kan användarna själva se vilka bidrag som sökts, se vilken plats de har i förskolekön, göra ändringar i inkomstdeklarationen osv., utan att andra kan ta del av uppgifterna.”

Eva Ekenberg
010-574 87 25

3.1.3 SKL:s strategi för e-samhället

Sveriges kommuner och landsting skriver i dokumentet Strategi för e-samhället:

”Sverige är bland de främsta länderna i världen när det gäller e-förvaltning och IT-mognad. Men utvecklingspotentialen är mycket stor och gränserna för vad som är möjligt förflyttas hela tiden. Allt fler tar för givet att ärenden ska kunna utföras enkelt och säkert via nätet.

…
Hur informationens säkerhetsnivå ska klassificeras och hur man styr vem som har tillgång till viss information kräver breda överenskommelser. En viktig grundbult i arbetet med att utveckla e-förvaltning är att alla grupper av privatpersoner garanteras en elektronisk identitet. Medarbetare och utförare behöver också e-legitimationer i tjänsten samt behörighetssystem som är kopplade till dessa. … E-legitimationsnämnden, i vilken SKL deltar, har i uppdrag att ta fram en Svensk e-legitimation. Denna ska bygga på en federativ modell som möjliggör att olika lösningar för autentisering och auktorisering kan samverka och ge åtkomst till andra aktörers register och tjänster. Detta skulle förenkla för privatpersoner, företag och medarbetare som bara behöver identifiera sig en gång vid varje givet tillfälle. De administrativa stödprocesserna för identitets- och behörighetshantering är förutsättningar för att autentisering och åtkomstkontroll ska fungera. Rätt kvalitet på informationen som beskriver identiteter och behörighet för privatpersoner och medarbetare är grundläggande. Landstingen har tillsammans tagit fram lösningar för identitets- och behörighetshantering inom eHälsa. Kommunerna har möjlighet att använda dessa lösningar. För de allra flesta kommunerna är det svårt att ensamma hantera och klara säkerhetskraven enligt rådande bestämmelser inom området för vård och omsorg.”

Eva Ekenberg
010-574 87 25

3.2 Dagens användning och andra behovsindikatorer

Dagens användning av e-legitimationer i digitala tjänster ger en uppfattning om behovet. De senaste siffrorna[1] som samlats in härrör från 2012 och ser ut på följande sätt:

Myndighet, kommun eller landsting	Antal legitimeringar och underskrifter, st
Skatteverket	28 miljoner
Försäkringskassan	20 miljoner
Centrala studiestödsnämnden	3 miljoner
Stockholms Läns Landsting Mina vårdkontakter	2,3 miljoner
Bolagsverket	1,7 miljoner
Pensionsmyndigheten	1,6 miljoner
Arbetsförmedlingen	1,5 miljoner
Transportstyrelsen	1,3 miljoner
Stockholms stad	0,9 miljoner
Jordbruksverket	0,4 miljoner
Sundsvalls kommun	0,14 miljon
Linköpings kommun	0,02 miljon
Sandvikens kommun	0,01 miljon

Skatteverkets har presenterat ytterligare statistik med uppgifter från 2011-2013, vilka visar på en stadigt ökande användning av e-legitimationer i Skatteverkets verksamhet, framför allt när det gäller underskriftsdelen:

Skatteverket	2011	2012	2013
Totalt antal inloggningar med e-legitimation	15 miljoner	16 miljoner	16 miljoner
Totalt antal underskrifter med e-legitimation	10 miljoner	12 miljoner	14 miljoner

[1] E-legitimationsnämnden ”Marknaden år 2012 för elektronisk legitimering och underskrift inom offentlig sektor” PM 2013-04-26 med undersökning baserad på Kammarkollegiets statistik från ramavtalsleverantörer och uppgifter från myndigheter, kommuner och leverantörer.

Eva Ekenberg
010-574 87 25

För 2014 räknar Skatteverket med en 30-40 % ökning av användning av e-legitimation i sina e-tjänster.

3.3 Enskilda myndigheters behov av e-legitimationer i digitala tjänster

I samband med detta uppdrag har E-legitimationsnämnden ställt frågor om behoven och synen på säkerhet till några myndigheter som använder e-legitimationer och till Sveriges kommuner och landsting. Frågorna rör utgångpunkter för säkerhetsarbetet inom Svensk e-legitimation.

Myndigheter med behov av e-legitimationer som har kommit in med svar är Skatteverket, Bolagsverket, Arbetsförmedlingen och Sveriges kommuner och landsting Dessa svar finns redovisade i Bilaga, se avsnitt 9.

De myndigheter som har svarat har ansett att regelverket fungerar som kravställning för konceptets säkerhet, att det tekniska regelverket är tillräckligt konkretiserat, att lösningen med offentlig federation är bra och att sårbarhetsaspekterna har omhändertagits tillfredställande.

Några synpunkter som har framförts är:

- Kontrollfunktionen att utfärdare och tjänsteleverantörer verkligen tillämpar regelverket är oklar
- Tillgänglighetskraven är lågt satta för att fylla krav från vården
- Gemensamma e-tjänster där både offentliga myndigheter, kommuner eller landsting och privata aktörer agerar i samma tjänst – hur ska detta hanteras?
- Kraven på säkerhet och godtagbar risknivå är beroende av vilka e-tjänster som i framtiden kommer att utnyttja e-legitimation, detta är svårt att bedöma
- Regelverkets språk bör kunna vara mer lättillgängligt
- Tydlig ändrings- och livscykelhanering av regelverket behöver kommuniceras
- Förvaltningsforum behöver snarast etableras
- Informationsmöten och workshops behöver fortsättningsvis ordnas
- Material på webbplatserna för E-legitimationsnämnden och Svensk e-legitimation behöver målgruppsanpassas bättre

4 Analyser av Svensk e-legitimation från ett säkerhetsperspektiv

I detta avsnitt redovisas E-legitimationsnämndens analys utifrån det hittillsvarande arbetet med uppbyggnad av federationen och regelverket, genomförd riskanalys, bidrag från de myndigheter som har lämnat synpunkter eller fört dialog under arbetet.

Eva Ekenberg
010-574 87 25

Analysen är baserad på de behov och synpunkter som myndigheterna har uttryckt och i dialog med MSB. MSB har även anlitat expertmyndigheter såsom FOI, MUST och FRA vilka har bidragit till MSB:s analyser.

4.1 De enskilda användarnas perspektiv

Tillit och enkelhet
Från en enskild användares perspektiv är det viktigt att det finns en allmänt accepterad tillit till systemet. Eftersom e-legitimation är väl etablerat idag och ambitionen är att användarna inte ska få någon större förändring vid övergång till det nya systemet är det troligt att den höga tilliten kommer att finnas kvar. Anvisningstjänsten kommer att förenkla för användarna att dirigeras till rätt eID-tjänst.

E-legitimationsnämndens vägledning för e-tjänster och legitimeringstjänster kommer att leda till att tjänsternas gränssnitt liknar varandra vilket underlättar för användaren som kommer att känna igen sig.

Det är också viktigt att det finns information i samhället om att en användares dator inte är att betrakta som en säker miljö så att användaren blir mer medveten om risker.

Genomförda riskanalyser visar att oönskade händelser kan inträffa om systemet Svensk e-legitimation skulle brista i säkerhet. Som konsekvens skulle brister kunna orsaka att användare kan riskera att drabbas av felaktigt utställda identitetsintyg med fel information i intygen, att obehöriga får åtkomst till uppgifter eller identitetsstöld. Dessa händelser kan potentiellt få svåra konsekvenser. Hela arbetet med uppbyggnad av regelverket och den infrastruktur som Svensk e-legitimation består av har tagit hänsyn till dessa risker vid kravställning och konstruktion av de olika delarna av Svensk e-legitimation.

Användargränssnitt och underskrifter
Användargränssnitt och utformningen av e-tjänster är viktiga för de enskilda användarnas tillit och för hur användbara de uppfattar e-tjänsterna och användningen av e-legitimationer. Anvisningstjänsten bidrar till att förenkla för användaren.

Det finns krav i regelverket att det ska visas vem som begärt identifieringen när användaren verifierar sin e-legitimation. Detta gör att användare vet hos vilken myndighet eller e-tjänst inloggningen sker.

När en e-tjänst har krav på elektronisk signatur kan en underskriftstjänst användas. Teknisk sett innebär underskriftstjänsten att användaren legitimerar sig, en checksumma av den handling som ska signeras skickas till underskriftstjänsten från e-tjänsten och därefter signerar underskriftstjänsten checksumman så att det skapas en elektronisk signatur för användarens räkning. Denna lösning har etablerats så att underskrift ska vara enkel att utföra för användare utan speciell programvara och enkelt att införa för e-tjänster. Endast en checksumma skickas till underskriftstjänsten, hela dokumentet skickas

Eva Ekenberg
010-574 87 25

aldrig. Handlingen som ska skrivas under lämnar aldrig myndigheten. Ingen ökad säkerhet uppnås av att hela dokumentet kommer in i underskriftstjänsten.

Underskriftstjänsten kommer efter utförd signering att skicka över till e-tjänsten all information och loggar som skapades vid signeringen. E-tjänsten bestämmer vilken information som ska bevaras (arkiveras). E-tjänsten ansvarar för att nödvändig information om signaturen arkiveras bl.a. i syfte att kunna styrka att signaturen har skapats av rätt person.

Användargränssnittet hos e-tjänsterna spelar en stor roll när det gäller att användaren blir uppmärksam på vad underskriften innebär och kan skilja på underskrift och legitimering. Användargränssnittet ska enligt regelverket utformas så att det är tydligt vad som är legitimering och vad som är underskrift och det ska även utformas så att det är tydligt vad användaren skriver under.

Som exempel har Skatteverket kravet att kunna skicka med en beskrivande text vid underskrift: ex:

"Du skriver nu under din inkomstdeklaration för inkomståret 2013"
"Du skriver nu under intyg för att Kalle Karlsson 3910dd-xyzw blir ombud för dig"

E-legitimationsnämnden har tagit fram en vägledning riktad till myndigheters e-tjänster som ger råd hur e-tjänsten bör utformas så att användare förstår vad som händer.

Mobilitet
Flera tillhandahållare av e-tjänster har efterfrågat hur användning av mobila enheter kan stödjas av den teknik som Svensk e-legitimation bygger på.

Svensk e-legitimation kan för många e-tjänster användas i mobila enheter, till exempel när användaren kommer till e-tjänsten via en webbläsare i den mobila enheten. Möjligheten att använda Svensk e-legitimation är beroende av hur de offentliga aktörerna har valt att utforma e-tjänsten när den används från de mobila enheterna. Några aktörer använder sig av tekniken för inbyggda appar (så kallade native appar) i de mobila enheterna. Det finns inget standardiserat sätt att utveckla dessa appar då de mobila enheterna ställer olika krav, vilket gör att särskild hänsyn måste tas i app-utvecklingen till hur respektive mobil enhet kan användas tillsammans med Svensk e-legitimation.

E-legitimationsnämnden driver ett arbete kring tekniken för native appar för att erbjuda det stöd som behövs. Ett viktigt krav även i det sammanhanget är naturligtvis att användning av mobila enheter kan ske med nödvändig säkerhet.

4.2 Infrastrukturen som helhet

Svensk e-legitimation kännetecknas av höga krav på såväl säkerhet som användbarhet samt hög komplexitet med många aktörer som måste samverka väl. Ansvaret är delat på

Eva Ekenberg
010-574 87 25

många och beroendet av god samordning och koordinering är stort. Kraven på hög tillgänglighet och god funktion är mycket höga.

Konceptet för Svensk e-legitimation bygger på väl utformade och utförda processer och delar med kvalificerad teknik i en IT-värld som på många sätt är utsatt för risker som kan genereras både med och utan uppsåt.

Konceptets riskbedömning måste utgå från att det finns risker som kan utlösas. Tekniken liksom hotbilden utvecklas ständigt, nya sårbarheter upptäcks, incidenter kan inträffa som medför olika grad av negativ påverkan. Nya innovationer på IT-området medför ständigt nya krav på utveckling och anpassning. Samtidigt är samhället i hög grad beroende av de digitala offentliga tjänster som Svensk e-legitimation ska bidra till att skydda och skapa förtroende för.

4.3 E-legitimationsnämndens arbete med informationssäkerhet

E-legitimationsnämndens säkerhetsarbete utgår från en riskanalys där identifierade risker och dess konsekvenser är grunden till nödvändiga skyddsåtgärder. Säkerhetsarbetet måste vara kontinuerligt och ingå i verksamhetens processer med tydliga relationer till samverkande aktörer. De skyddsåtgärder som tillämpas måste utvärderas och korrigeras löpande.

Kraven på konceptet är i vissa fall motsatser till varandra. Hög säkerhet kontra god användbarhet. Aktörer inom både privat och offentlig sektor som delvis har olika behov och krav. Komplexa funktioner med många samverkande aktörer kontra krav på rimliga kostnadsnivåer är några exempel.

E-legitimationsnämnden har ansvar för att upprätthålla regelverket, ansvar för kravställning och ansvar för att granska kravuppfyllnad hos utfärdarna. Beslut om förändringar av regelverket ska fattas inom federationen. Regelverket anger hur förändringar får göras.

I tillitsramverket finns krav på utfärdarna i fråga om

- Organisation och styrning
- Informationssäkerhet
- Villkor för underleverantörer
- Spårbarhet, gallring och handlingars bevarande
- Granskning och uppföljning
- Fysisk, administrativ och personorienterad säkerhet
- Teknisk säkerhet
- Ansökan, identifiering och registrering
- Utfärdande och spärr av e-legitimation
- Kontroll av elektronisk identitet och utställande av identitetsintyg

Eva Ekenberg
010-574 87 25

I det tekniska ramverket anges de tekniska specifikationer som gäller inom federationen. I detta finns normativa krav som E-legitimationsnämnden, leverantörerna av eID-tjänst och myndigheter som tillhandahåller e-tjänster måste följa.

4.3.1 Ledningssystem

E-legitimationsnämnden har antagit ett Ledningssystem för informationssäkerhet. Ledningssystemet omfattar såväl det interna arbetet inom E-legitimationsnämnden och dess kansli som infrastrukturen för identitetsfederationen.

När det gäller identitetsfederationen är det regelverket som är de styrande dokumenten och ledningssystemet hänvisar i dessa frågor till kraven i regelverket. Detta innebär att kraven i regelverket ingår i de processer som ledningssystemet föreskriver.

4.4 Risker

4.4.1 Riskanalys och åtgärdsplan

E-legitimationsnämnden genomförde en riskanalys för konceptet Svensk e-legitimation under 2012-2013 med metodstöd från MSB.

Resultatet av genomförd riskanalys har påverkat de krav som ställs på samtliga aktörer inom ramen för konceptet. Kraven finns uttryckta i regelverket.

Som ett resultat av bl. a. riskanalysen men också utifrån krav som ställs på myndigheter pågår ett införande av former för ett kontinuerligt informationssäkerhetsarbete i E-legitimationsnämndens verksamhetsprocesser (LIS). I det arbetet ingår också analys och säkerhetsaspekter kopplat till berörda intressenter och aktörer.

Ett fokusområde för riskanalysen och det fortsatta säkerhetsarbetet är naturligtvis också användarperspektivet. Det gäller risker för identitetsstöld, felaktig utgivning, missbruk av annans identitet och integritetsproblematiken där risken för att personuppgifter görs tillgängliga på ett oacceptabelt eller lagstridigt sätt. Användbarheten är också en viktig faktor för att möjliggöra enkel användning och acceptans för Svensk e-legitimation.

4.4.2 Risker i E-legitimationsnämndens riskanalys

Nedan beskrivs några av de identifierade riskerna som behandlats i den riskanalys som E-legitimationsnämnden arbetar med. De tänkbara händelserna, hoten och riskerna är bedömda enligt en skala med konsekvenser vid utlöst risk och sannolikhet att risken inträffar. Konsekvenser kan vara begränsade, måttliga, betydande eller svåra medan sannolikheten kan vara obefintlig, liten, måttlig eller stor. För varje identifierad risk har åtgärder för att minska risken angivits.

Varje risk är bedömd för följande händelsetyper:

- Risker som skapar olägenhet, oro eller ryktesskada
- Finansiell skada eller skadeståndsansvar

Eva Ekenberg
010-574 87 25

- Röjande av känslig information till obehöriga
- Straffrättsligt brott
- Skada på verksamhet eller allmänintresse
- Personsäkerhet

De allvarligaste hoten ur ett säkerhetsperspektiv utgörs framförallt av händelser som leder till röjande av känslig information, brott, personsäkerhet eller skada på verksamhet eller allmänintresse. Nedan beskrivs risker ur analysen som E-legitimationsnämnden har bedömt ha måttliga eller svåra konsekvenser och ha måttlig eller hög sannolikhet. I sammanställningen tas också risker och hot med som identifierats i den senaste tidens dialog med MSB och med andra myndigheter.

Hot på grund av brister i organisation

Eventuella brister i hur E-legitimationsnämnden utför sitt uppdrag som ansvarig för basstrukturen kan utgöra hot mot infrastrukturen. Några exempel är om godkännandeprocessen inte fungerar och en eID-leverantör eller utfärdare som inte håller måttet blir godkända. Bristande resurstillgång eller kompetens kan leda till bristfällig kravställning, dålig kvalitet i uppföljning, dålig anpassning av kravställningen till omvärldsutvecklingen och därmed bristande kvalitet i de centrala tjänsterna.

Konsekvenserna kan bli att e-legitimationer ges ut felaktigt, till exempel till fel användare eller inte håller säkerhetsmässigt tillräckligt hög nivå.

Risker reduceras med en väl utformad process för godkännande av leverantörer med insyn från flera aktörer, tydliga ansvarsbeskrivningar, väl fungerande och tekniskt relevant testmiljö och med regelbundet genomförda kontroller av leverantörer och processer. Vidare elimineras risker med god verksamhetsplanering inom E-legitimationsnämnden, regelbunden kvalitetsutvärdering och god respons från uppdragsgivaren på behoven. Det är också viktigt att arbetet bedrivs så att de aktörer som är beroende av infrastrukturen får insyn och kan påverka arbetet på lämpligt sätt.

Om E-legitimationsnämnden inte skulle agera tillräckligt på en anmäld säkerhetsbrist eller misstanke om brist hos en utfärdare, att nämnden skulle brista i sin förmåga att hantera säkerhetsbrister eller om E-legitimationsnämnden inte följer den tekniska utvecklingen, identifierade säkerhetshot och inträffade incidenter kan det ge svåra konsekvenser. Resultatet blir att Svensk e-legitimation inte anpassas till olika säkerhetshot.

Risken reduceras med tydliga krav på en sammanhållen incidentrapportering- och hanteringsprocess där samtliga aktörer vet sina roller, uppgifter och ansvar. Tillräcklig kompetens och resurser hos nämnden och regelbunden uppföljning och revision av utfärdare. Ett tydligt fördelat ansvar mellan aktörer, väl utformade avtal och dialog med aktörerna reducerar också risken.

Eva Ekenberg
010-574 87 25

Om E-legitimationsnämnden inte skapar förvaltningsforum och inte fångar upp och skapar förutsättningar för förändringar när säkerhetsutvecklingen kräver det, uppstår liknande brister. Den komplexa uppbyggnaden av avtal kan också göra att systemet blir trögrörligt, att nödvändiga förändringar tar för lång tid.

Risken kan få svåra konsekvenser och går att reducera men inte att fullständigt eliminera.

I händelse att ansvarsförhållandena är alltför otydliga kan en incident eller ett problem leda till att ingen tar ansvar. Denna risk är liten men konsekvenser kan vara betydande. Risken elimineras med tydliga ansvarsförhållanden och heltäckande incidentrapportering och hantering.

Hot på grund av brister i de centrala tjänsterna och tekniska lösningar

Brister i de centrala tjänsterna, det vill säga metadatatjänsten, anvisningstjänsten och underskriftstjänsten kan leda till stora störningar. Händelser som skulle innebära svåra konsekvenser men med måttlig eller liten sannolikhet. Riskerna reduceras genom väl fungerande incidentrapportering och samordnade kontinuitets- och beredskapsplaner liksom krav på redundans och driftkapacitet. Regelverket bidrar till att minska riskerna.

Det ständigt aktuella hotet att det kan finnas säkerhetsluckor i den offentliga identitetsfederationen som ännu inte upptäckts måste alltid mötas med kontinuerlig och heltäckande riskhantering, eftersom konsekvenserna kan vara mycket svåra. Sårbarhet på grund av säkerhetsluckor kan till exempel medföra risker i form av intrångsförsök, missbruk av andra identiteter eller överbelastningsattacker mot de ingående aktörernas system. Riskerna reduceras med kontinuerlig omvärldsbevakning och experthjälp i säkerhetsteknisk analys av processens delar, något som ska ske regelbundet för att identifiera sårbarhet och dess konsekvenser. En viss kvarstående risk finns alltid. En närliggande risk är att de krypteringsmetoder eller de standarder som systemet bygger på anses inte längre säkra eller betrodda, även detta hot kräver ständigt omvärldsbevakning och kunskaper om metoder och standarder. Implementering av SAML-protokollet måste göras på bästa sätt, med programvaror som hanterar kända hot och med korrekt validering av identitetsintyg.

Signering av metadata och en process för kontroll att metadata är korrekt minskar riskerna för felaktigheter i metadata. Risken för obehörig åtkomst till metadataregistret möts med åtkomstshantering och loggning. Det är också viktigt att de aktörer som är användare av metadataregistret kontrollerar att hämtat data är korrekt signerat.

Överbelastningsattack mot någon av aktörerna inklusive en central tjänst kan orsaka driftsstopp. Det är viktigt att alla inblandade har ett gott skydd mot DoS och DDoS-attacker. Anvisningstjänsten bygger på möjligheten till lokal hantering vilket reducerar risken.

Eva Ekenberg
010-574 87 25

Hot på grund av brister hos leverantör av eID-tjänst eller utfärdare

Om en leverantör av eID-tjänst skulle ha stora brister i sin tjänst avseende autentisering av användare och leverans av identitetsintyg, uppstår allvarliga konsekvenser ur ett säkerhetsperspektiv. Bristerna kan innebära bland annat felaktigt utställda identitetsintyg, fel information i intygen och obehörig åtkomst och identitetsstöld.

En annan händelse som medför risk är att en oseriös utfärdare uppfyller villkoren och ansluts.

Hoten har svåra konsekvenser och reduceras med tillämpning av regelverket i form av kravställning, testning, granskningar, uppföljning och verkställande av sanktioner.

4.4.3 Analys av regelverket

Synpunkter och bidrag i analyser har kommit från flera håll. Via MSB har FOI, MUST och FRA bidragit. Andra sakkunniga myndigheter som har besvarat E-legitimationsnämndens frågor är Datainspektionen, RPS och Sunet.

Regelverket för Svensk e-legitimation är den stomme som bygger upp säkerheten. Samtliga aktörer är bundna till regelverket med civilrättsliga avtal. De dokument som är mest intressanta ur säkerhetssynpunkt är det tekniska ramverket och tillitsramverket.

Det tekniska ramverket och tekniska specifikationer anger standarder och andra tekniska detaljer.

Tillitsramverket är utformat för att styra tillitsnivåer. Ramverket är avsiktligt utformat för att vara teknikneutralt och tillåta olika tekniska lösningar. Tillitsramverket är baserat på den internationella standarden ISO 29115 men har också hämtat kunskap från STORK[2] QAAA modell och Kantara[3].

Sunet har framfört synpunkten att högre krav kan ställas på oberoende revision av identitetsutfärdare i tillitsramverket för att garantera att granskningar sker på oberoende sätt och förordar att tillitsramverket Kantara används istället för E-legitimationsnämndens eget ramverk.

Rikspolisstyrelsen har i samtal betonat vikten av att identifieringen är god.

God samstämmighet
I samband med MSBs genomgång av Svensk e-legitimation har bl.a. regelverket analyserats och sammanfattningsvis kan sägas att dagens regelverk överlag visar god samstämmighet på hög nivå med övriga regelverk och standarder som finns publicerade. Regelverket är sparsamt med detaljkrav vilket innebär tolkningsutrymme för vad kraven egentligen betyder.

---

[2] European eID Interoperability Platform, EU-projekt

[3] Kantara, sammanslutning i syfte att främja identity management.

Eva Ekenberg
010-574 87 25

MSB har studerat överensstämmelse mellan regelverket och standarder och andra styrande dokument ur aspekterna personuppgifter, ledningssystem för informationssäkerhet, riskhantering, tillsyn, incidenthantering och sanktioner och har även gjort jämförelse med kravställningar i EU-förordningen eIDAS, med det amerikanska FIPS[4] krav på incidenthantering och med brittiska motsvarigheten till Svensk e-legitimation.

Personuppgifter
Samtliga avtal tar tydligt upp ansvarsförhållanden och ansvarsfördelning vad gäller personuppgifter och samtliga aktörer är bundna av lagstiftningen i och med personuppgiftslagen. Regelverket täcker väl in personuppgiftsfrågor.

Ledningssystem för informationssäkerhet
Tillämpning av standarder för ledningssystem för informationssäkerhet, SS-ISO/IEC 27001 och SS-ISO/IEC 27002 krävs för de centrala federationstjänsterna, kravställning mot utfärdare och för underskriftstjänsten innehåller krav på tillämpning av SS-ISO/IEC 27001. MSB efterlyser tydligare referenser till standarder eller dokumenterad branschpraxis även för andra aktörer, såsom eID-leverantörer och tillhandahållare av e-tjänster. Kravställningen riktad mot eID-leverantörer uttrycker att dessa ska utföra sina uppgifter på ett fackmannamässigt sätt med god branschpraxis. För de statliga myndigheter som tillhandahåller e-tjänster och för federationsoperatören gäller dock MSB:s föreskrifter om statliga myndigheters informationssäkerhet (2009:10) vilka i sin tur ställer krav på tillämpning av SS-ISO/IEC 27001 och 27002. Kraven finns därför på dessa standarder för dessa aktörer.

Sammantaget är kravställningen på ledningssystem genomförd men det finns utrymme för förbättring genom att precisera sådant som i standarden ISO 27002 är rekommendationer i form av bör-krav.

Ledningssystemen innehåller krav på riskhantering. MSB efterlyser att det ska finnas krav på process för riskhantering för alla aktörer, vilket ingår i ISO 27001.

Kontroll av efterlevnad av regelverket
E-legitimationsnämnden kan, om det finns sakliga skäl för misstanke, låta en oberoende tredje part genomföra kontroll hos eID-leverantör för att undersöka om denne följer regelverket och anslutningsavtalet. 14 dagars varsel ska ges före kontrollen.

Det finns inte krav på extern revision eller certifiering av ledningssystemet för informationssäkerhet. Krav finns i tillitsramverket på internrevision av oberoende intern kontrollfunktion, minst var tredje år. MSB påpekar att begreppet oberoende intern revision behöver förtydligas.

[4] Federal Information Processing Standard, en serie standarder inom IT-området, fastställda av amerikanska regeringen för användning i USA:s myndigheter

Eva Ekenberg
010-574 87 25

Säkerhetsskyddet av metadatatjänster finns reglerat i säkerhetsskyddsavtal och ger E-legitimationsnämnden rätt att kontrollera att de avtalade säkerhetsskyddsbestämmelserna följs. Myndigheten kan då biträdas av Säkerhetspolisen.

Incidenthantering
Incidenthantering regleras på ett flertal ställen i regelverket. Kravställning av rapporteringsrutiner beskriver när en incidentrapport ska skapas och vad den ska innehålla.

Sanktioner
Sanktionsmöjligheter finns i form av vite om en eID-leverantör brister i tillgänglighet. Samtliga anslutningsavtal reglerar förtida upphörande, till exempel om aktören begår avtalsbrott, brister i förpliktelser enligt tillitsramverket eller hamnar på obestånd.

Jämförelse med andra kravställningar

eIDAS, EU-förordning som antogs i juli 2014. eIDAS har många gemensamma grundtankar med Svensk e-legitimation, till exempel användandet av tillitsnivåer enligt standarden ISO 29115. Inom flertalet områden harmoniserar eIDAS och regelverket för Svensk e-legitimation väl. Generellt är eIDAS-förordningens krav runt strukturerat säkerhetsarbete i linje med de krav som ställts i regelverket för Svensk e-legitimation.

FIPS om incidenthantering
FIPS, de amerikanska regelverken för IT innehåller krav på incidenthantering vilka i hög grad överensstämmer med kravställningen i regelverket, eftersom många krav återfinns i ISO 27001. Några skillnader finns, bland annat ställer ISO 27001 inte krav på att det ska finnas IT-stöd för incidenthantering.

Tillitsnivåer
Electronic Authentication Guideline från FIPS och standarden ISO 29115 beskriver hur tillitsnivåer definieras och FIPS-dokumentet överensstämmer på en övergripande nivå väl med regelverket som också är baserat på ISO standarden 29115. FIPS-dokumentet är mer detaljerat, skriver MSB.

Det är dock ett medvetet val att Svensk e-legitimations regelverk är mindre detaljerat eftersom regelverket har ambitionen att vara teknikneutralt och tillåta olika typer av lösningar.

4.5 Sammanfattande analys från ett säkerhetsperspektiv

Att upprätthålla IT-säkerhet och informationssäkerhet är alltid att sikta på ett rörligt mål och frågorna måste bevakas kontinuerligt av alla inblandade. Viktigt är att fortsatt använda och utveckla processerna, ha kontroll och använda ledningssystemet för informationssäkerhet.

Eva Ekenberg
010-574 87 25

Som all resurshantering är säkerhetsnivåer och säkerhetskrav en avvägning mellan risker och hot, rimlig resursåtgång och systemets användbarhet. Denna avvägning måste ständigt vara närvarande och prövas. Att åtgärda tekniska sårbarheter är viktigt men också att se till att procedurer kring tekniken fungerar annars kan den tekniska uppbyggda robustheten ändå sättas ur spel. Det är därför viktigt med beredskap och omvärldsbevakning med holistisk syn och rutiner för att hantera upptäckta hot, incidenter etc.

De myndigheter som uttalat sig om sina behov, se avsnitt 3.3, har alla uppfattat säkerheten i infrastrukturen som tillräcklig för myndigheternas behov.

Analysen av regelverket och regelverkets överensstämmelse med standarder och dokumenterade branschpraxis visar på att det finns en god överensstämmelse.

Grunden för säkerhetsarbetet är den ständiga förbättringen, strukturerat arbete med tydliga roller, ansvar och processer. Regelverket har definierat detta och det utgör grunden för säkerheten. Allt eftersom federationen etableras och blir operationell kommer diskussioner om förbättringar att kunna föras.

God omvärldsbevakning måste ständigt pågå och de resurser som finns tillgängliga i staten och inom federationen behöver hjälpas åt och bidra till detta. Det är också väsentligt att hålla igång fora för dialog med intressenter i form av workshops och seminarier.

5 Överväganden som behöver göras ur säkerhetssynpunkt

5.1 Förbättrings- och åtgärdsförslag

En omvärldsbevakning av utvecklingen på säkerhetsområdet är ett kontinuerligt arbete för aktörerna i infrastrukturen Svensk e-legitimation. Några områden som för närvarande är aktuella att diskutera inom federationen har föreslagits. I det förvaltningsforum som kommer att etableras, se avsnitt 6, kan nedanstående områden diskuteras för att förbättra infrastrukturen.

5.1.1 Använd tillgänglig expertis

Använd tillgänglig expertis inom staten och inom federationen för att säkra hög kompetens i omvärldsbevakning i syfte att upptäcka och värdera hot, risker och åtgärder i förhållande till myndigheternas behov.

5.1.2 Implementera SAML-protokollet på bästa sätt

Utforma information till aktörerna i federationen om hur SAML-protokollet bäst ska implementeras så att inte redan kända sårbarheter byggs in av misstag.

Eva Ekenberg
010-574 87 25

SAML-standarden är omfattande så att även om den innehåller krav på implementationen så kan viktiga krav förbises av den som inte är tillräckligt insatt. Det är viktigt att sådana krav lyfts fram på ett enkelt sätt genom information eller i regelverket.

5.1.3 Förslag att överväga när det gäller kryptoalgoritmer

Ett förslag till förbättring av regelverket är att bryta ut avsnittet om kryptoalgoritmer till ett eget dokument samt att införa en rutin för ständig bevakning och hantering av svagheter i kryptotekniken. I detta arbete utgör expertmyndigheters kunskap ett viktigt bidrag där dessa kan bistå i den ständiga bevakning som är en del av regelverkets processer.

5.1.4 Överbelastningsattacker

Den infrastruktur som bildar Svensk e-legitimation kan drabbas av överbelastningsattacker. Varje aktör som är exponerad mot Internet måste använda tillgängliga metoder för att skydda sig mot överbelastningsattacker, såsom DoS och DDoS. Detta bör studeras närmare i samverkan med federationens parter för att minimera risken för dessa attacker.

5.1.5 Överföring av information till e-tjänster, så kallad riskinformation

Riskinformation kallas extra information som lämnas till e-tjänster tillsammans med identitetsintyg och som ger uppgifter som kan användas att bättre upptäcka riskbeteenden och attacker och därmed öka säkerheten.

Sådan information är specificerad i regelverket och det finns möjligheter för e-tjänsterna att begära detta. Dock behöver behovet och möjligheterna utredas vidare inom de myndigheter som tillhandahåller e-tjänster. Till exempel kan det hända att informationen innehåller personuppgifter, konsekvenserna av detta måste därför utredas vidare.

6 Samarbete och samverkan för säker Svensk e-legitimation

Samarbete och samverkan är nödvändigt för att infrastrukturen Svensk e-legitimation ska fungera. Ett gott samarbete mellan aktörer och intressenter är en viktig del av kvalitetssäkringen när det gäller den kontinuerliga hanteringen av säkerhetsfrågorna i infrastrukturen Svensk e-legitimation.

För närvarande finns en referensgrupp med tänkbara deltagare i identitetsfederationen och andra intressenter. När federationen är färdigetablerad planeras samverkan ske inom ett förvaltningsforum för Svensk e-legitimation. Förslag finns till hur forumet ska organiseras. För de avtalsbundna aktörerna är samverkan inom identitetsfederationen reglerad i anslutningsavtalen.

Eva Ekenberg
010-574 87 25

Förvaltningsforum kommer inte ha någon formell beslutsrätt, det är ett forum för samverkan, men det troliga är att resultat av samverkan kommer att bli starkt styrande för den fortsatta utformningen av federationen.

Exakt uppbyggnad av Förvaltningsforum är inte beslutad eller reglerad i regelverket utan måste bli en fråga för de aktörer som börjar ansluta sig till federationen. Ett angreppssätt kan vara att beredning av frågorna sker i arbetsgrupper, där deltagandet är öppet såväl för deltagare i federationen som för andra intressenter, deltagandet styrs av aktörernas intresse och kompetens. I arbetsgrupper behandlas driftsfrågor, säkerhetsfrågor, användbarhets- och kommunikationsfrågor, teknikfrågor och juridiska frågor.

Om det ska finnas någon övergripande gruppering inom Förvaltningsforum som konkluderar förslag från arbetsgrupperna bör diskuteras med parterna i federationen.

Sunet har påpekat att E-legitimationsnämnden behöver bli bättre på omvärldsbevakning i internationella sammanhang där standardisering och dialog kring digital identitet sker och erbjuder sig att bidra i detta arbete.

7 Ytterligare åtgärder och framtida utvecklingsmöjligheter för att trygga en säker Svensk e-legitimation

När federationen är i drift, det vill säga såväl utfärdare som eID-tjänster och tillhandahållare av e-tjänster har anslutit sig, är det enligt MSB:s rekommendation lämpligt att genomföra en genomgång av hela systemet ur informations-säkerhetsperspektiv. En sådan genomgång bör även göras vid större förändringar.

Andra åtgärder är att E-legitimationsnämnden satsar på kommunikation, till exempel genom att målgruppsanpassa informationen på webbplatserna för Svensk e-legitimation. Det är också viktigt att fortsätta att uppdatera och precisera regelverket, att utforma och sprida vägledningar om hur användardialoger och e-tjänster bör utformas och ge råd och information om bästa sätt att implementera SAML-protokoll för att undvika kända hot.

De myndigheter som tillhandahåller e-tjänster bör göra en behovsanalys med riskanalys av e-tjänsterna för att kunna välja rätt tillitsnivå för e-legitimeringar.

I kommande förvaltningsforum byggs rutiner upp för att aktörerna gemensamt ska kunna identifiera och riskbedöma nya hot som uppkommer.

Eva Ekenberg
010-574 87 25

8 Uppdraget och dess genomförande

8.1 Dialog med MSB

MSB har genomfört en analys av informationssäkerheten i Svensk e-legitimation och inhämtat underlag från Försvarets radioanstalt, Försvarsmakten (MUST) och Försvarets forskningsinstitut.

8.2 Synpunkter från myndigheter som använder e-legitimationer i e-tjänster

Skatteverket, Bolagsverket, Arbetsförmedlingen och Sveriges kommuner och landsting har inkommit med synpunkter, se bilaga.

8.3 Synpunkter från myndigheter med expertroller

Datainspektionen och Vetenskapsrådet/SUNET har lämnat synpunkter och förslag. De skriftliga synpunkter som kommit in redovisas i Bilaga, avsnitt 9.

Eva Ekenberg
010-574 87 25

9 Bilaga Inkomna synpunkter

Myndigheter har på förfrågan från E-legitimationsnämnden uttryckt sina behov och sina synpunkter på säkerhet i Svensk e-legitimation, svar på detta redovisas nedan.

9.1.1 Sveriges kommuner och landsting

SKL har inte identifierat några sårbarheter för Svensk e-legitimation utifrån tillgänglig dokumentation. När det gäller säkerhet och incidentrapportering finns detta reglerat men behöver trimmas in för att fungera i praktiken. Gäller det generellt så finns ett stort informationsbehov till kommunal sektor. Hur ska nuvarande system växlas till det nya i kommunala e-tjänster och vad behöver respektive budgetera för (autentiseringar, underskrifter).

På frågan: ”Är gällande regelverk för Svensk e-legitimation tillräckligt omfattande och tillräckligt tydligt som kravställning när det gäller frågor kopplat till konceptets säkerhet?” svarar SKL:

”Bedömningen är att kraven finns beskrivna. Kraven kan realiseras på olika sätt vilket möjligen kan uppfattas som otydligt. eIDAS förordningen 910/2014 har i vissa fall en mer långtgående kravställning till exempel när det gäller skadestånd mm. En revision av nuvarande regelverk behöver troligen initieras ganska omgående för att kunna vara i harmoni med eIDAS.” I övrigt har SKL synpunkterna att

- Tillgänglighetskravet är lågt satt för att fylla kraven från vården, enligt vårdföreträdares bedömning
- En fråga är hur gemensamma e-tjänster där både myndigheter och privata agerar i samma tjänst ska hanteras

För privatpersoner så täcks behovet av e-legitimationer i digitala tjänster idag för kommunal sektor. Utvecklingen går dock fort och det gör att behovet att kunna revidera och tillföra nya tekniker, utan att regelverk och tillitsramverk påverkas.

Kommunal sektors välfärdstjänster sker till stor del av privata utförare vilket ger utmaningar då konturerna av ett privat federationsalternativ inte framträder. Vidare ger uppdelningen utmaningar för gemensamma tjänster där offentliga myndigheter och privata utförare samsas.

Den stora utmaningen är hantering av e-legitimation i tjänsten. Idag florerar flera lösningar och i en del fall finns ingen annan lösning än att nyttja den privata e-legitimationen vid samröre med myndigheter.

Eva Ekenberg
010-574 87 25

9.1.2 Arbetsförmedlingen

Arbetsförmedlingen delar E-legitimationsnämndens uppfattning att användarperspektivet är en grundförutsättning för säkerhetsarbetet. Vi ser det positivt att E-legitimationsnämnden arbetar riskorienterat när det gäller hur olika säkerhetsfrågor ska hanteras. Det är dock i sak svårt att bedöma vilka kontroller och krav vi ser relevanta för att risknivån skall vara acceptabel utan att ha tillgång till de riskanalyser som genomförts.

Risknivån är direkt avhängig de tjänster som i en framtid kommer att tillgängliggöras inom ramen för Svensk e-legitimation. Eftersom det inte finns någon beskrivning över dessa tänkbara tjänster och vilka leverantörer som kommer att tillhandahålla dessa tjänster så är det mycket svårt att uttala sig om eventuella sårbarheter och om dessa hanterats nöjaktigt.

Naturligtvis är användbarheten en framgångsfaktor för spridningen av användandet av e-tjänster. Eventuella motsättningar mellan användbarhet och säkerhet måste analyseras avseende den skada som kan uppstå för någon part om säkerheten skulle komprometteras. Åter igen så är det svårt att från ett generellt resonemang kompromissa med säkerheten om det inte finns en koppling till maximal risknivå för tjänsterna inbyggd i regelverket.

Arbetsförmedlingen delar även E-legitimationsnämndens åsikt att ett väl fungerande samarbete mellan tillhandahållare av e-tjänster och e-legitimationsnämnden är en förutsättning för en väl fungerande infrastruktur för e-tjänster. Arbetsförmedlingen skulle även gärna se att någon part har ett konkret ansvar för att möta och aktivera marknaden för leverantörer av eID.

Arbetsförmedlingens uppfattning är att det tekniska regelverket är tillräckligt konkretiserat. Arbetsförmedlingen ser dock vissa oklarheter avseende de administrativa reglerna;

- Det är till exempel inte klart om privata aktörer kan leverera e-tjänster som en egen affär eller om detta alltid ska ske som ett uppdrag från en myndighet.
- Regelverket tillåter olika tillitsnivåer på identifieringen. Arbetsförmedlingen ser det heller inte klarlagt hur och under vilka omständigheter dessa olika nivåer ska användas.
- Arbetsförmedlingen upplever kontrollfunktionen att utfärdare och tjänsteleverantörer verkligen tillämpar regelverket som oklar. Ett bättre sätt borde vara att tillämpa ett ackrediteringsförfarande med återkommande tillsyn från ackrediteringsorganet.
- Arbetsförmedlingen anser även att regelverket är skrivet på ett mycket svårbegripligt språk och borde kunna formuleras på ett mer lättillgängligt sätt.
- Arbetsförmedlingen saknar en vision för den framtida utvecklingen av e-legitimationer och deras användningsområden. Frågor som vi funderar över är bland annat hur ser framtiden ut för mobila lösningar för identifiering och

Eva Ekenberg
010-574 87 25

kommer dessa att kunna användas i andra tjänster än rena e-tjänster som till exempel telefonkontakter, hur kommer privata aktörer att delta i tjänsteutvecklingen?

9.1.3 Skatteverket

1. Stämmer utgångspunkterna för säkerhetsarbetet inom ramen för Svensk e-legitimation enligt ovan med er uppfattning?

Den lösning som nu etableras med en offentlig federation för Svensk E-legitimation anser Skatteverket är bra. En förändring mot dagens lösning är att parterna i federationen troligen blir fler och alla ska följa samma regelverk. För att regelverket inte ska stagnera och att alla parter ska ha en rimlig framförhållning till förändringar krävs tydlig planering och kommunikation. Här saknar Skatteverket en tydlig och kommunicerad ändringshanteringsplan, rapportering över identifierade brister, planerad livscykelhantering av regelverket. Skatteverket saknar även inspel ifrån marknaden kring befintliga e-legitimationer. Vi har förhoppningar att detta arbete förbättras när arbetet med förvaltningsforum etableras, som vi anser bör ske omgående.

2. Finns sårbarheter som ni uppfattar inte omhändertagits tillfredställande inom ramen för Svensk e-legitimation?

Det har påtalats att det är en brist att det inte finns stöd i regelverket att tydligt påvisa vad en användare skriver under. E-legitimationsnämnden har ställt frågan vidare till oss myndigheter om vi har det kravet.

Skatteverket har kravet att kunna skicka med en beskrivande text vid underskrift: till exempel:

"Du skriver nu under din inkomstdeklaration för inkomståret 2013"

"Du skriver nu under intyg för att kalle karlsson 7411dd-xxxx blir ombud för dig"

Påtalad brist att inte Mobila appar stöds är delvis felaktig, det pågår ett arbete kring tekniken nativa appar för att erbjuda det stödet. Skatteverket i sig påverkas inte direkt i dagsläget av denna brist.

3. Vid kompromisser mellan användbarhetskrav och krav på säkerhet, vad ska väga tyngst?

Säkerhetskraven är viktigast för att upprätthålla en beslutad säkerhetsnivå, användarbarhetskraven är viktiga och kan med rätt hjälpmedel göras begripliga.

Skatteverket fäster stor vikt vid användbar säkerhet, där användbarheten testas av olika användargrupper.

Eva Ekenberg
010-574 87 25

Går inte tjänsterna att använda eller upplevs som alltför svåra/krångliga för gemene man väljs ofta manuella pappersalternativ.

4. Konceptet är beroende av ett väl fungerande samarbete och god dialog mellan E-legitimationsnämnden och Tillhandahållare av e-tjänst (myndigheter). Har ni förslag på agerande för att detta ska vara tillfredställande?

E-legitimationsnämnden bör snarast etablera förvaltningsforum enligt tidigare förslag för att fånga upp:

- Förändrade krav på säkerhetsrutiner
- Marknadens parter för vidare- och nyutveckling
- Tydliga supportvägar
- Löpande information om federationens utveckling.
- Förändringar i användandet som kräver anpassningar hos parters produkter eller förändring av regelverk

Planerad livscykelhantering av regelverket och dess tjänster

5. Är gällande regelverk för Svensk e-legitimation tillräckligt omfattande och tillräckligt tydligt som kravställning när det gäller frågor kopplat till konceptets säkerhet?

Ändringshantering och livscykelstatus på regelverk bör förtydligas för att erbjuda en ordnad in- och utfasning av godkända regler. I detta arbete bör en bredare skara ifrån offentlig sektor ingå, (Myndigheter och SKL), privata sidan med federationsoperatör och utfärdare av E-legitimation.

6. Ytterligare synpunkter utöver ovanstående frågeställningar?

Kommunikationsförmågan hos e-legitimationsnämnden behöver lyftas och bli mer konkret mot olika målgrupper. Idag är materialet omfattande och inte anpassat för olika nyttjare, både tillhandahållare av e-tjänst, utfärdare av E-legitimation samt medborgare. Det finns även en otydlighet vilken information som publiceras på respektive sida sveleg.se och elegnamnden.se. Det är viktigt att information läggs ut löpande, kanske i form av veckobrev.

7. För att säkerställa att vi får med behoven på ett korrekt sätt i redovisningen av regeringsuppdraget så ser vi gärna om ni har möjlighet att inkomma med svar på frågan vilket behov ni har av e-legitimationer.

Skatteverkets inriktning att bredda e-vägen för att underlätta för medborgare och företagare att använda våra e-tjänster har ett starkt beroende till en väl fungerande säkerhetslösning som är allmänt accepterad i samhället. Genom att på ett säkert och användarvänligt sätt erbjuda elektronisk identifiering och underskrift genom e-legitimationer bidrar det till att bibehålla och höja viljan att göra rätt för sig, det blir även en effektivare hantering i skatteverkets verksamhet.

Eva Ekenberg
010-574 87 25

9.1.4 Bolagsverket

- Stämmer utgångspunkterna för säkerhetsarbetet inom ramen för Svensk e-legitimation med er uppfattning?

  Svar: Ja, Bolagverkets uppfattning är att detta stämmer.

- Finns sårbarheter som ni uppfattar inte omhändertagits tillfredställande inom ramen för Svensk e-legitimation?

  Svar: Bolagsverket anser att sårbarhetsaspekterna har omhändertagits tillfredställande inom ramen för Svensk e-legitimation.

- Vid kompromisser mellan användbarhetskrav och krav på säkerhet, vad ska väga tyngst?

  Svar: Ingen går att bortse ifrån, båda aspekterna är viktiga för att få användares förtroende att använda Svensk e-legitimation. Ska man ändå göra en viktning mellan dessa två så väger säkerhetsaspekten tyngre. Dock kan man inte förringa behovet av höga användbarhetskrav för att skapa förtroende för och generera hög användning av Svensk e-legitimation.

- Konceptet är beroende av ett väl fungerande samarbete och god dialog mellan E-legitimationsnämnden och Tillhandahållare av e-tjänst (myndigheter). Har ni förslag på agerande för att detta ska vara tillfredställande?

  Svar: Det är fortsatt viktigt med en öppen och tydlig dialog och information vad som händer inom arbetet med Svensk e-legitimation, bland annat för att kunna planera och agera internt inom den egna organisationen – och det är lika viktigt för alla parter som kan ingå i federationen. Därför är det Bolagsverkets uppfattning att det är viktigt att fortsätta med informationsmöten, workshops etc. som E-legitimationsnämnden gjort hittills.

Är gällande regelverk för Svensk e-legitimation tillräckligt omfattande och tillräckligt tydligt som kravställning när det gäller frågor kopplat till konceptets säkerhet?

Svar: Ja, det är Bolagsverkets uppfattning.

9.1.5 Datainspektionen

Bakgrunden till mötet är ett regeringsuppdrag (N2014/2207/ITP) åt e-legitimationsnämnden, där det bland annat ingår att inhämta Datainspektionens synpunkter.

Eva Ekenberg
010-574 87 25

Datainspektionen har inte gjort någon genomgång av regelverket kring Svensk e-legitimation, men inspektionens generella synpunkter när det gäller personuppgiftsbehandling och spontana synpunkter på Svensk e-legitimation efterfrågades. Datainspektionen yttrade sig i samband med remissen av betänkandet E-legitimationsnämnden och Svensk e-legitimation (SOU 2010:104). I huvudsak diskuterades följande under mötet.

Frågan om personuppgiftsansvar

Det är av särskild vikt att inblandade parter har klart för sig vilket personuppgiftsansvar respektive part har och vad det ansvaret innebär, det vill säga att det står klart för parterna vem som ansvarar för vad, enligt vilket regelverk och inför vem. I samband med detta diskuteras också frågan om laglighet, se 9 § första stycket a personuppgiftslagen (1998:204).

Personuppgiftsansvarig enligt personuppgiftslagen är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter, se 3 §. Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bland annat varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, dvs. ”hur” behandlingen ska gå till, t.ex. vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifterna, när uppgifter ska raderas med mera. Det är den som faktiskt – med eller utan rätt – har bestämt över behandlingen som är personuppgiftsansvarig. Vem som bestämmer över en behandling, det vill säga vem som är personuppgiftsansvarig, är alltså en fråga om fakta och något som, i sista hand, kan bli föremål för domstolsprövning.

Inbyggd integritet

Datainspektionen har tagit fram ett informationsblad om så kallad inbyggd integritet (eng. privacy by design, PBD) som finns tillgänglig på myndighetens webbplats. Informationsbladet ger stöd vid systemutveckling och harmonierar med de grundläggande dataskyddsprinciperna som de uttrycks i 9 § personuppgiftslagen. Det går i huvudsak ut på att minimera antalet personuppgifter som behandlas och minimera spridningen av dem till vad som är nödvändigt i förhållande till det aktuella ändamålet samt att skydda personuppgifterna från otillåten behandling.

Säkerhet för personuppgifter

Bestämmelserna om säkerhet vid behandling i 30, 31 §§ personuppgiftslagen är till för att skydda den registrerades personliga integritet. Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda de personuppgifter som behandlas och åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig. Ur såväl integritetsskydds- som

Eva Ekenberg
010-574 87 25

rättssäkerhetsperspektiv ställs höga krav på säkerheten i de delar som ingår i infrastrukturen kring Svensk e-legitimation. Det är därför viktigt att det, bland annat, finns en förvaltningsprocess för svensk e-legitimation som omfattar ett operativt och kontinuerligt säkerhetsarbete som innefattar bland annat rutiner för risk- och sårbarhetsanalyser, incidenthantering och kontinuitetsplanering. På frågan om säkerhet eller användbarhet, vid en kompromiss mellan dessa, ska väga tyngst konstaterar Datainspektionen att tillräcklig säkerhet är ett lagkrav som inte kan kompromissas bort.

Underskriftstjänsten

Vid användning av en underskriftstjänst är det viktigt att användaren inte vilseleds i förhållande till vad som signeras. Vilken information som visas för användaren vid underskriftstillfället, som i praktiken innebär en återautentisering av användaren, får här betydelse eftersom denna information även görs tillgänglig för utfärdaren. Det kan i sin tur påverka de bedömningar kring laglighet och säkerhet som beskrivs ovan. I botten ligger den så kallade oavvislighetsproblematiken, som diskuteras i förhållande till skillnaderna mellan direkt matematisk koppling mellan användaren och dennes digitala aktiviteter och spårbarhet genom korrekta loggar i en slags beviskedja.

Utifrån diskussionen kring underskriftstjänsten diskuterades också förhållandet mellan användare och utfärdare utifrån förlitande parters överföring av uppgifter till utfärdare. Finns det i e-legitimationsnämndens regelverk några begränsningar för vilka tjänster en utfärdare, med stöd av samtycke, får erbjuda en användare? Tydligheten i den information som behövs för att ett giltigt samtycke ska kunna lämnas diskuteras också.

9.1.6 SUNET

- Stämmer utgångspunkterna för säkerhetsarbetet inom ramen för Svensk e-legitimation enligt ovan med er uppfattning?

Ja.

- Finns sårbarheter som ni uppfattar inte omhändertagits tillfredställande inom ramen för Svensk e-legitimation?

Ja. SUNET menar att Mobilt BankID inte har analyserats ur ett säkerhetsperspektiv av en oberoende säkerhetsexpert. Eftersom ett antal av SUNET kunder använder Mobilt BankID undersöker SUNET för närvarande möjligheten att genomföra en oberoende säkerhetsanalys av Mobilt BankID.

- Vid kompromisser mellan användbarhetskrav och krav på säkerhet, vad ska väga tyngst?

SUNET menar att denna fråga (om den dyker upp) är felställd. Det finns ingen egentlig konflikt mellan användbarhet och säkerhet: dålig användbarhet leder till dålig säkerhet.

Eva Ekenberg
010-574 87 25

Om denna fråga trots allt skulle dyka upp menar SUNET att e-legnämnden bör bjuda in till konsultation kring frågan med syfte att genomlysa problemet så att rätt frågeställning diskuteras.

- Konceptet är beroende av ett väl fungerande samarbete och god dialog mellan E-legitimationsnämnden och Tillhandahållare av e-tjänst (myndigheter). Har ni förslag på agerande för att detta ska vara tillfredställande?

SUNET menar att e-legnämnden bör överväga återuppta en kontinuerlig dialog med marknadens olika aktörer i form av seminarier och workshops eventuellt tillsammans med SUNET.

- Är gällande regelverk för Svensk e-legitimation tillräckligt omfattande och tillräckligt tydligt som kravställning när det gäller frågor kopplat till konceptets säkerhet?

SUNET menar att tillitsramverket inte ställer tillräckliga krav på oberoende revision av identitets-utfärdare. Vi menar att sammansättningen och organisationen av granskningsfunktionen inte ger tillräckliga garantier för att granskningar sker på ett oberoende sätt. SUNET har sedan länge ansett att det är och var ett misstag att e-legnämnden skrev ett eget förtroenderamverk istället för att använda och hjälpa till att vidareutveckla Kantaras ramverk vilket SUNET rekommenderade.

- Ytterligare synpunkter utöver ovanstående frågeställningar?

SUNET menar att e-legnämnden behöver bli mycket bättre på omvärlds-bevakning, inte minst i de internationella sammanhang där standardisering och dialog kring digital identitet sker. SUNET har lång erfarenhet av detta och erbjuder oss (som alltid) att hjälpa till.