Dokumentklass: Öppen
Datum: 2015-09-14
Version: 1.0

Robusthetshöjande åtgärder

Fördjupad analys:

eID

- En studie om användningen av e-legitimation för samhällsviktiga utbetalningar inom SOES-myndigheterna

Representanter från kommuner

SOES ska verka för att enskilda individer, företag och det allmänna ska ha tillgång till och förtroende för att:

- samhällets betalningar* fungerar och
- systemen för att betala varor och tjänster fungerar

Syftet är att förebygga allvarliga störningar för att minska konsekvenser av händelser som kan få allvarliga samhällspåverkande effekter.

Detta sker genom att ur ett samhällsperspektiv analysera risk och sårbarhet för kritiska resurser samt beroenden, dokumentera dessa, ta fram förslag för åtgärder, och tillställa ansvariga aktörer.

* *Med samhällets betalningar menas hela kedjan från generering av underlag för utbetalning till att mottagaren kan använda medlen. I målet ingår delar som de olika aktörerna inte har ett direkt ansvar för, men där avbrott påverkar mottagaren menligt. Exempel på detta är aktörer inom finansiella sektorn, för dessa gäller att SOES analyserar och informerar om risker.*

Sammanfattning

Utgångspunkten för studien av myndigheternas användning av e-legitimationer har varit fördjupning av risker för externa angrepp, en av de risker som identifierades inom ramen för SOES rapport ”Riskanalys för myndigheterna inom SOES” från 2014.

Studien har haft till uppgift att skapa förutsättningar för de individer som är centrala inom samhällsviktiga utbetalningsprocesser att förstå och förhålla sig till e-legitimation på ett effektivt sätt i risk- och kontinuitetshanteringsarbetet. Målsättningen har i sin tur bestått i på ett kortfattat och lättillgängligt sätt beskriva vad e-legitimation är; hur de används av myndigheter inom samhällsviktiga utbetalningsprocesser; samt ge exempel på såväl vidtagna som potentiella robusthetshöjande åtgärder för säkrare eID-tjänster.

Studien har utgått från, och även visat, att myndigheter använder sig av e-legitimation som kritisk resurs vid samhällsviktiga utbetalningsprocesser. Inom myndigheterna används e-legitimationer såväl inom handläggningsfunktionen som ekonomifunktionen för att genomföra sina åtaganden. Säkerheten i användningen av e-legitimationer beror i sin tur dels på den tekniska lösningen och dels på de rutiner som utarbetats för användningen av e-legitimationer. Av slutsatserna framgår att det identifierats ett behov av ett tydligt utpekat tillsynsansvar för e-legitimationer samt ett behov av samverkan mellan SOES-myndigheterna genom exempelvis erfarenhetsutbyte och gemensamma övningar.

Innehåll

1 Inledning

Samverkansområde Ekonomisk säkerhet (SOES) arbetar för att enskilda individer, företag och det allmänna ska ha tillgång till och förtroende för samhällets betalningar samt att systemen för att betala varor och tjänster fungerar. Verksamheten inom SOES har därmed till uppgift att förebygga allvarliga störningar i betalningssystemet och att minska konsekvenser av händelser som kan få allvarliga samhällspåverkande effekter.

Arbetet ”Samhällskonsekvensanalys för myndigheterna inom SOES” och ”Robusthetshöjande åtgärder” har varit en del i AG Kritiska Resursers, sedermera AG Analys, arbete för säkrare samhällsutbetalningar. Inom detta arbete har samhällsviktiga kartlagts och beroendeanalyser genomförts. Under 2014 utvecklade SOES Arbetsgrupp Riskanalyser även rapporten ”Riskanalys för myndigheterna inom SOES”, där relevanta risker identifierades (med utgångspunkt i SOES syfte och mål) och konsekvenser beskrevs för utvalda risker. Under 2015 genomför SOES AG Analys en fördjupning av ett antal utvalda risker, varav denna rapport utgår från risken för externa angrepp. Fördjupningen utgörs av en analys av SOES-myndigheternas användning av eID, även kallat e-legitimation, för bemyndigande av utbetalningar samt för åtkomst till känslig information.

1.1 Bakgrund

Rapport ”Riskanalys för myndigheterna inom SOES-myndigheterna” var att identifierade ett antal relevanta risker (med utgångspunkt i SOES syfte och mål), samt beskrev konsekvenser för utvalda risker. Syftet med rapporten var även att utveckla förslag till fortsatt arbete. En av de risker som bedömdes vara prioriterad inom ramen för SOES fortsatta arbete utgjordes av risken för externa IT-angrepp. Bland annat nämndes attacker som leder till att information i myndigheternas IT-system förloras eller korrumperas, alternativt att felaktiga utbetalningar görs av extern angripare. Samtidigt konstaterades ett behov av att konkretisera och exemplifiera vad externa angrepp skulle kunna innefatta, för att därigenom ge en fördjupad riskbild. I samband med SOES kartläggning av samhällsviktiga processer har ett beroende till såväl fysiska som elektroniska identitetshandlingar (eID) kunnat konstateras. SOES Arbetsgrupp Analys (AG Analys) har inför 2015 års arbete valt att fördjupa risken för externa angrepp mot denna bakgrund, genom att analysera elektroniska identitetshandlingar utifrån ett robusthetshöjande perspektiv.

E-legitimation används för inloggning i olika system och för bemyndigande av samhällsviktiga utbetalningar. Externa angrepp i form av ID-kapning ger de negativa konsekvenser som beskrivits i tidigare riskanalys, dvs. uteblivna, försenade eller felaktiga utbetalningar, vilket i förlängningen även kan minska förtroendet för SOES-myndigheterna.

1.2 Mål och syfte

Syftet med denna studie är att skapa förutsättningar för de individer som är centrala inom samhällsviktiga utbetalningsprocesser att förstå och förhålla sig till eID på ett effektivt sätt i risk- och kontinuitetshanteringsarbetet.

Målet med denna fördjupning är därför att på ett kortfattat och lättillgängligt sätt beskriva vad e-legitimation är; hur de används av myndigheter inom samhällsviktiga utbetalningsprocesser; samt ge exempel på såväl vidtagna som potentiella robusthetshöjande åtgärder för säkrare eID-tjänster.

Avgränsning
Hur privatpersoner använder sig av e-legitimation i dialog med myndigheter inkluderas inte i studien.

1.3 Metod i två steg

Arbetet har gjorts i två steg. Det första steget bestod i inventering och inläsning av material som en redogörelse för vad eID är och hur dessa används av myndigheter i samhällsviktiga utbetalningsprocesser. Informationskällor bestod av tidigare genomfört arbete inom ramen för SOES arbete såväl som öppna källor. I det andra steget genomfördes intervjuer med representanter från myndigheter inom SOES som på olika sätt arbetar med eID i samhällsviktiga utbetalningsprocesser samt med representanter från andra relevanta aktörer såsom Post- och Telestyrelsen (PTS), e-legitimationsnämnden och e-delegationen.

2 Om digitala certifikat

Ett certifikat är – enkelt beskrivet - en datafil som används för en digital kontroll av en uppgiven identitet och är att likställa med användning av ett körkort eller annan identitetshandling, med internet som användningsområde. Certifikat används inte bara av enskilda individer utan också av system, exempelvis då en webbplats legitimerar sig mot en webbläsare. Certifikaten kan på så sätt utfärdas för fysiska personer såväl som för organisationer och/eller system.

2.1 Olika certifikat för olika användningsområden

Kontrollen av identitet (autentiseringen) är det grundläggande användningsområdet för ett certifikat. Därtill kan certifikat användas för digitala underskrifter som är att likställa med en fysisk signatur på ett papper. Genom användningen av certifikat kan även säker kommunikation upprättas; då information görs otillgänglig (krypteras), alternativt tillgänglig (dekrypteras) för användare eller system vilka genom certifikatet identifierats som behöriga. På samma sätt som certifikat kan användas på olika sätt finns också flera olika former av certifikat. Formen för vilket certifikat som används styrs helt enkelt av i vilket syfte certifikatet ska användas.

Vilken aktör som helst i Sverige kan utfärda ett certifikat, men det finns dock endast ett begränsat antal utfärdare i Sverige som tidigare har, via ramavtal, upphandlats rätten att utfärda certifikat som kan användas inom myndigheternas verksamheter. Dessa utgivare utgörs bland annat av: BankID, Nordea, Telia och Steria.[1] En utfärdad e-legitimation innebär att utfärdaren går i god för att en persons identitet är säkerställd och att e-legitimationen är utfärdad till rätt person.[2]

BankID utfärdas av svenska banker, där tolv av Sveriges banker gemensamt startat bolaget Finansiell ID-Teknik BID AB för utgivning av BankID.[3] Oavsett vilken bank som gett ut BankID har legitimationen samma funktion genom att göra det möjligt för företag, banker, organisationer och myndigheter att både identifiera och ingå avtal med privatpersoner på internet.[4] E-legitimation kan vidare fås från Telia, en tjänst som bland annat Skatteverket använder vid utfärdande av ID-kort.[5]

2.2 Certifikat för identifiering, signering och validering

Certifikat ska ses som synonymt med begreppen eID/e-legitimation och BankID, vilka kort sagt utgör olika produktnamn för samma form av certifikat. Funktionen är alltså ungefär densamma och används vanligen för identifiering och underskrifter vid elektronisk kommunikation. Produktnamnen påvisar i sin tur

---

[1] CGI (2015). *Om utgivare av e-legitimation*.

[2] MSB (2014). *Analys av informationssäkerheten i Svensk e-legitimation*. MSB-dnr 2014-1360.

[3] De banker som ger ut BankID är Danske Bank, Handelsbanken, ICA Banken, Ikano Bank, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Sparbanken Öresund, Swedbank och Ålandsbanken.

[4] Finansiell ID-teknik (2015). *Om bankID*.

[5] Skatteverket (2015). *Utgivare av e-legitimation*.

vilken utgivare som tagit fram certifikaten. Låt oss - för enkelhetens skull - härefter kalla dessa certifikat för identifiering och underskrifter för *e-legitimationer*.

Enligt e-legitimationsnämnden finns idag närmare 7 miljoner utfärdade e-legitimationer, vilket är en hög andel i förhållande till befolkningen internationellt sett. E-legitimationer används ca 100 miljoner gånger per år i olika offentliga e-tjänster.[6]

E-legitimationer kan utfördas till användare såväl privat som i tjänsten (e-tjänstelegitimationer). E-tjänstelegitimationer kan innehålla uppgifter om organisationstillhörighet, det finns dock inga krav på detta. Organisationer kan ha en egen intern utgivning av e-tjänstelegitimationer till de anställda, vilka endast kan användas inom den egna organisationen för åtkomst till interna system. Det finns olika sätt att göra en elektronisk identifiering för myndighetsanställda, däribland att använda tjänstekort, e-tjänstelegitimation och BankID.[7] Det finns även vissa interna e-tjänstelegitimationer som används gemensamt över en viss bransch, som exempelvis så kallade SITHS-certifikat inom sjukvården.

Med hjälp av e-legitimation kan en individ logga in, ta del av information samt skriva under avtal och transaktioner vid myndigheters, bankers och företags webbplatser.[8] Användaren identifierar sig genom att visa sin e-legitimation och ange sin säkerhetskod. En kontroll av giltigheten för e-legitimationen görs automatiskt i den e-legitimationsintegration som krävs i tjänsten och e-legitimationen verifieras även mot en aktuell spärrlista. Användaren skriver under eller godkänner dokument och handlingar på samma sätt som vid inloggning och identifiering. Om e-legitimationen är giltig och korrekt säkerhetskod angivits är det säkerställt att det elektroniskt underskrivna avtalet är ingånget med rätt person.[9]

2.3 Säkerhet vid användning av certifikat

Säkerheten i certifikat beror på hur den utfärdande aktören valt att bygga den tekniska lösningen och hur processen för användningen av det enskilda certifikatet är utformad.

Mjuka och hårda certifikat

Utfärdande aktörer kan exempelvis välja att använda sig av hårda eller mjuka certifikat, vilket enkelt beskrivet redogör för hur certifikatet lagras och används. Ett mjukt certifikat utgörs av en fil som kan kopieras och användas vid obegränsat antal åtkomstpunkter medan ett hårt certifikat begränsas till en specifik och fysisk enhet, exempelvis en bankdosa eller på mobilens SIM-kort/SMART-kort. Hårt certifikat betraktades tidigare som mer säkra i och med att det ansågs svårare för en obehörig att nå informationen genom att det krävs en tillgång till den fysiska

---

[6] e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[7] Intervju Skatteverket 2015-04-24.

[8] Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

[9] Finansiell ID-teknik (2015). *Så fungerar bankID*.

enheten.[10] Denna ansats har dock kommit att revideras då flera mjuka certifikat idag ses som jämförbara med hårda certifikat utifrån ett säkerhetsperspektiv.[11]

Mjuka certifikat för banktjänster har funnits sedan 2003, där en hemlig kodnyckel laddas ner och därefter lagras på datorns hårddisk. Funktionen fungerar även om filerna flyttas mellan olika datorer. Installation av certifikat på persondator kräver även en installation av ett tillhörande säkerhetsprogram.

2005 lanserades e-legitimation för banktjänster på kort. Denna funktion bygger på att en hemlig privat kodnyckel lagras i smartkortets chip, (hårt certifikat) där det kräver fysisk access till kortet för att identifieringstjänsten ska kunna fungera. En utveckling under senare år är mobila lösningar (exempelvis mobilt BankID) som består av en e-legitimation som finns tillgänglig via en applikation i exempelvis moderna smarttelefoner och surfplattor. Den mobila lösningen är en form av mjukt certifikat för identifikation och signering där den hemliga nyckeln lagras i den mobila applikationen. Processen för identifiering/signering sker via webben på en vanlig persondator, där mobilen fungerar som separat säkerhetsdosa.[12]

Tillitsnivåer för certifikat

Valet av olika tekniska lösningar är som bekant förenat med olika säkerhetsegenskaper, där valet av säkerhetsfunktioner vanligen överlåts till de enskilda utfärdarna istället för att begränsa dem till en särskild teknik. Ett sätt för offentliga aktörer att öka säkerheten i dess upphandlade lösningar är att ställa krav på så kallade tillitsnivåer. Detta är även något som rekommenderas av e-legitimationsnämnden och är även tänkt att ingå i den nya infrastrukturen för svensk e-legitimation. Dessa nivåer är teknikoberoende och anger vilken säkerhetsnivå den valda lösningen har istället för vilka enskilda säkerhetslösningar som bör användas.[13]

Internationellt finns en rad ramverk som stipulerar krav för tillitsnivåer. Bland annat har ett ramverk tagits fram inom ramen för det så kallade Kantara-initiativet och det så kallade tillitsramverket har utvecklats inom den internationella standarden ISO/IEC 29115:2013. Det finns en rad olikheter mellan de olika ramverken samtidigt som det utifrån ett riskperspektiv finns enighet kring fyra övergripande tillitsnivåer.[14]

Tillitsnivå 1 beskrivs utifrån ”Ingen eller liten tilltro till angiven identitet”. Nivån anses lämplig i de fall där en felaktig identifiering endast förväntas leda till ”mycket begränsade negativa följder”. [15] Exempel på användningsområden är uppgiftslämnande via e-tjänst där ingen information av känslig karaktär delges. De utvecklade teknikerna kan i detta fall bestå i lösenord eller motsvarande. Tillitsnivå 2 innefattar i sin tur ”viss tilltro till angiven identitet” och anses lämplig i de fall då en felaktig identifiering leder till ”måttliga negativa konsekvenser” och där

[10] Intervju Riksgälden 2015-04-08.

[11] Intervju e-legitimationsnämnden 2015-05-22.

[12] Finansiell ID-teknik (2015). *Om bankID.*

[13] Intervju e-legitimationsnämnden 2015-05-22.

[14] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

[15] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

användning av ett starkt lösenord via internet beskrivs vara en jämförbar teknisk lösning. [16]

Vid tillitsnivå 3 finns ”hög tilltro till angiven identitet” och beskrivs lämplig när felaktig identifiering kan leda till betydande skador. Denna nivå kräver flerfaktorsidentifiering som styrker både kännedom om personlig kod samt kontroll över e-legitimationshandling. Vid denna nivå är såväl mjuka som hårda e-legitimationshandlingar samt engångslösenord en lämplig teknisk lösning. Nivån fastställer högre krav på kontroll av identitet i rättslig mening. [17]

Vid den högsta tillitsnivån, nivå 4, finns ”mycket hög tilltro till angiven identitet” och anses lämplig då felaktig identifiering kan leda till svåra konsekvenser. Denna nivå kräver identifiering via tillhandahållande av e-legitimationshandling vid fysiskt besök, på motsvarande sätt som för traditionell legitimationshandling. [18]

Nämnda tillitsnivåer tillämpas ännu inte i Sverige vid utfärdande av e-legitimationer och ännu har heller ingen granskning utifrån tillitsnivåer genomförts. Enligt en e-legitimationsnämndens bedömning är e-legitimationer i Sverige vanligen kopplade till tillitsnivå 3 vilket förutsätter tekniska lösningar för en hög tilltro till angiven identitet.[19] Värt att nämna är att principen att utfärdare äger ansvar för utformning av säkerhetslösningar förutsätter kompetenta kravställare som kan avgöra i vilken mån leverantören faktiskt uppfyller kraven.[20]

[16] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

[17] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

[18] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

[19] Intervju e-legitimationsnämnden 2015-05-22

[20] E-legitimationsnämnden (2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09.

3 Myndigheternas användning av eID

3.1 Tjänstebaserad användning av eID

Processen för framtagande av betalningsunderlag och verkställande av samhällsutbetalningar hanteras vanligen av olika delar av myndigheten, vid en handläggningsfunktion respektive en ekonomifunktion. Båda dessa funktioner använder sig av någon form av e-legitimation för att legitimera sig och sedan kunna genomföra sina åtaganden.[21]

Inloggning i interna system

Vid handläggning hos myndigheter används vanligen tjänstekort (med e-tjänstelegitimation) för identifiering och inloggning i interna system. Hos de tillfrågade myndigheterna inom ramen för denna analys ges de anställda vanligen tillgång till interna system genom användning av tjänstekortet i datorn, där vissa kort kräver tillgång till myndighetens nätverk. E-tjänstelegitimation gör det möjligt för den anställde att logga in i interna system och utföra handläggningsärenden. Behörigheter, där den anställda ges tillgång till olika system via tjänstekortet, utformas i sin tur inom den enskilda myndigheten genom tilldelning av olika behörighetsnivåer. Det finns en intern tillsyn över att det enbart är ett kort utfärdat per person och att tjänstekort avregistreras vid händelse av att ett kort förlorats.

System-till-system-modellen används för kommunikation mellan myndigheter

I kommunikationen mellan myndigheter används främst modellen system-till-system där myndigheterna identifierar sig via myndighetscertifikat (även kallat serverlegitimation). På så sätt används varken personlig e-legitimation eller e-tjänstelegitimation vid kommunikationen mellan myndigheternas system. Bakgrunden till att myndigheterna i huvudsak använder denna lösning är en förenklad administration och för en tydlig ansvarsfördelning där myndigheterna ansvarar för sin egen interna tillitsnivå och säkerhet. Det är således aldrig möjligt för en myndighet att ge sina anställda behörighet till andra myndigheters interna system.

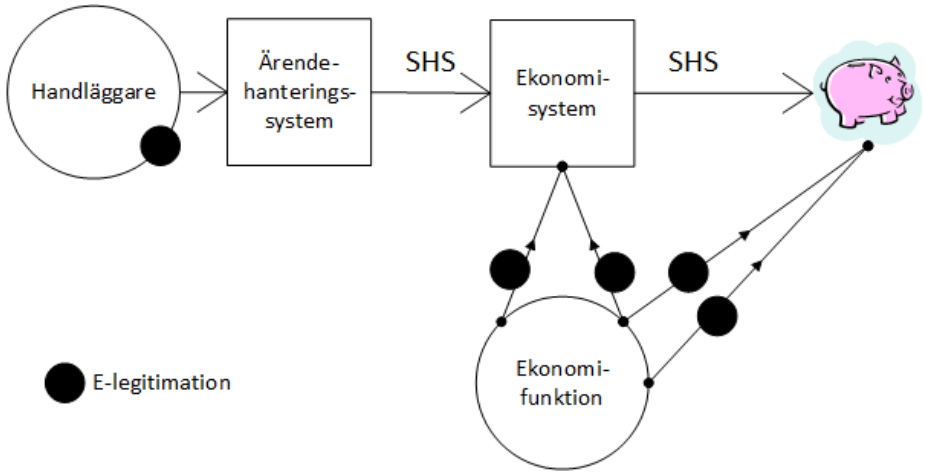
Bemyndigande av utbetalningar

E-legitimation används vid flera tillfällen i processen för myndigheternas samhällsutbetalningar. Beslut om en samhällsutbetalning sker i ett internt ärendehanteringssystem hos myndigheten. Därefter attesteras utbetalningen i ett internt ekonomisystem av minst två anställda som godkänner den genom att skriva under med sin e-tjänstelegitimation. Då utbetalningen är godkänd skapas en betalningsfil som skickas vidare till ramavtalsbankerna via en automatiserad process och inväntar där ett bemyndigande av utbetalningen som en sista signering.[22] Denna signering görs av två personer via de e-identifieringslösningar som de enskilda ramavtalsbankerna tillhandahåller. Normalt finns alltså en rutin för elektronisk signering och bemyndigande där minst två personer attesterar och bemyndigar en myndighetsutbetalning. De anställda loggar in på

[21] Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

[22] Intervju Försäkringskassan 2015-04-15; Intervju Arbetsförmedlingen 2015-04-20.

ramavtalsbankens internetbank och bemyndigar där utbetalningen genom en elektronisk signering, vilket kontrolleras mot bankens register av behöriga.[23] Hos de banker som använder BankID som inloggningslösning använder den anställda vanligen sitt privata BankID alternativt en tjänstedosa som utfärdas av bankerna. Det räcker att de anställda har ett BankID då det fungerar att logga in med samma BankID på alla ramavtalsbanker. När de anställda har bemyndigat samhällsutbetalningen hos ramavtalsbanken förs medlen vidare mot slutmottagaren. Som reservrutin är det möjligt för anställda att attestera betalningsfilen från sin arbetsdator och sen logga in på ramavtalsbanken på annan fysisk plats, exempelvis hemifrån, och då bemyndiga själva utbetalningen.



Figur 1. Användning av e-legitimation vid myndigheternas utbetalningar.

3.2 Samordning för e-legitimationer i Sverige

I takt med att digitaliseringen av offentlig förvaltning i Sverige tagit fart och att IT-utvecklingen fortsatt, har utveckling och diskussion kring olika standardramverk legat i ropet. Utvecklingen avspeglar sig även i den politiska utvecklingen där ramverk för e-legitimationer legat i fokus vid diverse statliga utredningar.[24]

I remissen ”Kompletterande bestämmelser till EU-förordningen om elektronisk identifiering”, som ska besvaras av ett flertal myndigheter, föreslås att det behövs en ny lag för att möjliggöra en säker åtkomst till gränsöverskridande digitala tjänster. Det föreslås att lagen (2000:832) om kvalificerade elektroniska signaturer ska upphävas. Detta föranleder vidare följdändringar i ett antal lagar. Lagändringarna föreslås träda i kraft den 1 juli 2016.

---

[23] Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

[24] SOU (2009:86). *Strategi för myndigheternas arbete med e-förvaltning*; Verva (2008) *Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar*; SOU (2010:104) *E-legitimationsnämnden och Svensk e-legitimation*.

Regeringen har bland annat uttryckt en ambition av sammanhållen och enhetlig infrastruktur för användningen av e-legitimationer, som förenklar för den offentliga sektorn och främjar utvecklingen av e-tjänster. Ambitionen var att samla till en federation för e-tjänster där alla e-legitimationer som uppfyller uppställda krav kan användas inom offentlig sektor. Därtill har regler för valfrihetssystem vid upphandlingsförfarande samt nya regler för upphandling stärkt behov av en översyn av den svenska modellen för e-legitimationer, då nuvarande funktion för avrop via Kammarkollegiet inte längre är möjligt.[25] Med bakgrund av regeringens ambition och det förtydligade behovet av en samordnande funktion inrättades e-legitimationsnämnden 2011, vilket har inneburit att respektive myndighet inte längre själva behöver sköta allt arbete kring e-legitimation på egen hand (upphandling, tillgång, säkerhet, utveckling etc.).

Svensk e-legitimation

E-legitimationsnämnden har ett särskilt uppdrag för samordning och stöd för elektronisk identifiering och signering i den offentliga förvaltningens e-tjänster som riktar sig till såväl myndighetens egna anställda som till medborgare. Genom inrättandet av e-legitimationsnämnden har en infrastrukturlösning för e-legitimationer inom den offentliga förvaltningen formats med uppgift att bland annat bistå vid upphandling av konkurrerande marknadslösningar på e-legitimationsområdet.[26] Infrastrukturen för e-legitimationer benämns *Svensk e-legitimation* och bygger på ett valfrihetssystem som ger de enskilda offentliga aktörerna rätt att välja leverantör av e-legitimation bland de leverantörer som e-legitimationsnämnden har godkänt. Svensk e-legitimation harmoniserar med gällande lagstiftning om valfrihetssystem (baserat på reglerna i lagen 2008:962 om just valfrihetssystem).[27]

Aktörer kan även använda sig av e-legitimationsnämnden vid avtalsskrivningen även om det aktuella avtalet i juridisk mening fattas mellan den enskilda leverantören och den offentliga aktören. Genom infrastrukturen kan de ingående myndigheterna uppdra åt e-legitimationsnämnden att administrera dess valfrihetssystem, även om de faktiska avtalen alltså formellt är mellan myndigheten och leverantören.[28]

För att nyttja de lösningar som den gemensamma infrastrukturlösningen erbjuder behöver den enskilda offentliga aktören (läs myndigheten): [29]

- Ansluta sig till svensk e-legitimation via ett fullmaktsavtal med e-legitimationsnämnden
- Anpassa de egna e-tjänsterna till beslutad lösning
- Integrera stöd för användning av upphandlade tjänster med hjälp av de stöd som e-legitimationsnämnden tillhandahåller.

---

[25] SOU (2010:104) *E-legitimationsnämnden och Svensk e-legitimation*.

[26] e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[27] SOU (2010:104) *E-legitimationsnämnden och Svensk e-legitimation*.

[28] Intervju e-legitimationsnämnden 2015-05-22.

[29] e-delegationen(2015). *Om e-legitimation*; Intervju e-delegationen 2015-04-24.

Infrastrukturen består av ett övergripande regelverk som nämnden tagit fram och som reglerar samordningen kring e-legitimation. Regelverket består i sin tur av två ramverk, tillitsramverket och det tekniska ramverket, vilka samtliga aktörer som vill använda sig av svensk e-legitimation måste förhålla sig till.[30] Ramverken reglerar bland annat SLA-nivåer i förhållande till leverantörer och tillitsnivåer och tar sin utgångspunkt i internationella standarder. Det är upp till den enskilda utfärdaren att välja vilken tillitsnivå de vill söka för (*se avsnitt 2.3 för tydligare beskrivning av tillitsnivåer*). Det är även ålagt utfärdare att visa hur de uppfyller krav för tillitsnivåerna för e-legitimationer och e-tjänster. På så sätt är det möjligt för utfärdare att fritt utforma och utveckla lösningar så länge de uppfyller de säkerhetskrav som anges i tillitsramverket. Detta gör utfärdaren exempelvis genom att beskriva hur e-legitimationen är utformad och hur en identitet säkerställs vid dess användning. Ramverken är transparanta, på så sätt att alla aktörer som har intresse av att ansluta sig kan ta del av vad regelverket föreskriver.[31]

E-legitimationsnämnden har av regeringen tilldelats ett särskilt uppdrag för förvaltning av infrastrukturen kring svensk e-legitimation. Nämnden ansvarar bland annat för det regelverk som framtagits och annonserar efter tjänster för elektronisk identifiering och godkänner leverantörer som uppfyller krav utifrån den kravspecifikation som E-legitimationsnämnden tagit fram. Avtal mellan myndigheter och leverantörer genomförs därtill genom e-legitimationsnämndens försorg. Vid misstanke om eventuella oegentligheter har nämnden rätt att genomföra stickprovskontroller vid aktören och därefter - vid behov - stänga av tjänster eller aktörer.[32] Enkelt beskrivet kan nämndens uppdrag beskrivas utifrån att de har ansvar för ett regelverk som påvisar vilka krav (*vad*) som måste uppnås men inte *hur* detta ska göras.

E-legitimationsnämnden arbetar inte isolerat, utan samordnar arbetet för svensk e-legitimation i samråd med en rad andra aktörer. Inom e-legitimationsnämnden finns för närvarande sju stycken ledamöter som utsetts av regeringen. Nämnden leder arbetet och beslutar om inriktning och utformning av svensk e-legitimation. I tillägg finns ett inrättat förvaltningsforum med ambition att samla samtliga aktörer som ansluter sig till svensk e-legitimation. Ambitionen är att samla förvaltningsforumet en gång i månaden för att bland annat diskutera vidareutveckling av infrastrukturen för svensk e-legitimation, risker, hantering av incidenter samt kapacitetsplanering.[33]

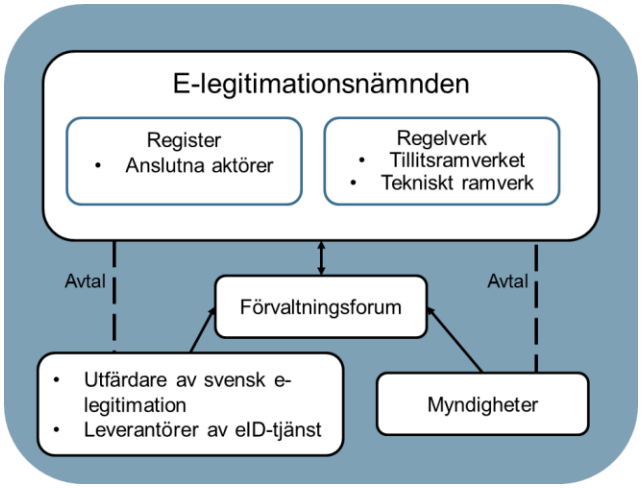
---

[30] e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[31] Intervju e-legitimationsnämnden 2015-05-22.

[32] Intervju e-legitimationsnämnden 2015-05-22.

[33] Intervju e-legitimationsnämnden 2015-05-22.



Figur 2. Översikt - Svensk e-legitimation

4 Robusthetshöjande åtgärder

4.1 Fördjupad riskbild

Det finns en rad identifierade riskområden kopplade till myndigheternas användning av e-legitimation i processer för samhällsviktiga utbetalningar. Konsekvenserna av dessa risker kan ha en påverkan på myndigheternas möjlighet att genomföra utbetalningar eller att korrekt genomföra utbetalningar.

Beskrivningen av de risker som kan ses förenliga med användandet av e-legitimation inom myndigheternas verksamheter har, vid sidan av de intervjuer som genomförts, tagit utgångspunkt i den riskanalys som e-legitimationsnämnden genomförde under 2012-2013 med stöd av Myndigheten för samhällsskydd och beredskap (MSB). Riskanalysen förtydligade bland annat behovet av ett fortsatt säkerhetsarbete gällande risker för identitetsstöld, felaktig utgivning, missbruk av annans identitet och integritetsproblematiken där risken för att personuppgifter görs tillgängliga på ett oacceptabelt eller lagstridigt sätt.[34] Beskrivningen har även utgått från den riskanalys som MSB genomfört under 2014 på uppdrag av tre enskilda myndigheter.[35]

Bristande intern kompetens/bristande resurser

En potentiell risk kopplad till myndigheternas användning av e-legitimation är brist på resurser eller bristande intern kompetens i beställarfunktionen. Brist på intern kompetens gällande tekniska lösningar kan ses utgöra en risk i kravställandet i upphandlingar av leverantörer kopplat till leverans av tjänst för elektronisk identifiering. I upphandlingen är det av vikt att myndigheter förmår ställa tillräckligt höga krav på de externa leverantörerna, exempelvis genom så kallade SLA:er (Service Level Agreements). I riskrapporten från 2014 konstaterades att det delvis råder viss brist på insyn gällande de externa IT-leverantörernas robusthet för SOES-myndigheterna och att det ofta finns en ansenlig grad av informationsasymmetri. [36] Detta kan leda till att myndigheterna har svårt att bilda sig en uppfattning om hur leverantörens tekniska lösningar har utformats, vilket kan utgöra en försvårande faktor. Brist på kompetens/resurser kan även leda till ett otillräckligt antal nyckelpersoner som hanterar bemyndigande av utbetalningar och har kunskap om hantering av e-tjänstelegitimation i denna process.

Det är viktigt att myndigheterna har en välutformad process för godkännande av leverantörer för e-legitimation. Otillräcklig resurstillgång eller kompetens kan leda

---

[34] e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[35] MSB (2014). *Analys av informationssäkerheten i Svensk e-legitimation*. MSB-dnr 2014-1360; e-legitimationsnämnden (2015). Analys och hantering av rapport från MSB – Analys av informationssäkerheten i Svensk e-legitimation. Dnr 131676133-14/9516.

[36] SOES AG Riskanalys (2014). *Riskrapport 2014*.

till bristfällig kravställning och undermålig kvalitet vid uppföljning.[37] Processen för godkännande av leverantörer kan ses stärkt genom införandet av e-legitimationsnämnden och den gemensamma process för godkännande av leverantörer som införts. Det är samtidigt viktigt att de offentliga aktörerna samverkar vid uppdatering av tillitsramverket och det tekniska ramverket för att säkerställa att dessa går i linje med de säkerhetslösningar som kan ses utgöra best practice i ett internationellt perspektiv. Detta behov understryks även av en rapport från MSB som betonar vikten av samarbete och en kontinuerlig omvärldsbevakning.[38]

Bristande tekniska lösningar från leverantör

Bristande tekniska lösningar som inte lever upp till de fastställda tillitsnivåerna utgör i sin tur ytterligare en riskfaktor. Bristande tekniska lösningar kan öka risken för externa IT-angrepp, och därmed inverka på myndigheternas användning av e-legitimation i processer för samhällsviktiga utbetalningar. Detta kan exempelvis ske genom ID-kapning av e-legitimationer som används inom myndigheter eller att information som i senare skede används vid utbetalningar förloras eller korrumperas. Utbetalningar som genomförs baserat på felaktig information kan i förlängningen resultera i att samhällsutbetalningar riktas till fel personer. Externa angrepp torde inte enbart inverka negativt på myndigheternas verksamhet och samhällsviktiga utbetalningar, men i förlängningen även negativt påverka allmänhetens förtroende för myndigheter.

Avbrott i kommunikation mellan myndighet och ramavtalsbank

Då myndigheterna genom e-legitimationer bemyndigar utbetalningar till mottagarna via ramavtalsbankerna, är det av stor betydelse att förbindelsen mellan myndighet och bank är god. Detta gäller såväl då utbetalningsuppdrag skickas som när myndigheterna via bankerna godkänner betalningar. Avbrott i kommunikationen mellan myndighet och bank är en risk som kan försvåra myndigheternas användning av elektronisk identifiering vid exempelvis bemyndigandet av betalningar. Ett flertal möjliga orsaker till risken kan noteras, exempelvis ett systemavbrott hos banken/myndigheten eller en hackerattack. Denna risk har tidigare undersökts av SOES, vilket sammanfattas i rapporten *Alternativa utbetalningsvägar* (SOES, 2010). I denna rapport konstaterades att ramavtalsbankernas reservrutiner för avbrott i nät skulle kunna kommuniceras tydligare.

Enligt vad som framkommit vid intervjuer bekräftas också att det finns etablerade manuella reservrutiner som kan träda in för att säkerställa att betalningsfiler når bankerna, vilket även finns fastställt i ramavtalen med bankerna. Detta är dock inte testat fullt ut.

---

[37] SOES AG Riskanalys (2014). *Riskrapport 2014*.

[38] MSB (2014). *Analys av informationssäkerheten i Svensk e-legitimation*. MSB-dnr 2014-1360; e-legitimationsnämnden (2015). Analys och hantering av rapport från MSB – Analys av informationssäkerheten i Svensk e-legitimation. Dnr 131676133-14/9516.

Bristande tillsyn

Ett bristande tillsynsansvar kan influera säkerheten för e-legitimation i ett livscykelperspektiv. Detta kan t.ex. handla om att bedragare med en falsk fysisk identitetshandling hämtar ut e-legitimation i annan persons namn och sedermera kan använda handlingen för bemyndigande av utbetalningar.[39] I nuläget finns inte någon enskild myndighet med enskilt ansvar för *tillsyn* av e-legitimationer utifrån ett livscykelperspektiv. Detta är en brist som uttrycks vid intervjuer såväl som via remissyttranden från enskilda myndigheter som svar på e-legitimationsnämndens riskanalys för förbättrad säkerhet inom svensk e-legitimation.[40]

För tillfället finns inte heller någon funktion för den enskilda individen att se vilka e-legitimationer som är utfärdade på honom/henne, en slags egenkontroll. Att genomföra regelbundna kontroller av att tjänster för elektronisk identifiering och signatur lyfts i intervjuerna fram som en bristvara. Bankföreningen och nationellt bedrägericentrum (Polisen) utreder för närvarande denna risk utifrån ett förslag om att utfärdaren ska behöva notifiera användaren vid utfärdande av e-legitimation i syfte att minska bedrägeririsken.[41]

4.2 Förbättrad säkerhet

Sett till den tekniska utvecklingen under de senaste åren kan det antas att de tekniska säkerhetslösningarna såväl som angreppen mot desamma kommer att utvecklas och bli alltmer sofistikerade. En förbättrad säkerhet i de elektroniska tjänsterna förutsätter på så sätt en nära samverkan mellan samtliga aktörer vid utveckling och användning av tjänsterna.

Sverige anses enligt e-legitimationsnämnden ligga långt fram i utvecklingen av e-legitimationer jämfört med internationella motsvarigheter. E-legitimationsnämnden konstaterar samtidigt att det finns behov av fortsatt arbete och vidareutveckling av kravställning på e-legitimationer för att möta behov och eliminera risker.[42] Att det finns förbättringspotential konstaterar även MSB, som på uppdrag av tre myndigheter analyserat informationssäkerheten i svensk e-legitimation som tagits fram av e-legitimationsnämnden.[43]

Den samlade infrastrukturen för svensk e-legitimation är tänkt att underlätta för myndigheterna vid utformning av egna e-tjänster eller vid upphandling av leverantörer för elektronisk identifiering mot tjänsterna. Genom det gemensamma regelverket fastställs exempelvis ett standardiserat gränssnitt som är gällande för samtliga parter och att samma säkerhetsnivåer säkerställs för samtliga e-legitimationer. I framtiden är det även tänkt att infrastrukturlösningen ska

---

[39] Dagens industri (2015). Om kapning av e-legitimation.

[40] Skatteverket remissyttrande i e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[41] Intervju e-legitimationsnämnden 2015-05-22.

[42] e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

[43] MSB (2014). *Analys av informationssäkerheten i Svensk e-legitimation*. Dnr 2014-1360; e-legitimationsnämnden (2015). Analys och hantering av rapport från MSB – Analys av informationssäkerheten i Svensk e-legitimation. Dnr 131676133-14/9516.

inkludera tilläggstjänster i form av utveckling och transport av så kallade *attribut* som inkluderar ytterligare information om en användare av e-legitimation, som exempelvis firmatecknare, vårdnadshavare eller olika säkerhetsklasser.[44]

Det bör i detta sammanhang dock nämnas att infrastrukturen för svensk e-legitimation utvecklats för samordning av e-tjänster inom offentlig förvaltning och berör på så sätt främst myndigheternas utvecklade e-tjänster gentemot medborgare samt delvis myndigheternas interna användning av e-tjänstelegitimationer. Infrastrukturen inkluderar därmed inte de e-legitimationer som kopplas till banktjänster (BankID) och på så sätt inte de risker som är förenade med användning av e-legitimationer vid bemyndigande av betalningsuppdrag etc. Denna aspekt bör beaktas vid avtalsskrivningar med de enskilda ramavtalsbankerna.

En granskning av myndigheternas utbetalningar som genomförts av Riksrevisionen visar att myndigheterna endast i undantagsfall har ett tydligt utpekat ansvar för den samlade betalningsprocessen.[45] Detta understryker i sin tur vikten av att se över befintliga rutiner och interna processer för exempelvis användningen av e-tjänstelegitimationer vid handläggningen och e-legitimationer (BankID) vid bemyndigande av utbetalningar. Särskilt då de tekniska lösningarna för bemyndigande av utbetalningar av stora summor är densamma som för mindre summor. Denna ansats styrks även av Riksrevisionen som i sin rapport för ett fördjupat resonemang kring att det finns en risk att säkerhetsnivån vid de större betalningarna inte motsvarar hotbilden.[46] En associerad risk är att den personal som utför betalningarna – på samma eller liknande sätt som de utför sina privata betalningar – inte förstår behovet av betydligt striktare rutiner och intern kontroll vid myndighetens betalningar, just för att samma tekniska lösning används. Under intervjuer uttrycktes ett behov och önskan om att det ska finnas möjlighet att som myndighetsrepresentant få e-tjänstelegitimation för bemyndigande av samhällsutbetalningar hos ramavtalsbankerna, vilket inte alltid är fallet då det händer att anställda använder sitt privata BankID i tjänsten.[47]

Vid myndigheternas användning av e-legitimationer (BankID) vid utbetalningar regleras säkerhetslösningarna av de enskilda bankerna. I sin rapport beskriver Riksrevisionen att bankerna själva hävdar att den befintliga tekniska säkerheten är fullgod. Betalningsförordningen[48] reglerar statliga myndigheters betalningar, där de enskilda myndigheterna ansvarar själva för säkerheten i sina verksamheter och de betalningar som de kontrollerar. Myndigheterna måste utnyttja de ramavtal för betalningstjänster som Riksgäldskontoret har tecknat, men kan i övrigt besluta över de egna säkerhetsrutinerna och den interna kontrollen inom ramen för vad som i övrigt är tillåtet.

I såväl samverkan mellan myndigheter som inom de enskilda myndigheterna bör arbetet kopplat till utformning och användning av elektroniska tjänster ske genom

---

[44] Intervju med e-legitimationsnämnden 2015-05-22.

[45] Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

[46] Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

[47] Intervju Arbetsförmedlingen 2015-04-20.

[48] Förordningen (2006:1097) om statliga myndigheters betalningar och medelsförvaltning.

ett långsiktigt strategiskt arbete. Arbetet bör inkludera informationssäkerhet vid utveckling av tjänster och tekniska lösningar och bör kombineras med en kontinuerlig riskanalys av de tillhandahållna tjänsterna. Riskanalysen och utvecklingen av de enskilda lösningarna bör även betraktas utifrån ett processperspektiv som ser till såväl användningen av exempelvis e-tjänstelegitimationer som till de tekniska och funktionsmässiga lösningarna. Ett exempel på det förstnämnda är att tillhandahålla stöd för myndighetspersonal vid användning av e-tjänstelegitimationer som bidrar till förståelse och förtydligar risker vid användandet. Därtill bör säkerhetslösningar bygga på tillitsnivåer som bygger på ”best practice” och internationella standards. För att detta ska kunna ske i form av ett strategiskt långsiktigt arbete bör det finnas en tydlig process för hur arbetet levandehålls och ständigt utvecklas.

Sammanfattning robusthetshöjande åtgärder:

- Beakta e-legitimation utifrån ett långsiktigt perspektiv
- Samverka för framgång i utvecklingsarbetet och förbättrad säkerhet
- Säkerställ rätt och tillräcklig nivå för tekniska lösningar

5 Avslutande kommentarer

Studien har utgått från, och även visat, att myndigheter använder sig av e-legitimation som kritisk resurs vid samhällsviktiga utbetalningsprocesser. Användningen sker vid handläggningen (e-tjänstelegitimation) vid framtagande av betalningsuppdrag såväl som vid bemyndigandet av betalningar (BankID). Studien har även beskrivit den nuvarande utvecklingen av en infrastruktur för svensk e-legitimation som myndigheterna kan använda sig av vid upphandling för stödtjänster gällande elektronisk identifiering. Bemyndigandet av betalningar innefattas för närvarande inte inom den enskilda infrastrukturen utan regleras av avtalen med bankerna.

Under flera av de intervjuer som genomförts har det framförts önskemål om ett utpekat tillsynsansvar för e-legitimationer i ett livscykelperspektiv. Flera av de intervjuade har understrukit behovet av samarbete mellan marknadens utveckling av nya säkerhetslösningar, tillsynsperspektivet och utvecklingen av myndigheternas interna e-tjänster. Att testa befintliga reservrutiner och särskilt i samråd med bankerna lyfts därtill fram som en åtgärd som bör prioriteras inom myndigheternas verksamheter.

6 Nästa steg

Det har tidigare konstaterats ett behov av fortsatt säkerhetsarbete gällande risker för identitetsstöld, felaktig utgivning och missbruk av annans identitet samt risken för att personuppgifter görs tillgängliga på ett oacceptabelt eller lagstridigt sätt.

Under denna studie har ytterligare behov påträffats, nedan presenteras identifierade förslag till fortsatt arbete inom såväl som utanför SOES.

6.1 Förslag till fortsatt arbete inom SOES

Det har identifierats ett behov av samverkan och erfarenhetsutbyte inom beroendet av e-legitimationer för SOES-myndigheternas samhällsviktiga utbetalningar. Förslagsvis bör inblandande aktörer, delta under gemensamma samverkansövningar, där scenario kan involvera ett särskilt fokus på e-legitimation, för att få ökad förståelse för vilka gemensamma beroenden och samverkansbehov som finns. Det bör även säkerställas att reservrutiner, i händelse av avbrott i kommunikationen mellan myndigheter och ramavtalsbank, finns på plats, samt att övningar om möjligt även genomförs tillsammans med ramavtalsbank. Aktörerna bör gemensamt utveckla redundans och kontinuitetsplaner inom den finansiella sektorn samt om möjligt vidareutveckla befintliga reservrutiner.

En risk som har identifierats under studien är den bristande tekniska lösningar som ligger till grund för att myndigheterna ska kunna använda e-legitimation på ett säkert sätt. Det är av stor vikt att SOES-myndigheterna säkerställer en tillräcklig nivå på tekniska lösningar. SOES-myndigheterna bör säkerställa sin interna kompetens vad gäller tekniska lösningar samt sin förmåga för kravställning för att kunna ställa tillräckligt höga krav avseende prioritering och segmentering i SLA-avtalen.

De enskilda SOES-myndigheterna bör även säkerställa att det finns tydligt utarbetade processer och rutiner för användning av e-legitimationer inom myndigheternas verksamheter (exempelvis vid attestering av beslut och bemyndigande av utbetalningar) samt att dessa upprätthålls. Därtill bör myndigheterna säkerställa att lämpliga stöd för dess medarbetare utformas, som förtydligar risker vid användandet och bidrar till förståelse för vikten av att följa utarbetade rutiner. En framgångsfaktor i detta arbete är ett strategiskt långsiktigt arbete som säkerställer att arbetet levandehålls.

SOES-myndigheterna bör avslutningsvis bevaka remissen ”Kompletterande bestämmelser till EU-förordningen om elektronisk identifiering”.

6.2 Förslag till fortsatt arbete för annan aktör

Det har under informationsinsamling till denna studie uttryckts behov av en enskild myndighet med enskilt ansvar för *tillsyn* av e-legitimationer utifrån ett livscykelperspektiv. Detta är en brist som bör ses över för att beakta myndigheternas användning e-legitimation utifrån ett långsiktigt perspektiv.

Bilagor

Bilaga 1 - Intervjuer

Genomförda intervjuer

Datum	Myndighet	Deltagare
8/4	Riksgälden	Karin Wernvall, Maria Lundin
15/4	Försäkringskassan	Susanne Wallinder
20/4	Arbetsförmedlingen	Eva Sundén
24/4	e-delegationen	Jan Sjösten
24/4	Skatteverket	Jan Sjösten
19/5	PTS	Björn Scharin
22/5	e-legitimationsnämnden	Eva Sartorius, Eva Ekenberg

Bilaga 2 - Intervjumall

Samverkansområdet
Ekonomisk säkerhet

SOES AG Analys

- Frågeställningar till intervju om eID

Försäkringskassan
FÖRSVARSMAKTEN
Länsstyrelserna
MSB
RIKSGÄLDEN
Skatteverket
Arbetsförmedlingen
PENSIONS MYNDIGHETEN
Representanter från kommuner
csn

Samverkansområdet
Ekonomisk säkerhet

Bakgrund

Syfte

- Att skapa förutsättningar för de individer som är centrala inom samhällsviktiga utbetalningsprocesser att förstå och förhålla sig till eID på ett effektivt sätt i risk- och kontinuitetshanteringsarbetet.

Mål

- Att på ett kortfattat och lättillgängligt sätt beskriva vad eID och liknande certifikat är; hur de används av myndigheter inom samhällsviktiga utbetalningsprocesser; samt ge exempel på såväl vidtagna som potentiella robusthetshöjande åtgärder för säkrare eID-tjänster.

2

Samverkansområdet
Ekonomisk säkerhet

Exempelfrågeställningar: Myndigheter

Funktion

- Hur används eID och andra certifikat inom myndigheten?
  - För skapande av betalningsuppdrag?
  - För samhällsutbetalningar? (ex. bemyndigande direkt i fil med betalningsuppdrag eller elektronisk signatur i bankens webbtjänst)
- Av vilken betydelse är valet av certifikatform vid olika aktiviteter inom myndigheten?
- Är det vanligt att myndigheter använder samma form av certifikat för liknande aktiviteter?
- Använder er myndighet olika leverantörer för certifikaten?

Robusthet och redundans

- Hur påverkar valet av certifikat säkerheten?
- Vilka robusthetshöjande åtgärder har vidtagits för att bemöta det kritiska beroendet inom er myndighet? (*Vid sidan av multipla signeringar*)
- Vilken redundans finns?
- Vilken kompetens finns inom myndigheten för att hantera dessa frågor?
- Om en kapning av något utav era certifikat skulle inträffa, hur skulle det upptäckas?

3

Samverkansområdet
Ekonomisk säkerhet

Exempelfrågeställningar: Experter

- Hur ser processen för kapning av eID och certifikat ut?
- Har kapningar av myndighetscertifikat inträffat i Sverige?
  - För åtkomst till känslig information?
  - För åtkomst till samhällsutbetalningar?
- Är det möjligt/troligt att sådana kapningar inträffar?
- Vad skulle en sådan händelse potentiellt innebära för den enskilda myndigheten?
- Vilka robusthetshöjande åtgärder används för att bemöta det kritiska beroendet?
  - I vilken utsträckning används dessa?

4

Bilaga 3 - Litteraturförteckning

Rapporter:

Verva (2008) *Slutrapport om säkert elektroniskt informationsutbyte och säker hantering av elektroniska handlingar*.

e-legitimationsnämnden (2015). *Analys och hantering av rapport från MSB – Analys av informationssäkerheten i Svensk e-legitimation*. Dnr 131676133-14/9516.

e-legitimationsnämnden(2012). *Kartläggning av internationella tillitsramverk*. Kirei 2012:09. Källa: [https://www.kirei.se/xfiles/tillit-pm.pdf] hämtad 2015-05-27.

e-legitimationsnämnden (2014). *Regeringsuppdrag – fördjupade analyser av Svensk e-legitimation ur ett säkerhetsperspektiv*. Dnr 131582625-14/9513.

MSB (2014). *Analys av informationssäkerheten i Svensk e-legitimation.* MSB-dnr 2014-1360.

Riksrevisionen(2010). *Säkerheten i statens betalningar*. RiR 2010:13.

Skatteverket (2015). *Utgivare av e-legitimation*. Källa: [http://www.skatteverket.se/privat/sjalvservice/allaetjanster/omelegitimation/utgivareavelegitimation.4.18e1b10334ebe8bc8000736.html] hämtad 2015-05-29.

SOES AG Riskanalys (2014). *Riskanalys för myndigheterna inom SOES*.

SOU (2010:104) *E-legitimationsnämnden och Svensk e-legitimation*.

SOU (2009:86). *Strategi för myndigheternas arbete med e-förvaltning.*

Webkällor:

CGI (2015). *Om utgivare av e-legitimation.* Källa: [http://eid.primeportal.com/eid/Sidor/utgivareeleg.aspx] hämtad 2015-05-29.

Dagens industri (2015). *Om kapning av e-legitimation*. Källa: [http://www.di.se/artiklar/2014/11/17/sa-kapar-bovarna-ditt-konto/] hämtad 2015-05-29.

e-delegationen(2015). *Om e-legitimation*. Källa: [http://www.edelegationen.se/Stod-och-verktyg/E-legitimation/] 2015-05-29.

Finansiell ID-teknik (2015). *Om BankID.* Källa: [https://www.bankid.com/om_bankid/detta_ar_bankid] hämtad 2015-05-27.

Finansiell ID-teknik (2015). *Så fungerar BankID*. Källa: [http://www.bankid.com/sv/Vad-ar-BankID/Sa-fungerar-BankID/] hämtad 2015-05-27.

Svenska datatermgruppen (2015). *Förkortningslistan*. Källa: [http://www.datatermgruppen.se/foerkortningslistan.html] hämtad 2015-05-27.

Svenska datatermgruppen (2015). *Om kryptering*. Källa: [http://www.datatermgruppen.se/index.php?option=com_content&view=article&id=89&Itemid=91&obj=a137&uttr=SSL] hämtad 2015-05-27.

Lagar och förordningar:

Förordningen (2006:1097) om statliga myndigheters betalningar och medelsförvaltning

Signaturlagen (2000:832) om kvalificerade elektroniska signaturer.