Dokumentklass:	Öppen
Datum:	2015-12-10
Version:	1.0

Slutrapport:

Robusthetshöjande åtgärder 2015

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.*

Innehåll

1 Inledning

Under 2013 inleddes arbetet *Samhällskonsekvensanalys för myndigheterna inom SOES* med målet att identifiera gemensamma kritiska beroenden och resurser för leverans av samhällsviktig verksamhet inom ramen för SOES-myndigheternas ansvarsområde. Under 2013 och 2014 kartlades sammanlagt elva samhällsviktiga betalningsprocesser och under 2015 har ytterligare två processer kartlagts.

Under 2014 valde SOES att ta resultatet av 2013 års arbete vidare i delprojektet *Robusthetshöjande åtgärder*, genom ett antal åtgärder kopplat till resurser och/eller aktiviteter som bedömts kritiska för kartlagda processer och på så sätt också för SOES syfte och mål för verksamheten.[1] Under 2014 genomfördes även ett arbete med att identifiera och analysera övergripande risker som kan äventyra SOES måluppfyllnad, vilket resulterade i rapporten *Riskanalys för myndigheterna inom SOES*.

Under 2015 har SOES Arbetsgrupp Analys identifierat ytterligare robusthetshöjande åtgärder, dels genom fördjupning kopplat till fem utvalda risker baserat på SOES övergripande riskanalys 2014, dels baserat på identifierade gemensamma beroenden från tidigare års processkartläggningar. Åtgärderna har valts ut och definierats så att de, direkt eller indirekt, förväntas bidra till att göra de kartlagda processerna mer robusta samt stärka SOES-myndigheternas förmåga att hantera gemensamma övergripande risker.

En kortare beskrivning av respektive åtgärd ges i kapitel 2, *Genomförda åtgärder*. Utkomsterna i sin helhet återfinns som separata bilagor.

1.1 Syfte och mål

Det övergripande syftet med delprojektet *Robusthetshöjande åtgärder* var att bidra till att göra SOES samhällsbetalningar mer robusta samt stärka SOES-myndigheternas förmåga att hantera gemensamma övergripande risker. Målet var att uppnå detta genom att:

- Genomföra en fördjupad analys av 5 utvalda risker (baserat på den övergripande riskanalys som genomförts under 2014)

- Genomföra fördjupade analyser av utvalda identifierade gemensamma beroenden (bl.a. baserat på kartlagda processer 2014).

- Identifiera ytterligare robusthetshöjande åtgärder baserat på genomförda analyser. Åtgärdsförslag som tas fram föreslås hanteras inom ramen för SOES-projekt för kommande år alternativt överlämnas till ansvarig/berörd aktör.

[1] SOES ska verka för att enskilda individer, företag och det allmänna ska ha tillgång till och förtroende för att samhällets betalningar fungerar och för att 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.

1.2 Metod

Arbetet med att välja ut och definiera vilka robusthetshöjande åtgärder inleddes med en genomgång av resultat och slutsatser i slutrapporterna från 2014 års arbete. Utifrån AG Analys diskussioner sammanställdes en bruttolista med möjliga åtgärder. Bruttolistan diskuterades och en nettolista prioriterades sedan fram av medlemmarna i SOES AG Analys.

Bland tidigare identifierade gemensamma övergripande risker, genomfördes för respektive utvald risk en särskild diskussion inom arbetsgruppen för att fastställa utgångspunkt och form för fördjupningen. För respektive robusthetshöjande åtgärd utvecklades ett underliggande syfte och mål, samt metod för genomförande.

Metoden för de robusthetshöjande åtgärderna har genomgående utgått från intervjuer och workshops med representanter från SOES myndigheter, samt med stöd i relevant dokumentation från ett antal öppna källor.

2 Genomförda åtgärder

I detta kapitel presenteras en kort sammanfattning av respektive genomförd robusthetshöjande åtgärd; *varför* åtgärden valts ut och genomförts, *vad* den innebär, samt kort om huvudsakliga *resultat* och slutsatser. Varje åtgärd återfinns i sin helhet som separat bilaga till denna rapport.

2.1 Fördjupad analys av gemensamma identifierade risker

Analysen har i ett första steg utgått från de risker som beskrivits och analyserats i SOES rapport *Riskanalys för myndigheterna inom SOES* från 2014. Urvalet av risker som har prioriterats för 2015 års fördjupade analys har baserats på kriterierna att utvalda risker:

- Är relevanta för en stor del av SOES-myndigheterna
- Kan leda till stora konsekvenser för samhället
- Kan påverka en kritisk del av den gemensamma infrastrukturen
- Kan ha stor påverkan på förtroendet för SOES-myndigheterna
- Ej har analyserats eller kartlagts tidigare (i helhet)

AG Analys har därutöver prioriterat de risker som av arbetsgruppen ansetts ligga mest i tiden och förväntas bli mest aktuella för SOES-myndigheterna framöver. Då riskerna från 2014 skiljer sig åt avseende omfattning och art, skiljer sig även fördjupningarna under 2015 åt avseende fokus och omfattning. För vissa risker har fördjupningen bestått i att analysera möjligheten till en viss reservrutin som föreslagits under 2014. För andra risker har den generella riskbeskrivningen från 2014 fördjupats genom att fokusera på en mer specifik aspekt av den gemensamma risken:

Övergripande risk 2014	Fördjupning 2015
Externt IT-angrepp	eID - En studie om användningen av e-legitimation för samhällsviktiga utbetalningar inom SOES-myndigheterna
Internetstörningar	Swedish Government Secure Intranet (SGSI) för robust kommunikation
Påverkan mot nyckelpersoner att utföra otillbörlig handling	Otillåten påverkan mot nyckelpersonal
Haveri hos gemensam IT-leverantör	Kontanthantering av samhällsutbetalande myndigheter och risken för penningtvätt
Enskild utbetalande ramavtalsbank står stilla	Single Euro Payment Area (SEPA) – Potentiella robusthetshöjande åtgärder till följd av SEPA

Gemensamt för samtliga fördjupade analyser är att analyserna bidrar till ökad kunskap om myndighetsövergripande risker, sårbarheten för riskerna och hur dessa kan förebyggas och hanteras. Den ökade kunskapen möjliggör för respektive myndighet att stärka sin egen robusthet och på så sätt bidra till en ökad gemensam robusthet i helheten. Genom analyserna har också ytterligare robusthetshöjande åtgärder identifierats baserat på fördjupningarna. Åtgärdsförslagen har föreslagits att hanteras inom ramen för SOES-projekt 2016 alternativt överlämnas till ansvarig/berörd aktör. Genomförandet av de

identifierade åtgärdsförslagen kan i förlängningen bidra till att förebygga allvarliga störningar av händelser som annars kan få allvarliga samhällspåverkande effekter.

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

Varför?

I samband med SOES kartläggning av samhällsviktiga processer har ett beroende till såväl fysiska som elektroniska identitetshandlingar (eID) kunnat konstateras. I tidigare riskanalyser har även risken för externa IT-angrepp identifierats och analyserats på en övergripande nivå. Externa angrepp i form av t.ex. ID-kapning kan ge negativa konsekvenser i form av uteblivna, försenade eller felaktiga utbetalningar, vilket i förlängningen även kan minska förtroendet för SOES-myndigheterna.

Ett behov identifierades av att fördjupa denna riskbild, för att skapa bättre förutsättningar för de individer som är centrala inom samhällsviktiga betalningsprocesser att förstå och förhålla sig till eID på ett effektivt sätt i risk- och kontinuitetshanteringsarbetet.

Vad?

Analysen (Bilaga 1) beskriver vad e-legitimation är, hur de används av myndigheter inom samhällsviktiga utbetalningsprocesser, samt vilka risker och sårbarheter som finns inom området. Analysen ger exempel på såväl vidtagna som potentiella robusthetshöjande åtgärder för säkrare eID-tjänster. Arbetet har utgått från ett antal relevanta rapporter men framförallt från intervjuer med representanter från myndigheter inom SOES, samt med aktörer utanför SOES såsom Post- och Telestyrelsen (PTS), e-legitimationsnämnden samt e-delegationen.

Resultat

- Studien beskriver och visualiserar hur myndigheterna använder sig av e-legitimation som kritisk resurs vid samhällsviktiga betalningsprocesser inom såväl handläggningsfunktionen som ekonomifunktionen.
- Underliggande riskområden kopplat till användningen av eID inkluderar intern kompetens/bristande resurser, tekniska lösningar från leverantör, avbrott i kommunikation mellan myndighet och ramavtalsbank, samt graden av tillsyn inom området.
- 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, t.ex. huruvida s.k. mjuka eller hårda certifikat används. Kravställning mot utfärdare om s.k. tillitsnivåer kan även vara ett sätt att minimera risker kopplat till eID.
- Den nuvarande utvecklingen av en infrastruktur för svensk e-legitimation kan användas av myndigheterna vid upphandling för stödtjänster gällande elektronisk identifiering.
- Fortsatt arbete inom SOES kopplat till eID rekommenderas innefatta följande:

- SOES bör överväga att vid gemensamma samverkansövningar involvera ett särskilt fokus på e-legitimation, för att få ökad förståelse för reservrutiner och samverkansbehov. Övningar bör även genomföras tillsammans med ramavtalsbank
- 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.
- SOES-myndigheterna bör säkerställa att lämpliga stöd för dess medarbetare utformas, som förtydligar risker vid användandet och bidrar till förståelse för vikten av att följa utarbetade rutiner.
- SOES-myndigheterna bör avslutningsvis bevaka remissen ”Kompletterande bestämmelser till EU-förordningen om elektronisk identifiering”.
- I studien uttryckts ett behov av att en enskild myndighet utses till ansvarig 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.

Swedish Government Secure Intranet (SGSI) för robust kommunikation

Varför?

I takt med att teknikberoendet ökar i samhället, ökar även beroenden till säker kommunikation mellan myndigheter. System som stödjer information och kommunikation blir därmed alltmer kritiska resurser, vilket även gäller SOES-myndigheter. Myndigheterna inom SOES är i hög grad beroende av fungerande elektronisk kommunikation, vilket tydligt framgår av beroendet till internet och datakommunikation som har identifierats i genomförda samhällskonsekvensanalyser. Därutöver identifierades ”internetstörningar” som en de övergripande och gemensamma riskerna för SOES-myndigheterna i tidigare års riskanalys. I 2014 års analys föreslogs att Swedish Government Secure Intranet (SGSI) skulle kunna utgöra ett robusthetshöjande alternativ vid internetstörningar. SGSI är ett avgiftsfinansierat nätverk för säker kommunikation mellan myndigheter i Sverige och i Europa.

Vad?

Analysen (Bilaga 2) beskriver Swedish Government Secure Intranet (SGSI) samt hur SGSI kan öka robustheten i myndigheternas kommunikation och därigenom reducera risken för internetstörningar. Analysen har främst utgått från en intervjustudie med representanter från Myndigheten för samhällsskydd och beredskap (MSB), som är systemägare till SGSI, men även från ett antal dokument som beskriver SGSI samt relevanta utredningar med koppling till området. Rapporten innehåller även en beskrivning av två internationella motsvarigheter till SGSI.

Resultat

- SOES-myndigheternas beroende till internet och datakommunikation medför påtagliga negativa konsekvenser kopplat till risken för internetstörningar. En robusthetshöjande åtgärd för att bidra till att denna risk minimeras, har varit att

beskriva de möjligheter SGSI innebär som alternativ för robust och säker kommunikation.

- SGSI möjliggör en säkrare kommunikation, i termer av tillgänglighet, tillförlitlighet och konfidentialitet, bl.a. genom separering från internet, dubblerad teknisk utrustning och krav på certifikat.
- Flera, men inte samtliga, av SOES-myndigheterna är anslutna till SGSI men kunskapen om möjligheterna med SGSI har bedömts som låg inom SOES myndigheter.
- En möjlig utmaning kring systemet, utifrån SOES perspektiv, är huruvida privata aktörer, såsom ramavtalsbanker, kan anslutas och i så fall hur.
- Fortsatt arbete inom SOES kopplat till SGSI rekommenderas innefatta följande:
    - Genomförande av en fördjupad studie av hur anslutna SOES myndigheter använder SGSI och vilka styrkor och utmaningar som kunnat konstateras vid användningen. Studien bör även utreda möjligheten att ansluta privata aktörer till SGSI.
    - Vidare bör SOES bevaka resultatet från Informationssäkerhetsutredningen NISU 2014, som bl.a. föreslår att samtliga myndigheter som pekas ut i förordningen (2006:942) om krisberedskap och höjd beredskap ansluts till SGSI.

Otillåten påverkan mot nyckelpersonal

Varför?

En av de risker som SOES identifierade i den övergripande riskbeskrivningen 2014 var ”påverkan mot nyckelpersoner att utföra otillbörlig handling”. Ofta används begreppet *otillåten påverkan*, som är ett samlingsnamn för olika handlingar som syftar till att påverka tjänstemän i deras arbete, såsom trakasserier, hot, våld och korruption. Myndigheters utsatthet för olika former av påverkan att utföra sådana handlingar, t.ex. obehöriga betalningar, har uppmärksammats i flera tidigare sammanhang, inom såväl SOES riskanalyser som i rapporter från andra aktörer. Även om dessa rapporter belyser många relevanta aspekter för SOES, så utgår de inte specifikt från SOES-myndigheterna, enskilt eller gemensamt. Rapporterna har inte heller specifikt behandlat otillåten påverkan som är riktad i syfte att påverka myndigheters utbetalningar, utan har genomförts på övergripande nivå och ofta med fokus på personsäkerhet.

Vad?

En fördjupad beskrivning (Bilaga 3) togs fram gällande risken för otillåten påverkan mot SOES-myndigheternas nyckelpersonal att utföra otillbörlig handling t.ex. otillbörlig utbetalning. Målet för fördjupningen är att presentera vilken nyckelpersonal inom SOES-myndigheterna som är utsatta för riskbilden, hur riskbilden förebyggs och hanteras av myndigheterna samt hur arbetet gemensamt kan förbättras inom SOES-

myndigheterna. Studien baserades framförallt på intervjuer med relevanta representanter från ett flertal SOES-myndigheter.

Resultat

- Studien beskriver vilka representanter som i huvudsak utsätts för otillåten påverkan och hur otillåten påverkan vanligen får uttryck, men även hur SOES-myndigheterna arbetar för att förebygga och hantera risken. Därutöver påvisar analysen vissa skillnader mellan de myndigheter som intervjuats, både avseende exponering mot och hantering av risken.
- Otillåten påverkan kan få allvarliga effekter på samhällets betalningar. Förutom att den är felaktig, kan en otillbörlig utbetalning även leda till förtroendeförlust från allmänheten för den aktuella SOES-myndigheten, men också för betalningssystemet i stort.
- Analysen bidrar till ökad robusthet inom SOES, genom att öka kännedomen om risken i en SOES-kontext. På så sätt skapas förutsättningar för att förebygga och hantera risken.
- Fortsatt arbete inom SOES kopplat till otillåten påverkan rekommenderas innefatta följande:
    - SOES-myndigheterna bör gemensamt se över möjligheten att skapa ett samverkansforum för informations- och erfarenhetsutbyte inom ramen för otillåten påverkan, samt i högre utsträckning nyttja de befintliga nätverk som finns inom området.
    - I samverkansarbetet har föreslagits att föreslås det att myndigheterna ser över möjligheterna att på ett förtroendefullt sätt kunna kan byta information mellan myndigheter ur erfarenhetsdelande syfte utifrån respektive organisations befintliga informationshanteringsregler.
    - SOES-myndigheterna bör enskilt se över rutiner och metoder för säkerhetsrelaterade samtal och uppföljning av anställd nyckelpersonal i syfte att öka förmågan för att upptäcka otillåten påverkan.

Kontanthantering av samhällsutbetalande myndigheter och risken för penningtvätt

Varför?

En av de risker som bedömdes vara prioriterad inom ramen för SOES fortsatta arbete var risken ”haveri hos gemensam IT-leverantör”. I diskussioner inom AG Analys betonades att en högre grad av kontanthantering skulle kunna bli aktuell vid sådana händelser, och att kontanthantering hos myndigheterna i sin tur är förknippat med vissa risker. Den aspekt av myndigheternas kontanthantering som bedömdes som mest

relevant att fokusera på, ansåg arbetsgruppen, handlar om risken för att kontanter används för att tvätta pengar i betalning av återkrav till SOES-myndigheterna.

Vad?

Arbetsgruppen beslutade att undersöka hur SOES-myndigheternas[2] mottagande och hantering av kontanta medel kan leda till bedrägerier och möjlighet för penningtvätt. Analysen (Bilaga 4) baserades dels på tidigare domar och rapporter inom området, dels på intervjuer med ett flertal SOES myndigheter. Syftet har bland annat varit att beskriva de underliggande krav som finns på myndigheter att ta emot kontanter, myndigheternas syn på risken samt vad myndigheterna kan göra för att hanterera risken.

Resultat

- Vissa av myndigheterna ser en potentiell risk för att medborgare använder kontanta återbetalningar som ett sätt att tvätta pengar. Risken berör dock Skatteverket i mindre omfattning, då myndigheten genom lag har andra möjligheter att neka kontanta betalningar.
- Analysen bidrar till stärkt robusthet inom SOES, genom att kännedom om risken ökar. Därutöver kan de förslag som lämnas i analysen leda till att risken förebyggs och hanteras på så sätt att risken mot myndigheterna minimeras.
- Möjliga lösningar skulle kunna handla om översyn av eller förtydligande i lagstiftning, exempelvis gällande myndigheternas möjlighet att neka kontanta betalningar.
- Analysen påvisar ett behov av utökat samarbete mellan SOES-myndigheterna för att bättre hantera denna risk. Fortsatt arbete inom SOES kopplat till kontanthantering rekommenderas innefatta följande:
    - Stärkt samverkan genom erfarenhetsutbyte inom området, t.ex. genom särskilda möten eller workshops med Kronofogden eller med Finanspolisen.
    - Myndigheterna bör säkerställa att lämpliga stöd för medarbetare utformas, som bidrar till en ökad förståelse för riskområdet och bättre rutiner för att förebygga och hantera risken.
    - En ytterligare del av stärkt samverkan skulle kunna komma från att inblandande aktörer deltar under gemensamma samverkansövningar, med särskilt fokus på misstänkt bedrägeri som kan leda till penningtvätt.

Single Euro Payment Area (SEPA) – Potentiella robusthetshöjande åtgärder till följd av SEPA

Varför?

En av de risker som identifierades under 2014 var ”att en enskild ramavtalsbank står stilla”. I bedömningen konstaterades att om kommunikationen till en enskild ramavtalsbank står stilla riskeras negativ påverkan på SOES verksamhet med felaktiga, försenade eller uteblivna samhällsbetalningar. AG Analys har identifierat ett behov av fördjupning av risken ”att enskild utbetalande ramavtalsbank står stilla”, där ökad harmonisering av format för betalningar genom SEPA har nämnts som en möjlighet till

[2] SOES myndigheter åsyftas i denna rapport till samhällsutbetalande myndigheter.

ökad robusthet i myndigheternas betalningar. Harmoniserande format för samtliga banker har beskrivits som en möjlighet att genomföra betalningar via andra banker i de fall där en enskild ramavtalsbank står stilla.

Vad?

En analys (Bilaga 5) genomfördes för att på ett kortfattat och lättillgängligt sätt beskriva vad SEPA är men även beskriva nuläge avseende SOES-myndigheternas syn på ökad harmonisering till följd av SEPA, samt möjligheten att genomföra betalningar via andra banker i de fall där en enskild ramavtalsbank står stilla.

För att nå den fastställda målsättningen har ett tillvägagångsätt i två steg valts. I ett första steg har material inventerats för att beskriva vad SEPA är och hur det fungerar. Därefter har intervjuer genomförs med SOES myndigheter för att undersöka potentiella effekter från införandet av SEPA dels avseende behovet av anpassningar och dels för robustheten i svenska samhällsbetalningar.

Resultat

- En svensk anpassning till SEPA skulle kunna medföra en stärkt robusthet, bl.a. då standardisering av format möjliggör att betalningar i Euro kan styras om för utbetalningar vid andra banker. SEPA-införandet skulle även i förlängningen kunna innebära harmoniserade format för betalningar i svenska kronor, vilket innebär än större robusthetshöjande effekt i takt med att betalningsvolymen ökar.
- Nulägesbeskrivningen av möjligheten att styra om betalningar, till följd av harmoniserade betalningsformat, kan emellertid inte bekräfta att ovan nämnda robusthetshöjande följder kommer att vara möjliga eller i så fall när sådana rutiner skulle kunna vara aktuella.
- Den robusthetshöjande effekten som SEPA-anpassningen kan medföra beror dels på utkomsten av en pågående svensk SEPA-anpassning och dels på om lydelser i gällande ramavtal samt bilaterala avtal mellan banker och myndigheter möjliggör dessa reservrutiner eller inte.
- Om myndigheterna ska kunna anpassa sig till de nya kraven i god tid behövs ytterligare förtydliganden kring hur det nya filformatet kommer att se ut och vilka åtaganden som myndigheterna behöver vidta. Denna avsaknad av information skapar i dagsläget stora osäkerheter kopplat till bland annat hur inhemska betalningar kommer att påverkas.
- Fortsatt arbete inom SOES kopplat till SEPA rekommenderas innefatta följande:
    - Närmare samverkan och erfarenhetsutbyte mellan myndigheterna inför omställningen till SEPA, framförallt gällande erfarenhetsdelning från de myndigheter som påbörjat anpassningen av SEPA.
    - Dialog och samarbete bör stärkas, bl.a. genom regelbunden kontakt mellan banker och SOES-myndigheter, gällande såväl anpassningar för svenska betalningar i Euro som myndigheters betalningar i SEK.
    - SOES bör bevaka Bankföreningens arbete med den kortsiktiga anpassningen till SEPA såväl som arbetet med utvecklingen av det svenska betalningssystemet.
    - SOES bör genomföra en analys under 2017, baserat på erfarenheterna från implementeringen av SEPA under 2016.

2.2 Fördjupad analys av gemensamma identifierade beroenden

Den fördjupade analysen av gemensamma identifierade beroenden har i ett första steg utgått från de beroenden som beskrivits och analyserats i SOES rapport *Samhällskonsekvensanalys för myndigheterna inom SOES* från 2014. Fördjupningen av beroenden från 2014 års kartläggningar har genomförts enligt:

Övergripande beroende 2014	Fördjupning 2015
Skatteverkets folkbokföringsregister med personuppgifter	Fördjupad analys: Folkbokföringsregistret med personuppgifter
Externa leverantörer	Kravställningsworkshop – Den kritiska kravställningen
System för myndigheters betalningar	Medborgarkonto – Tillämpligheten av systemet med NemKonton och NKS i svensk kontext

Åtgärderna har valts ut och definierats så att de, direkt eller indirekt, förväntas bidra till att göra de kartlagda processerna mer robusta. De antas även göra andra samhällsviktiga processer inom ramen för SOES-myndigheternas verksamhet mer robusta, då flera av de resurser och aktiviteter som åtgärderna riktar sig mot är frekvent förekommande och centrala i flera delar av SOES arbete.

Fördjupad analys: Folkbokföringsregistret med personuppgifter

Varför?

Inom ramen för såväl 2013 som 2014 års samhällskonsekvensanalys konstaterades att en fungerande informationsförsörjning SOES-myndigheterna emellan är av avgörande betydelse för samtliga kartlagda utbetalningsprocesser. I flertalet av dessa framgick tydligt att Folkbokföringsregistret med personuppgifter är en kritisk resurs. Då kunskapen om registret föreföll vara låg hos representanter som inte direkt arbetar med det, men som ändå är beroende av att det fungerar, beslutade SOES Arbetsgrupp Analys att göra en fördjupad analys och beskrivning av Folkbokföringsregistret med personuppgifter. Detta för att skapa förutsättningar för de individer som är centrala inom samhällsviktiga betalningsprocesser att förstå och förhålla sig till Folkbokföringsregistret med personuppgifter på ett effektivt sätt i sitt planerings-, kontinuitetshanterings-, och samverkansarbete.

Vad?

AG Analys har sammanställt en kortfattad, lättillgänglig beskrivning (Bilaga 6) av vad Folkbokföringsregistret med personuppgifter är och hur det används. Beskrivningen baseras framförallt på intervjuer med myndighetsrepresentanter som arbetar med registret, men även på information från öppna källor.

Resultat

- Folkbokföringsregistret med personuppgifter spelar en betydelsefull roll för förmågan hos myndigheter inom SOES att leverera samhällsviktiga betalningar.
- Fortsatt arbete inom SOES kopplat till Folkbokföringsregistret med personuppgifter rekommenderas innefatta följande steg:

- Översyn av SOES-myndigheternas reservrutiner kopplat till Folkbokföringsregistret med personuppgifter, samt hur reservrutiner tillgodoses i de egna kontinuitetsplanerna.
- Myndigheterna bör, inom ramen för sitt arbete med kontinuitetshantering, fastställa hur aktuell data de behöver och jämföra mot SLA som ges av Skatteverket.
- SOES bör genomföra en gemensam övning som kan fokusera på såväl avbrott i tillgängligheten till Folkbokföringsregistret med personuppgifter som läckage av känsliga uppgifter eller manipulering av data.
- SOES bör genomföra en fördjupad studie avseende bankernas användning av SPAR och hur detta förhåller sig till de kritiska betalningsprocesser som har kartlagts inom SOES, samt även överväga möjligheten att kopplat till kontinuitetsplaner nyttja SPAR i större utsträckning.

Kravställningsworkshop – Den kritiska kravställningen

Varför?

I tidigare analyser av SOES-myndigheternas kritiska processer, har ett starkt beroende kunnat konstateras av externa leverantörer, såsom leverantörer av IT-drift, el och olika former av elektronisk kommunikation. Tidigare analyser har tydliggjort behovet av ändamålsenlig och effektiv kravställning gentemot leverantörer, detta i samverkan mellan SOES myndigheter, inte minst då beroendet till externa leverantörer många gånger är gemensamt.

Vad?

En två timmar lång workshop genomfördes med relevanta deltagare från SOES-myndigheterna, Post- och telestyrelsen (PTS), Kammarkollegiet och Statens Servicecenter. Resultatet av workshopen sammanställdes i en rapport (Bilaga 7). Deltagarna var dels representanter från AG Analys, dels personer från myndigheterna som arbetar med frågor kring inköp och upphandling eller inom berörda områden såsom IT eller informationssäkerhet. Workshopen bestod av tre delmoment, där en uppsättning generella och specifika frågor var vägledande i respektive moment.

Syftet med arbetet var att fördjupa SOES-myndigheternas förståelse för kravställningsprocessen, och de utmaningar och möjligheter den innebär. Målet med workshopen var identifiera och beskriva övergripande och gemensamma erfarenheter från kravställningsarbetet, baserat på de enskilda organisationernas syn på kravställning. Målet var även att identifiera förslag till hur myndigheterna, enskilt och gemensamt, kan stärka sin kravställningsförmåga.

Resultat

- Genom upprättande av kontakter mellan myndigheter, inom och utanför SOES, kan erfarenheter delas och kunskap höjas avseende kravställningsprocessen. En stärkt kravställning mot leverantörer bidrar i förlängningen till upprätthållandet av samhällsviktiga betalningar från SOES-myndigheterna. Genomförandet av

workshopen och dokumentationen av erfarenheter och lärdomar utgör en robusthetshöjande åtgärd för SOES myndigheter.

- I arbetet identifierades en rad övergripande områden som myndigheterna bedömer som utmanande i kravställningsarbetet och framgångsfaktorer för att hantera utmaningarna.
- Fortsatt arbete inom SOES kopplat till kravställning mot leverantörer rekommenderas innefatta följande steg:
    - SOES-myndigheterna bör främja samlingsplatser mellan myndigheter och mellan myndigheter och leverantörer, bl.a. genom att nyttja de kontakter som upprättats inom ramen för workshopen.
    - SOES-myndigheterna föreslås upprätta en nätverksgrupp för frågor som berör kravställning vid upphandling. En sådan grupp skulle både kunna bidra till en generell kunskapshöjning hos myndigheterna och till konkret stöd i enskilda frågor.
    - SOES-myndigheterna bör nyttja de konkreta tips, goda exempel och verktyg som lyftes fram vid workshopen, såsom tips på vägledningsdokument, konkreta exempel för att skapa incitament hos leverantören, samt intervju- och utvärderingsmall för att bedöma leverantörers förmåga.
    - SOES-myndigheterna föreslås även, enskilt och gemensamt, sätta sig in i och gemensamt diskutera EU:s nya upphandlingsdirektiv och de nya upphandlingslagarna som väntas träda i kraft under 2016. Bland annat bör beaktas eventuella utökade möjligheter till dialog mellan myndigheter och leverantörer.

- Ett annat förslag som beskrivits är upprättandet av en erfarenhetsdatabas kopplat till kravställning. En sådan databas skulle kunna innehålla goda exempel och utmaningar från tidigare upphandlingar och bör inkludera en sökmotorfunktion. Vid workshopen föreslogs att ett sådant arbete skulle kunna initieras och drivas av Upphandlingsmyndigheten.

Medborgarkonto – Tillämpligheten av systemet med NemKonton och NKS i svensk kontext

Varför?

En förstudie och en fördjupad studie genomfördes av SOES under 2014 av det danska systemet med NemKonton. Analysen under 2014 har studerat och beskrivit den danska modellen och därigenom bidragit till att lärdomar dras från arbetet med robusthethöjande åtgärder i Danmark. Slutsatserna från studien gav en rad förslag till vidare analys, däribland att den danska modellens tillämplighet i Sverige borde undersökas vidare.

Vad?

Under 2015 har kompletterande studie (Bilaga 8) sökt undersöka systemet med medborgarkontons tillämplighet i Sverige för stärkta och mer robusta samhällsbetalningar. Arbetsgruppen har valt att inledningsvis inventera tidigare utredning samt pågående arbete inom Riksgälden. Dessa inledande moment bidrog till

att samla relevanta erfarenheter och lärdomar som kan analyseras utifrån den danska modellens tillämplighet i Sverige. Därefter har en behovsanalys, genom workshop och ett flertal intervjuer med SOES myndigheter genomförts utifrån SOES-myndigheternas syn på befintlig modell i Sverige och hur en modell liknande den danska skulle kunna tillämpas i en svensk kontext.

Resultat

- Myndigheter ser flera positiva potentiella effekter med införande av ett liknande system i Sverige, som kan stärka robustheten i samhällsbetalningar. SOES-myndigheterna har dock verksamheter som skiljer sig åt och således har olika förutsättningar att såväl stödja det fortsatta arbetet som att dra nytta av en implementering
- Potentiella positiva effekter med en modell liknande den danska har framförts gällande såväl effektivitet som säkerhet och robusthet. I förhållande till SOES syfte och mål om att verka för att samhällets betalningar fungerar och att förtroendet för dessa betalningar upprätthålls, betonas dessa aspekter i synnerhet.
- Behov har identifierats av bl.a. ytterligare utredning, ytterligare förankring och fastställande av roller och ansvar innan en motsvarande svensk modell kan upprättas. Möjliga steg mot denna robusthetshöjande åtgärd skulle kunna vara förankring av frågan inom berörda myndigheter och gärna på generaldirektörsnivå, upprättandet av en avsiktsförklaring, samt fokus på frågan i berörda myndigheters regleringsbrev.
- Det huvudsakliga arbetet med att möta utestående behov sker lämpligen fortsatt utanför ramen av SOES-analysarbete, även om de nätverk och forum som SOES inbegriper kan stödja det fortsatta arbetet. I ett längre perspektiv har bland annat föreslagits att en statlig utredning genomförs på området. Som ett första steg har även föreslagits att ett samverkansprojekt kan inrättas mellan ett antal berörda myndigheter i syfte att bygga en gemensam infrastruktur för samhällsbetalningar och med ambitionen att initiera det praktiska arbetet med att upprätta ett svensk system liknande det danska.

3 Avslutande kommentarer

Under 2015 har SOES Arbetsgrupp Analys genomfört ett flertal robusthetshöjande åtgärder, dels genom fördjupning kopplat till fem utvalda risker baserat på SOES övergripande riskanalys 2014, dels baserat på identifierade gemensamma beroenden från processer från tidigare års kartläggningar. Åtgärderna har valts ut och definierats på så sätt att de, direkt eller indirekt, förväntas bidra till att göra de kartlagda processerna mer robusta samt stärka SOES-myndigheternas förmåga att hantera gemensamma övergripande risker. Inom ramen för arbetet har även ytterligare robusthetshöjande åtgärder har identifierats. Genomfört arbete bidrar till en ökad kunskap om underliggande beroenden och sårbarheter kopplat till samhällets betalningar samt om myndighetsövergripande risker.

En övergripande slutsats från är att flera av åtgärderna pekar på behov av ytterligare fördjupade analyser, bl.a. analyserna identifierat nya utestående frågor eller då pågående arbete sker inom området, vilket medför osäkerhet om nuläge och framtid.

Många av de robusthetshöjande åtgärderna ger ingångsvärden till kunskapshöjande och robusthetshöjande aktiviteter inom de enskilda myndigheterna. Dessa lärdomar kan användas som en del av egna utbildningsinsatser och som del av arbetet med risk- och kontinuitetshantering. Den ökade kunskapen möjliggör för respektive myndighet att stärka sin egen robusthet och på så sätt bidra till en ökad gemensam robusthet.

Därutöver understryker flertalet av åtgärderna på nyttan av övning, enskilt inom myndigheterna och inom ramen för gemensamma samverkansövningar. Analyserna pekar på områden där myndigheters förmåga att hantera risker eller avbrott i kritiska beroenden skulle gynnas av övning med specifikt fokus på analyserade risker och beroenden.

I arbetet har flera åtgärder belyst behovet av särskilda samverkansforum utanför SOES, för att diskutera specifika frågor kring analyserade risker och beroenden. Dessa frågor kräver ofta ett löpande engagemang och inte bara enskilda analyser och workshoptillfällen. Frågorna kräver även att särskilda funktioner inom myndigheterna involveras, och i vissa fall även att organisationer utanför SOES behöver involveras.

Externa aktörer utgör inte sällan myndighetsgemensamma kritiska beroenden, vilket understryks av såväl beroende- som riskanalyser inom 2015 års robusthetshöjande åtgärder. Behov av stärkt kravställning mot externa aktörer betonas även i årets analysarbete.

Avslutningsvis är en gemensam slutsats från arbetet att möjligheten till informations- och erfarenhetsdelning mellan myndigheterna i hög grad styrs av myndigheters interna regler och rutiner för sekretess. I dagsläget ges möjligheter till informations- och erfarenhetdelning såväl inom SOES som inom andra mer eller mindre formella myndighetsnätverk. Myndigheterna ser dock ofta ett behov av förtydligande av vilken information som kan delas och identifierar ett behov av att se över åtgärder för att ytterligare stärka möjligheten att dela information och erfarenheter.

4 Nästa steg

Utifrån de slutsatser som dras i föregående kapitel kan även följande övergripande förslag på fortsatt arbete lämnas.

Genomföra riktad omvärldsbevakning och ytterligare analys

- Bevaka pågående arbete och förändringar inom analyserade områden som är under utveckling, t.ex. i form av särskilt relevanta statliga utredningar, arbete från aktörer utanför SOES, m.m.
- Genomföra ytterligare fördjupade analyser inom områden som är under utveckling och som väntas präglas av förändring.
- Genomföra ytterligare fördjupade analyser inom områden som inte inkluderats inom ramen för 2015 års arbete, t.ex. av risker från 2014 som inte prioriterats under 2015 eller som ett resultat av åtgärder som föreslagits i 2015 års analyser.

Främja informations- och erfarenhetsutbyte

- Förtydliga och vid behov eventuellt se över myndigheters interna regler och rutiner för sekretess. Sådant arbete kan beakta möjlighet till ändringar, alternativt förtydliga vilka möjligheter som finns till informations- och erfarenhet inom ramen för befintlig sekretess. Ett steg mot ökad tydlighet skulle kunna vara att ta fram ett stöddokument, t.ex. som ”Vägledning till dialog mellan SOES myndigheter – möjligheter och begränsningar till informations- och erfarenhetsdelning”.
- Främja och/eller upprätta samverkansforum för särskilda frågor, som gynnas av löpande samverkan inom specifika sakfrågor och/eller där aktörer utanför SOES bör ingå.

Stärka förmågan till kravställning

- Nyttja befintliga stöd och vägledningar inom kravställningsområdet, samt utveckla nya stöd och verktyg för att stärka myndigheters förmåga till kravställning. Detta kan inkludera nyttjandet av verktyg från aktörer utanför SOES, men även att SOES t.ex. utvecklar nya mallar, checklistor, vägledningar eller en erfarenhetsdatabas inom området.
- Föra en fortsatt dialog och samverkan med relevanta externa aktörer såsom PTS, Kammarkollegiet och Statens Servicecenter för att få ökad kunskap om kravställnings- och upphandlingsprocessen samt de ramar och regelverk som styr denna. Dessa aktörer kan bidra med relevanta lärdomar och praktiska stöd och verktyg i myndigheternas kravställningsarbete.

Kontrollera genom översyn, test och övning

- Gemensamt se över och testa kontinuitetsplaner och reservrutiner, samt säkerställa att dessa är förenliga med varandra. Översyn kan i ett första steg göras med fokus på ett specifikt gemensamt beroende eller med fokus på hanteringen av en särskilt utpekad risk.
- Öva scenarier som tydliggör och ökar förståelsen för såväl myndighetsgemensamma risker som gemensamma beroenden i kritiska processer. Övningarna kan, och bör i vissa fall, även inkludera aktörer utanför SOES såsom ramavtalsbanker eller leverantörer av särskilda gemensamma beroenden.