Myndigheten för digital förvaltning (Digg)

Synpunkter på krav och villkor för leverantörer inom auktorisationssystem

(2024-3372)

Utifrån de utgångspunkter Försäkringskassan har att beakta, har myndigheten följande synpunkter.

Allmänna synpunkter

E-legitimeringsfrågan är en kritisk del av Försäkringskassan verksamhet samt i Försäkringskassans tillhandahållande av samordnad och säker it-drift (SSSID) i enlighet med förordningen (2024:1005) om samordnad och säker statlig it-drift.

I dagsläget tillhandahåller Försäkringskassan it-tjänster till över 70 myndigheter, inklusive 21 länsstyrelser. I olika erbjudanden till anslutna myndigheter erbjuds också säkra inloggningsmetoder baserat på till exempel e-tjänstelegitimationer och e-legitimationer för att stärka säkerheten mot myndighetens olika avtalade tjänster.[1]

Försäkringskassans förmåga att säkra robusthet och kontinuitet

Försäkringskassans uppfattning är att enskilda myndigheters ansvar och möjligheter att säkra sina behov inte bör begränsas. Om en myndighet som ansluter sig till auktorisationssystemet identifierar hot och risker hos en leverantör, behöver myndigheten ha möjlighet att omgående kunna stänga av leverantören för att skydda den egna verksamheten, eventuella samverkande myndigheters verksamhet och i förlängningen även allmänheten.

Det finns säkerhetsrisker med centrala system vad gäller till exempel cyberangrepp mot samhällsviktig infrastruktur. Därför måste det vara väldigt tydligt att om förtroendet inte upprätthålls av leverantören så har den tillhandahållande myndigheten förutsättningar att omgående återkalla auktorisationen. Om auktorisationssystemet kommer att omfatta en teknisk implementation – vilket går att tolka i vissa delar av dokumenten, se till exempel avsnitt 4.1 (b) i anslutningsavtalet – blir systemet en kritisk funktion för hela statsförvaltningen. Systemet som samhällskritisk digital förmåga och som del av totalförsvaret blir därför en väldigt sårbar angreppspunkt. Att centralisera förmågan till en myndighet ökar avsevärt risken för påverkan och är negativt för tillgänglighet och robusthet.

För att minska sårbarhet och sprida risker för hela systemen bör istället de kritiska komponenterna i auktorisationssystemen, inklusive underliggande tjänster, tillhandahållas som förmåga från flera parter parallellt. Ett förslag skulle kunna vara att myndigheterna som anges i förordningen om samordnad och säker statlig it-drift får ett sådant uppdrag att parallellt tillhandahålla förmåga.

[1] Se https://www.sgit.se

Aktiv kontrollförmåga av leverantörer

Det är av yttersta vikt att få till den aktiva kontrollen, det vill säga att skapa en aktiv kontrollförmåga i förhållande till systemets leverantörer. Det här är en angreppsvektor för att exempelvis i egenskap av underleverantör komma in i systemet för att kunna göra skada.

Den tekniska arkitekturen

Den tekniska arkitekturen och tillhörande integration har en mycket stor påverkan på Försäkringskassan. Auktorisationssystemet får inte ha någon påverkan på exempelvis:

- etablerade integrationer (API/http, Relying Party API) med de olika e-legitimationsutfärdarna
- etablerade integrationer med Försäkringskassans olika e-tjänster
- tillhandahållandet av SSSID i enlighet med tillhörande förordning.

Övrigt

Försäkringskassan saknar slutligen några väsentliga punkter i dokumenten. Det måste finnas en tydlig hantering av underleverantörer till de som verkar som leverantörer inom systemet. Försäkringskassan hade vidare gärna sett skrivningar om löpande kontroller av bolagsföreträdares lämplighet och vilka åtgärder som kan vidtas vid förändrade ägarförhållanden.

Myndigheten för digital förvaltnings föreskrifter om krav på leverantörers ansökan om anslutning till auktorisationssystem för elektronisk identifiering och digital post

Försäkringskassan har följande synpunkter på de föreslagna föreskrifterna.

4 §

Försäkringskassan anser att kraven som ställs bör vara utformade genom att leverantören ska ge in underlag vid tidpunkten för ansökan för att möjliggöra Diggs kontroll av om ansökan ska godkännas eller avslås. Som kravet är formulerat nu undrar Försäkringskassan vilken impuls som skulle kunna aktualisera att Digg på eget initiativ inhämtar underlag? Försäkringskassan ser en risk att förlita sig på ett uppgifterna som leverantören lämnar är korrekta och förordar istället en formulering där underlag ska ges in för möjlighet till granskning innan godkännande. Av 12 § lagen (2023:704) om auktorisationssystem i fråga om tjänster för elektronisk identifiering och för digital post ”lagen om auktorisationssystem”, följer vilka underlag Digg kan begära in. Försäkringskassan ser dock inte att det föreslagna underlaget omfattas i 12 §.

7 §

Försäkringskassan föreslår att regleringen justeras så till vida att intygandet kombineras med ingivande av underlag motsvarande 6 § i de föreslagna föreskrifterna så snart sådant underlag är tillgängligt.

8 §

Försäkringskassan anser att kraven som ställs bör vara utformade genom att leverantören ska ge in underlag vid tidpunkten för ansökan för att möjliggöra Diggs kontroll av om ansökan ska godkännas eller avslås. Som kravet är formulerat nu undrar Försäkringskassan vilken impuls som skulle kunna aktualisera att Digg på eget initiativ inhämtar underlag? Försäkringskassan ser en risk att förlita sig på ett uppgifterna som leverantören lämnar är korrekta och förordar istället en formulering där underlag ska ges in för möjlighet till granskning innan godkännande. Vidare noterar Försäkringskassan att övriga krav (11 § lagen om auktorisationssystem) och möjlighet till inhämtande av

underlag (12 § samma lag) inte följer av föreskrifterna. Försäkringskassan föreslår att samtliga krav som uppställs i lagens 11 § konkretiseras i föreskrifterna och formuleras på så sätt att leverantören ska ge in underlag i samband med ansökan för granskning av Digg, när så är tillämpligt.

10 §

Försäkringskassan noterar att begreppet *låg risk* används i bestämmelsen och att detta begrepp inte är närmare definierat. Eftersom olika kreditupplysningsföretag använder sig av olika benämningar, kan det vara svårt att bedöma om det är fråga om *låg risk*.

12 §

Försäkringskassan välkomnar justeringen så till vida att man noterar föreslagen ansvarsbegränsning i utkastet till Anslutningsavtal punkt 16.5.

13 §

Försäkringskassan noterar att det saknas klargörande i såväl förslag till förskrifter som i utkastet till Anslutningsavtal att leverantören svarar för underleverantörs arbete såsom för eget. Detta föreslås justeras så till vida att detta skrivs in uttryckligen. Enligt Försäkringskassans uppfattning kan detta tillgodogöras genom skrivelse i Anslutningsavtal.

15 §

Försäkringskassan noterar att det i denna bestämmelse saknas förtydligande om hur leverantörer som är företag under bildande kan uppfylla kraven på nödvändig ekonomisk och finansiell kapacitet enligt 9 §.

16 §

Försäkringskassan anser att det inte med tydlighet framgår om kravet på godkännande enligt tillitsramverket omfattar samtliga punkter i ramverket. Finns det till exempel en möjlighet att särhantera e-legitimationsutfärdare respektive en leverantör av identifierings- och intygsfunktion?

Auktorisationssystem för elektronisk identifiering - Anslutningsavtal

Försäkringskassan har följande synpunkter på det föreslagna avtalet.

3. Definitioner

I punkten 7 definieras begreppet *legitimering* med att ”en Användare aktiverar sin e-legitimation ”. Försäkringskassan föreslår att begreppet *aktiverar* byts ut mot *använder*, *brukar* eller *nyttjar*.

4. Beskrivning av auktorisationssystem i fråga om tjänster för elektronisk identifiering

4.1

Innebär det som står i första stycket att en offentlig aktör, som vill använda sig av leverantörernas tjänster för de som har samordningsnummer, måste upphandla dessa vid sidan av auktorisationssystemet?

4.4

Av denna punkt framgår att *avsikten* är att endast offentliga aktörer anslutna till auktorisationssystem ska kunna förlita sig på identitetsintyg och annan information som används. Förhindrar detta att privata leverantörer av e-legitimationer samt leverantörer av identifierings- och intygsfunktion inte kan ingå i eller anslutas till auktorisationssystemet? Användandet av begreppet avsikt innebär att det inte är helt

tydligt om andra än offentliga aktörer ska kunna förlita sig på identitetsintyg och annan information som används.

6.3 Identifierings- och intygsfunktion, Identitetsintyg samt avancerade elektroniska underskrifter

6.3.1

Är det användande/brukande/nyttjande eller är det aktiverande som avses? Begreppen används inte konsekvent i de remitterade dokumenten.

Hur ser Digg på ett proxyförfarande där identitetsintyg inte levereras direkt från Leverantör till Offentlig aktör? Försäkringskassan har idag etablerade scenarios med IdP-proxy till ansluten myndighet till Försäkringskassan i och med uppdraget för SSSID.

6.3.2

Det behöver förtydligas vad som avses med *mindre tekniska förändringar*. Ett förslag är att skriva mindre tekniska förutsättningar som inte förändrar tjänsten. Detta eftersom mindre tekniska förutsättningar kan förändra tjänsten.

6.4 Teknisk anslutningsmetod

6.4.1

Om Digg med begreppet *vedertagna standarder och tekniska principer* syftar på tillitsramverket bör det framgå av denna punkt. Vedertagna standarder och tekniska principer är föränderliga och det framgår inte av bestämmelsen varifrån dessa standarder och principer härleds, om det är standarder och principer i en svensk, europeisk eller utomeuropeisk kontext.

6.4.2

”*Anslutningsmetoden ska följa de tekniska integrationsmönstren som specificeras i Tekniska ramverket eller annan anslutningsmetod***.”**

Försäkringskassan behöver ett tydliggörande om formuleringen innebär att integrationer via API/http, Relying Party API – vilket är verkligheten för våra befintliga integrationer – är ett officiellt alternativ?

6.5 Tillgänglighet

6.5.1

Av bestämmelsens utformning får Försäkringskassan intrycket att det finns en direkt koppling mellan leverantör och myndighet, vilket motsäger det som står under punkt 6.8.3 där vi gör tolkningen att Digg öppnar upp för en annan integratör än Digg.

Vad gäller tillgänglighetskraven bör dessa uppgå till 100% och inte 99.9%. Systemet borde byggas så pass robust så att det klarar av fullständig tillgänglighet**.**

6.5.2

Inom ett robust och säkert system bör det inte förekomma några nedtider för tjänsterna överhuvudtaget. Denna skrivning utgör en säkerhetsrisk för en samhällskritisk tjänst. Förslagsvis ska planerade avbrott meddelas mycket tidigare än vad som föreslås, exempelvis minst tre månader i förväg. Försäkringskassan anser att även den maximala nedtiden bör regleras under denna punkt.

6.8 Teknisk integration

6.8.1

Försäkringskassans tolkning är att bestämmelsen beskriver behovet av insamling av bevis vid en incident. Bestämmelsen borde då finnas med i underlaget Bilaga 2 – Incidentrapportering.

6.8.3

Försäkringskassan undrar om denna skrivning innebär att en offentlig aktör skulle kunna ha en annan integratör än Digg? Om så är fallet, hur blir avtalet med integratören kopplat till avtalet med auktorisationssystemet?

8. Incidenthantering och rapportering

Det framgår av bestämmelserna i detta avsnitt att den kommunikation som avses är kommunikation mellan Digg och leverantören. Försäkringskassan anser att det bör beskrivas vad som gäller vid akuta incidenter. Det behöver finnas väl fungerande uppsatta och tydliga processer där Digg, leverantören och förlitande part har kännedom om vad som gäller. Detta bör formuleras som en punkt i avsnittet.

8.1.1

Enligt bestämmelsen ska den leverantör som upptäcker missbruk av dess tjänster skyndsamt stänga av den aktuella tjänsten. Försäkringskassan anser att rekvisitet *skyndsamt* bör ändras till *omedelbart*. Säkerheten i systemet måste upprätthållas genom att leverantörer omgående stänger av tjänster när missbruk upptäcks.

8.1.3

Försäkringskassan anser att en leverantör ska medverka vid utredning av incidenter *i den mån som krävs*, i stället för *i skälig omfattning*.

13. Befrielsegrund

13.2

Försäkringskassan noterar att begreppet *regelverket* saknar en definition.

Bilaga 2 – Incidentrapportering

Av dokumentet framgår att en incidentrapport bland annat ska omfatta uppgift om när *Utfärdaren* upptäckte händelsen. I övrigt används begreppet *Leverantören* i dokumentet. Syftar begreppet *Utfärdaren* på någon annan det någon annan aktör än *Leverantören?*

Försäkringskassan noterar att begreppet *Rapporteringspliktiga säkerhetsincidenter* saknar en definition.

Beslut i detta ärende har fattats av rättschef Marie Axelsson i närvaro av IT-direktör Peter Haglind, verksamhetsutvecklare Azize Cuydur och rättslig expert Marcus Lundén, den senare som föredragande.

Marie Axelsson

Marcus Lundén