Myndigheten för samhällsskydd och beredskap

Remissvar

Datum
2021-03-16

Ärendenr
MSB 2020-16060

Ert datum
2020-12-17

Er referens
I2020/03269

Enheten för säkerhet i cyberfysiska system
Gustav Söderlind
010-240 4257
Gustav.Soderlind@msb.se

Regeringskansliet
Infrastrukturdepartementet
Enheten för samhällets digitalisering
103 33 Stockholm

Remiss av promemorian Auktorisationssystem för elektronisk identifiering och för digital post

Sammanfattning

MSB har inga direkta invändningar mot de förslag som läggs i promemorian men anser att ett antal frågor behöver vidare bearbetas för att kunna uppnå en långsiktigt säker lösning.

Behov av fördjupad analys eller kravställning: digital post

Informationssäkerhetsfrågan får ökad vikt i och med att stor mängd digital post från både offentlig sektor och privata aktörer kommer att aggregeras hos ett fåtal leverantörer vilket gör dessa mer intressanta ur ett antagonistiskt perspektiv och bör föranleda mer stringenta krav på säkerhet hos dessa leverantörer.

Eftersom mängden offentliga aktörer som kommer att kunna skicka digital post via auktorisationssystemet för digital post utökas kommer risken för att skadlig kod överförs till den enskilde via detta medium öka, exempelvis genom missbruk av en ansluten offentlig aktörs system. Detta är ett system som allmänheten har högre tillit till än vanlig e-post. Detta bör föranleda att säkerhetskrav som beaktar denna problematik skall ställas på leverantörer och offentliga aktörer som ansluter till auktorisationssystem (avsändarna).

Det framhålls i promemorian att enligt 5 § förordningen (2018:357) om myndighetsgemensam infrastruktur för säkra elektroniska försändelser får Myndigheten för digital förvaltning (DIGG) meddela de föreskrifter som behövs för inrättande och drift av infrastrukturen, vilket möjliggör reglering av vilken information som får skickas samt vilka krav som skall gälla för avsändarna. Det bör fastställas i denna förordning eller annorstädes att DIGG skall samråda med MSB rörande föreskriftskrav som rör informationssäkerhet.

Vi noterar att det i promemorian anges att "Kivra anser sig inte kunna fortsätta erbjuda tjänster inom Mina meddelanden utan att få ersättning". Detta tydliggör att leverantörer kan komma att dra sig ur auktorisationssystemen, vilket leder till frågeställning rörande de enskilda som använder den digitala brevlådan som ett arkiv för inkommande meddelanden. Det bör framhållas att kravställning på leverantörer bör innehålla krav på system för långtidsbevarande, alternativt krav på att låta den enskilde kunna ta ut informationen i ett format för långtidsförvarande eller för överföring till annan leverantör. Interoperabilitet mellan tjänster för digital post bör vara ett grundläggande krav från offentlig förvaltning när framtida tjänster ansluts.

Vi välkomnar att DIGG i de villkor de ställer vid avtal för "mina meddelanden"[1] tillser att kontroll att parter sköter sina åtaganden kan ske med hjälp av oberoende tredje part.

Behov av fördjupad analys eller kravställning: elektronisk identifiering

Det föreslås att statliga myndigheter som har behov av elektronisk identifiering genom förordning skall vara skyldiga att ansluta sig till auktorisationssystemet. Då det är tillhandahållande myndighet som skall vara ansvarig för kravställning mot leverantörerna i auktorisationssystemet är det av vikt att statliga myndigheter ges möjlighet att löpande föra dialog med tillhandahållande myndighet rörande både initiala säkerhetskrav och behov av förändringar i kravställning för auktorisationssystemet. Vidare bör statliga myndigheter ges möjlighet att avvakta med att ansluta sig tills dess att de – som informationsägare – har bedömt att tillräcklig säkerhet kan garanteras för auktorisationssystemet. Det är varje myndighets eget ansvar att genomföra riskanalyser i syfte att bedöma vilken information som myndigheten skall tillåta respektive inte tillåta vara åtkomlig genom auktorisationssystemet.

MSB noterar att DIGG ställer krav på utfärdare av e-legitimationer genom avtal[2] som refererar exempelvis till "Tillitsramverk för kvalitetsmärket Svensk e-legitimation" där exempelvis anges att "efterlevnad av krav ska under en treårsperiod vara föremål för internrevision av oberoende intern eller extern kontrollfunktion."

Det bör fastställas att tillhandahållande myndighet skall samråda med MSB rörande den kravställning mot leverantörerna som berör informationssäkerhet.

Det bör klargöras om det finns begränsningar i hur statliga myndigheter får använda de system för elektronisk identifiering som inte är anslutna till auktorisationssystemet.

Det bör klargöras vilka ansvarsförhållanden som gäller för; leverantör, tillhandahållande myndighet, offentlig aktör och enskilde då en elektronisk identifiering missbrukas, exempelvis då en e-legitimation utfärdats till bedragare och använts för åtkomst av information hos offentlig aktör.

Det bör klargöras hur en leverantör kan sanktioneras och/eller helt stängas av från medverkan i auktorisationssystem, exempelvis då denna a) ej längre uppfyller säkerhetskraven i auktorisationssystemet eller b) denna utsatts för ett angrepp som omöjliggör tillit till utgivna e-legitimationer eller den tjänst som utger SAML-intyg.

Det bör klargöras - alternativt kravställas – hur och när uppföljning och tillsyn av leverantör skall ske, i syfte att identifiera informationssäkerhetsbrister och andra avvikelser från de krav som ställts för medverkan i auktorisationssystemet.

Det bör klargöras - alternativt kravställas – hur och när leverantör skall rapportera incidenter.

---

[1] https://www.digg.se/digital-post/leverantor/allmanna-villkor
[2] https://www.digg.se/digital-identitet/e-legitimering/offentlig-aktor/nationell-e-legitimering#dokument_och_lankar

MSB vill även understryka behovet av att företrädare för myndigheter ska ha tillgång till en förvaltningsgemensam infrastruktur för elektronisk identifiering som möjliggör för företrädare för myndigheter att i kontakt med medborgare eller vid samverkan med andra organisationer identifiera sig elektroniskt utan att behöva använda sina privata e-legitimationer.

I detta ärende har generaldirektör Camilla Asp beslutat. Gustav Söderlind har varit föredragande. I den slutliga handläggningen har också avdelningschefen Åke Holmgren samt handläggare Carl Önne deltagit.

Camilla Asp

Gustav Söderlind

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984