Säkerhetspolisen

REMISSVAR

Datum: 2022-05-23
Diarienummer: 2022-4247-2
Enhet: Rättsenheten

Mottagare:
Infrastrukturdepartementet
103 33 Stockholm

Referens: I2021/01954

Remissvar Användning av e-legitimation i tjänsten i den offentliga förvaltningen (SOU 2021:62)

Säkerhetspolisen är i huvudsak positiv till utredningens förslag. Säkerhetspolisen har följande synpunkter som främst rör frågor om säkerhetsskydd.

Övergripande synpunkter

Utredningen föreslår att Myndigheten för digital förvaltning (DIGG) ska tillhandahålla en federationslösning för e-legitimationer. Säkerhetspolisen bedömer att det är sannolikt att e-legitimationer som ingår i DIGG:s federationslösning kommer att användas i säkerhetskänslig verksamhet, men inte i informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter (se 2 kap. 1 § säkerhetsskyddsförordningen 2021:955). Om sådana e-legitimationer även kommer att användas i informationssystem som hanterar säkerhetsskyddsklassificerad information behöver säkerhetsskyddsaspekterna på det utredas.

Om e-tjänstelegitimationer som ingår i DIGG:s federationslösning kommer att användas i säkerhetskänslig verksamhet innebär det att bestämmelser om säkerhetsskydd blir tillämpliga. Det innebär t.ex. att om det informationssystem som e-legitimationen ska användas för åtkomst till utgör säkerhetskänslig verksamhet, måste alla delar av funktionen uppfylla det högsta säkerhetsskydd som de anslutna informationssystemen ska ha (4 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd [PMFS 2022:1]). Utredningen går inte närmare in på hur säkerhetsskyddsregelverket kan komma att påverka DIGG:s federationslösning.

Säkerhetspolisen behöver av säkerhetsskäl skydda uppgifter om vissa anställda och uppgifter om vissa tekniska system som används i myndighetens verksamhet. Polismyndigheten har i sitt remissvar anfört att den anser att myndighetens egna e-tjänstelegitimationer av säkerhetsskäl ska undantas från kraven på erkännande och granskning. Polismyndigheten anser vidare, av samma skäl, att myndigheten ska undantas från kraven på erkännande av andras e-tjänstelegitimationer. Även Säkerhetspolisen bör av säkerhetsskäl omfattas av motsvarande undantag samt undantag från kravet på att utfärda e-tjänstelegitimationer.

Utredningen föreslår att DIGG ska samråda med Myndigheten för samhällsskydd och beredskap (MSB) inför utfärdandet av föreskrifter. Med tanke på att e-legitimationer som ingår i federationstjänsten kan komma att användas i säkerhetskänslig verksamhet, och på Säkerhetspolisens uppdrag inom säkerhetsskyddsområdet, bör samråd om föreskrifter även ske med Säkerhetspolisen. Säkerhetsskyddsaspekter kommer att vara viktiga bl.a. vid utformandet av de krav som ska ställas på e-legitimationer som ska ingå i federationslösningen.

9.4.9 Hantering av säkerhetsincidenter

Utredningen föreslår att utfärdare av medel för elektronisk identifiering ska rapportera säkerhetsincidenter till DIGG samt till förlitande parter som påverkas av incidenten. I betänkandet anges att rapporteringsskyldigheten kan sammanfalla med annan rapporteringsskyldighet som följer

av andra författningar. Det bör enligt utredningen poängteras att rapporteringsskyldigheten då ska fullföljas enligt alla de regelverk som en uppkommen incident omfattas av. Säkerhetspolisen bedömer, som tidigare nämnts, att det är sannolikt att e-legitimationer som ingår i DIGG:s federationslösning kommer att användas i säkerhetskänslig verksamhet. Enligt säkerhetsskyddsförordningen ska IT-incidenter anmälas till Säkerhetspolisen och Försvarsmakten. Säkerhetspolisen anser att en incidentrapport i säkerhetskänslig verksamhet endast bör ges in till Säkerhetspolisen och Försvarsmakten. Detta med hänsyn till att uppgifter om IT-incidenter kan vara känsliga ur säkerhetsskyddssynpunkt. Säkerhetspolisen kan därefter informera DIGG, och andra berörda, i nödvändig omfattning.

E-legitimationstjänster kan bli säkerhetskänslig verksamhet

Om flera olika säkerhetskänsliga verksamheter är beroende av samma e-legitimationstjänst, eller ett fåtal tjänster, kan en eller flera e-legitimationstjänster i sig själva bli säkerhetskänslig verksamhet. Även DIGG:s federationstjänst kan komma att utgöra säkerhetskänslig verksamhet. Säkerhetspolisen saknar i betänkandet ett resonemang kring detta. T.ex. kring frågan om DIGG bör ha ett ansvar för att ge en signal om en eller flera e-legitimationstjänster i sig själva är på väg att bli, eller enligt DIGG:s bedömning redan är, säkerhetskänslig verksamhet. Det kan även finnas ett behov av att arbeta preventivt.

Säkerhetskänslig verksamhet och samhällsviktiga tjänster kan inte vara beroende av tjänster som inte fungerar vid en kris, t.ex. om förbindelser med andra länder inte fungerar som de ska. Säkerhetspolisen saknar i betänkandet ett resonemang kring hur rådigheten över federationstjänsten och e-legitimationstjänster ska säkerställas. I sammanhanget kan nämnas att verksamhetsutövaren, beträffande informationssystem som är skyddsvärda utifrån perspektiven riktighet och tillgänglighet, ska ha rutiner och funktioner som krävs för att upprätthålla kontinuitet i den säkerhetskänsliga verksamheten (4 kap. 32 § PMFS 2022:1).

Detta remissyttrande har beslutats av biträdande enhetschefen för rättsenheten Ewa Bokwall. Verksjuristen Ulrika Moberg har varit föredragande.