



REMISSYTTRANDE

2022-05-24

FRA beteckning
3.2:3279/22:2

Infrastrukturdepartementet
Enheten samhällets digitalisering
103 33 Stockholm

Er handläggare

Ert datum

Er beteckning

2022-02-21

I2021/01954

FRA handläggare
Kári Ólafsson

FRA föreg. datum

FRA föreg. beteckning

Utredningen om betrodda tjänsters slutbetänkande ”Användning av e-legitimation i tjänsten i den offentliga förvaltningen” (SOU 2021:62)

Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på förslagen i det remitterade betänkandet.

Synpunkterna nedan följer dispositionen i betänkandet.

9.3 Statliga myndigheter under regeringen ska tillhandahålla e-tjänstelegitimationer till sina anställda (s. 140 ff.)

FRA har inte någon erinran mot förslaget i denna del. Utredningen har inte föreslagit några undantag från regleringen i denna del men anger i betänkandet, s. 142, att det vid en eventuell vidare beredning kan övervägas om det finns anledning att exempelvis undanta försvarsmyndigheterna. Även om FRA inte identifierat någon omedelbart behov av ett undantag vad gäller tillhandahållande av e-tjänstelegitimationer bör frågan utredas vidare.

9.4.5 Ett system för erkännande av e-tjänstelegitimationer (s. 154 ff.)

Även om det i vissa författningar ställs säkerhetskrav för e-tjänster är det, såsom utredningen anger, som huvudregel upp till varje tillhandahållare av en e-tjänst att själv bedöma vilka krav på säkerhet som tjänsten måste leva upp till. Det är en rimlig ordning att statliga myndigheter själva bedömer hur skyddsvärda dess e-tjänster är och att de utifrån den bedömningen avgör vilken tillitsnivå tjänsten ska kräva. Det finns dock en risk att myndigheter inte kommer att göra likvärdiga bedömningar av skyddsbehovet avseende likartad information. Det finns även risk för att myndigheters nättjänster som har samma tillitsnivå kommer omgärdas av olika säkerhetsåtgärder. Regeringen har i sin skrivelse Nationell strategi för samhällets informations- och cybersäkerhet (Skr. 2016/17:213) (regeringens skrivelse) pekat på denna problematik.

I dagsläget bedriver de olika aktörerna i samhället sitt informationssäkerhetsarbete på delvis olika sätt, utifrån olika förutsättningar och behov, baserat på flera olika regelverk och delvis olika uppfattningar om hot och risker. Samma information kan få olika skydd i olika organisationer och kunskapen om vilket skydd som är lämpligt och tillgängligt för en viss typ av information är hos många aktörer ofullständig. När många aktörer är beroende av varandra i sin informationshantering är det också nödvändigt med samordnade åtgärder för att reducera risker och behålla säkerhetsnivån. Aktörer som har en sämre informationssäkerhet kan äventyra säkerheten för övriga. Detta har betydelse för möjligheterna till en digitalt samverkande förvaltning, men även för den återupptagna planeringen för civilt försvar som är beroende av goda förutsättningar att dela känslig information inom statsförvaltningen.¹

Förslagen i nu remitterade betänkande utgör ett exempel på varför det alltså finns ett stort behov av en sådan nationell modell för systematiskt informationssäkerhetsarbete som föreslås i regeringens skrivelse. En sådan modell kan ge en gemensam plattform där regelverk, metoder, verktyg, utbildningar med mera samordnas och samlas. Detta i syfte att riskbedömningar, kartläggningar av skyddsvärda tillgångar och bestämmande av skyddsnivåer med tillhörande säkerhetsåtgärder blir enhetliga mellan olika verksamhetsutövare, så att en likartad och adekvat skyddsnivå uppnås.

¹ Regeringens skrivelse s. 10.

9.5 En samverkande infrastruktur mellan offentlig och privat sektor (s. 171 f.)

FRA instämmer i utredningens bedömning att erkännande av e-tjänstelegitimationer även bör omfatta den privata sektorn. Detta gäller särskilt avseende betalningar, som utgör en central del av statliga myndigheters användning av nättjänster. Enligt FRA:s mening vore det därför önskvärt att banksektorn omfattas av kravet att erkänna e-tjänstelegitimationer i sina nättjänster. I annat fall kommer alla betalningar som genomförs i statlig verksamhet även fortsättningsvis behöva genomföras med privata e-legitimationer.

Allmänt om FRA

FRA är en civil myndighet under Försvarsdepartementet med ca 900 anställda. FRA är en del av svensk underrättelsetjänst med uppgift att bedriva försvarsunderrättelsetjänst till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Inom försvarsunderrättelseverksamheten ska FRA bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning.

FRA bedriver signalspaning i syfte att kartlägga bl.a. yttre militära hot, hot mot svensk personal under internationella insatser, internationell terrorism, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik. All signalspaning är riktad mot utländska förhållanden och sker på uppdrag av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten.

Uppdragsgivarna (regeringen m.fl.) är fortlöpande i behov av underrättelserapportering och signalspaningsverksamheten bidrar kontinuerligt till att skydda Sverige och svenska intressen.

Utöver ovanstående bedriver FRA teknisk informationssäkerhetsverksamhet. FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt hän-

FRA

seende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd.

Uppgifter rörande FRA:s verksamhet omfattas till stora delar av sekretess bl.a. enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400), OSL.²

I detta ärende har biträdande chefsjuristen, tillika tjänsteförättande enhetschefen, Jessica Sjöstrand beslutat. I den slutliga handläggningen har också juristen Kári Ólafsson (Rätts) deltagit, tillika föredragande.

Försvarets radioanstalt

Jessica Sjöstrand

Kári Ólafsson

Sändlista

För kännedom

Försvarsdepartementet/Sund

Försvarsdepartementet/Rättssekretariatet

Internt FRA

GD

ÖD

Chefsjuristen

Biträdande chefsjuristen

C GD:s stab

C KOM

Säkerhetsskyddschefen

AC

² Av 15 kap 2 § OSL framgår att sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.