Beslutsunderlag om ändringar avseende informationssäkerhetskrav i tillitsramverket för Fidus

Förslag till beslut

Projektägaren föreslås besluta

att förändra kravet på federationsoperatörers informationssäkerhetsarbete så att ISO 27000-certifiering inte krävs.

att införa en skyldighet för federationsoperatörer, som inte är statliga myndigheter, att styrka att de uppfyller informationssäkerhetskraven genom oberoende revision eller certifiering.

att införa ett krav på informationssäkerhetsarbete hos organisationer ingående i federationsoperatörens federation.

att införa en skyldighet för federationsoperatörer att tillhandahålla dokumentation som styrker att de ställer krav på informationssäkerhetsarbete för organisationer som ingår federationsoperatörens federation.

Bakgrund

Skolverket har fått i uppdrag att utveckla och tillhandahålla digitaliserade nationella prov- och bedömningsstöd i grundskolan och på gymnasial nivå. Inom ramen för det arbetet har Skolverket driftsatt en provtjänst för digitala nationella prov och bedömningsstöd, bland annat innefattande en plattform för provgenomförande.[1]

Interfederationen Fidus skapades mot bakgrund av att inloggningen till provtjänsten för digitala nationella prov ska vara federerad. Det betyder att inloggningen inte görs i provtjänsten utan inloggningen sker hos varje användarorganisation i en inloggningstjänst i egen eller annans regi. Detta benämns ofta som en federerad inloggning. Användarorganisationernas inloggningstjänst måste i sin tur vara ansluten till en identitetsfederation likt SWAMID eller Skolfederation.

För att möjliggöra för fler federationer att ansluta till Fidus och därmed indirekt att möjliggöra för flera huvudmän att ansluta sig ser Skolverket ett behov av att göra förändringar av tillitsramverket.

Frågeställningar

Informationssäkerhetskrav på federationsoperatörer

Den nuvarande lydelsen för informationssäkerhetskrav i Fidus Deklaration av medlemskap lyder:

2. Federationsoperatören ska antingen:
    a. För federationsverksamhet vid var tid kunna uppvisa ett giltigt certifikat avseende aktuell version av ISO/IEC 27001
        i. *Eller (om statlig myndighet)*
    b. uppfylla kraven i
        i. MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter
        ii. MSBFS 2020:7 Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter.

Certifiering är en process genom vilken en oberoende tredje part bedömer och intygar att till exempel en process eller verksamhet uppfyller specifika krav eller standarder. Certifieringen blir ett enkelt medel för den certifierade att visa att den

[1] Skolverkets provtjänst är en helhetslösning för planering, genomförande och resultathantering för digitala nationella prov och bedömningsstöd. Det är en elektronisk samverkan mellan skolor och Skolverket som består av en säker inloggning, möjlighet till överföring av uppgifter, provgenomförande i en provplattform samt resultathantering.

lever upp till vissa krav, och ett enkelt sätt för andra att försäkra sig om att den certifierade lever upp till en viss kravnivå.

Ett krav i tillitsramverket på certifiering enligt ISO-27000-serien riskerar dock att utestänga organisationer från interfederationen. En organisation kan till exempel inte se något värde i att bli certifierade, men ändå ha ett högkvalitativt informationssäkerhetsarbete. Det är även möjligt att en organisation utgår från en annan standard i sitt informationssäkerhetsarbete, vilket kan försvåra eller förhindra en ISO-certifiering. Relevant för en anslutning till Fidus är inte att federationsoperatören är certifierad, utan att den har ett högkvalitativt informationssäkerhetsarbete.

Att en organisation har ett informationssäkerhetsarbete som uppnår en kvalité som möjliggör att organisationen kan anslutas till Fidus behöver dock säkerställas. Ett alternativ till certifiering är en oberoende revision som syftar till att granska att organisationen som önskar ansluta lever upp till de ställda kraven.

Punkt 2 i medlemskapsdeklaration föreslås därför att ändras till:

2. Federationsoperatören ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna *SS-EN ISO/IEC 27001 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet - Krav* och *SS-EN ISO/IEC 27002 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder* eller motsvarande. Avgränsningen för ledningssystemet ska innefatta åtminstone alla delar i Federationsoperatörens verksamhet som berör dennes medverkan i Fidus. Om federationsoperatören väljer att använda andra standarder än ISO-standarderna ska federationsoperatören analysera och dokumentera de likheter och skillnader som finns mellan ISO-standarderna och valda standarder för att säkerställa att de ger tillräckligt stöd i det systematiska och riskbaserade informationssäkerhetsarbetet.
    a. Om federationsoperatören inte är en statlig myndighet ska federationsoperatören styrka att ett sådant informationssäkerhetsarbete bedrivs genom certifiering eller revision.
    b. Revision av informationssäkerhetsarbetet ska ske i en treårscykel som inleds med en ny- eller omrevision. Övriga år ska federationsoperatören genomgå en uppföljningsrevision.
    c. Revision enligt punkterna 2 a och 2 b ska utföras av en oberoende extern revisor med kompetens inom informationssäkerhet och i enlighet med god revisionssed.

Kravet är formulerat utifrån MSB:s föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter, varför även aktörer som omfattas av de föreskrifterna uppfyller informationssäkerhetskravet för anslutning. Statliga

myndigheter är därför även undantagna från kravet på certifiering eller oberoende revision.

Informationssäkerhetskrav på organisationer ingående i anslutande federation

För att säkerställa en hög gemensam lägstanivå på informationssäkerhetsarbetet inom interfederationen bör det även ställas informationssäkerhetskrav på de organisationer som ingår i federationsoperatörens federation. Samtidigt finns det stora variationer i de anslutande organisationernas resurser och förutsättningar.

Mot bakgrund därav föreslås införandet av ett krav på federationsoperatören att ställa ett bör-krav avseende informationssäkerhet på organisationer som ingår i federationsoperatörens federation:

A. Federationsoperatören ska ställa krav på att de organisationer som är anslutna till Federationsoperatörens federation bör bedriva ett informationssäkerhetsarbete motsvarande följande: Informationssäkerhetsarbetet inom de anslutna organisationernas verksamhet ska ledas, styras, utvärderas och utvecklas med stöd av ett ledningssystem. Till grund för ett sådant arbete kan ledningssystem-standarden ISO/IEC 27001 användas. Kravet på organisationens ledningssystem kan avgränsas till att innefatta alla delar i verksamheten som berör organisations medverkan i federationen.

Kravet är formulerat utifrån det informationssäkerhetskrav som Skolfederationen idag ställer på användarorganisationer i avtalet för medlemskap. Skolfederationen ställer högre krav på informationssäkerhetsarbetet hos tjänsteleverantörer.

För att ett krav på informationssäkerhetsarbete i anslutande organisationer ska kunna införas bör det först utredas om ett sådant krav skulle innebära att någon nuvarande federationsoperatör därmed inte skulle efterleva det förändrade interfederationsramverket.

Förutsättningarna att ställa krav på medlemmar kan skilja sig mellan federationsoperatörer. Statliga myndigheter kan till exempel vara förhindrade att ställa sådana krav till följd av bristande föreskriftsrätt. Undantag till punkt A enligt ovan föreslås därför enligt följande:

B. Federationsoperatörer som är statliga myndigheter undantas från kravet i punkt A. Statliga myndigheter ska istället ställa krav på informationssäkerhetsarbete hos de anslutande organisationerna utifrån vad som är lämpligt med hänsyn till syftet med den statliga myndighetens federation samt den statliga myndighetens uppdrag och verksamhet.
C. Undantag från hela eller delar av kraven i punkt A får med hänsyn till omständigheterna i det enskilda fallet medges av Fidus.

Konsekvenser

Konsekvenser av slopat krav på certifiering

Ett krav på att en organisation ska vara certifierad enligt ISO 27000 innebär inte enbart att organisationen granskas inför att den ska anslutas, utan löpande granskas för att få behålla certifieringen. För att säkerställa att organisationer som inte är certifierade vidmakthåller ett informationssäkerhetsarbete av hög kvalité behövs det även ett krav som syftar till en löpande granskning av dessa. En sådan granskning kan behöva ske av förekommen anledning, men bör även ske med ett visst intervall. Att en granskning sker minst vart fjärde år bedöms som en lämplig avvägning mellan kostnaden för att bli granskad och behovet av att säkerställa kvalitén på informationssäkerhetsarbetet.

För att Fidus ska kunna säkerställa att federationsoperatörer ställer de krav på informationssäkerhetsarbete för anslutande organisationer bör Fidus även ha ett mandat att begära dokumentation som visar på efterlevnad.

Mot den bakgrunden föreslås följande krav införs i medlemskapsdeklarationen.

- Federationsoperatören ska på begäran av Fidus Federationsråd genomgå en oberoende revison som visar att Federationsoperatören bedriver ett informationssäkerhetsarbete i enlighet med punkt 2.
  Federationsoperatören ska minst vart fjärde år genomgå en oberoende revision som visar att federationsoperatören bedriver ett informationssäkerhetsarbete i enlighet med punkt 2.
- Federationsoperatören ska på begäran av Fidus Federationsråd tillhandahålla dokumentation som visar att Federationsoperatören kravställer i enlighet med punkt [*ny punkt om informationssäkerhetskrav på anslutande organisatione*r].

Förslag till diskussionsfrågor utifrån vägval under arbetsprocessen

- Är kravet på att styrka informationssäkerhetsarbetet än rimlig avvägning mellan att kunna säkerställa kvalitén på informationssäkerhetsarbete och att kunna medge organisationer som inte är certifierade medlemskap?
- Är det behövligt att organisationer ingående i federationsoperatörens federation omfattas av informationssäkerhetskrav? Om så är fallet, behöver informationssäkerhetskraven gälla alla användarorganisationer eller endast de användarorganisationer som nyttjar tjänster registrerade i Fidus?
- Utöver att ställa krav på federationsoperatörens informations-säkerhetsarbete, finns det även ett behov av att ställa krav på säkerhetsåtgärder? Så som i MSB:s föreskrifter (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter.

- Bör det ställas olika informationssäkerhetskrav på användarorganisationer och tjänsteleverantörer som ingår i federationsoperatörens federation?
- Det har under arbetet med detta underlag gjorts en initial bedömning att det finnas ett behov av att se över Fidus interfederationsramverk och tillitsdeklarationen som helhet.