# Beslutsunderlag om komplettering av tillits-ramverket för Fidus avseende ömsesidig TLS

## Förslag till beslut

Styrgruppen för Fidus föreslås besluta

att Fidus i sin egenskap av interfederation utökas med funktioner för autentisering med stöd av federerad TLS (FedTLS) för autentisering till provisioneringstjänsten för digitala nationella prov genom smärre korrigering av ramverket.

att anslutningar till provisioneringstjänsten för digitala nationella prov som inte använder federerad TLS, istället ska använda kvalificerade certifikat för webbserverautentisering (QWAC) i enlighet med eIDAS-förordningen[1]. Certifikaten behöver vara försedda med attribut för klientautentisering och innehålla organisationsnummer.

att för mTLS, under en övergångsperiod, även tillåta användningen av historiskt etablerade funktionscertifikat som utfärdats före 2024-07-01 från följande utfärdare:

- SITHS e-id funktionscertifikat (Inera)
- E-identitet för offentlig sektor – EFOS (Försäkringskassan)
- ExpiTrust EID CA V4[9] (tidigare Steria AB e-Tjänstelegitimationer Kort CA v2 hos Expisoft AB)

[1] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG

## Bakgrund

Interfederationen Fidus[2] skapades mot bakgrund av att inloggningen till provtjänsten för digitala nationella prov[3] och bedömningsstöd ska vara federerad. Det betyder att inloggningen inte görs i provtjänsten utan inloggningen sker hos varje användarorganisation i en inloggningstjänst, antingen i egen eller i annans regi. Detta benämns ofta som en federerad inloggning.

Användarorganisationernas inloggningstjänst måste i sin tur vara ansluten till en identitetsfederation likt SWAMID[4] eller Skolfederation[5]. Skolverket såg tidigt behovet av att möjliggöra för alla identitetsfederationer som möter Skolverkets krav på tillit att ansluta sig. I samarbete med Vetenskapsrådet (Sunet) skapades därför interfederationen Fidus där alla identitetsfederationer vars medlemmar vill nyttja Skolverkets tjänster som tillämpar federerad inloggning kan ansluta sig förutsatt att Skolverkets krav på tillit möts.

För att beskriva hur interfederationen Fidus styrs skapades ett interfederations-ramverk med en tillhörande deklaration som är ett avtal med ett antal förpliktelser som en federationsoperatör åtar sig att följa. Tillsammans uttrycker detta Skolverkets krav på tillit för anslutande federationer.

För att säkerställa åtkomst till Skolverkets provisioneringstjänst för digitala nationella prov används ömsesidig transportlagersäkerhet, ofta benämnd mutual TLS[6] vilket ofta förkortas mTLS. mTLS innebär att både huvudmannen och Skolverket autentiserar sig för varandra med certifikat vid anslutningen.

En federerad variant av mTLS har vuxit fram som benämns federerad TLS (Federated TLS Authentication, FedTLS[7]) där Moa[8][9] är ett exempel på praktisk tillämpning av FedTLS. Att använda FedTLS är en naturlig förädling av ursprungsidén med Fidus.

Önskemål har väckts att även använda klassisk certifikatbaserad ömsesidig TLS (mTLS) för åtkomst till provisioneringstjänsten för de organisationer som inte vill eller kan använda federerad TLS.

Frågan som har väckts är om Fidus också kan utgöra grund för tillit till FedTLS och certifikatbaserad ömsesidig TLS (mTLS) vilket kräver en smärre ändring av ramverket för Fidus.

---

[2] https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov/tekniska-forutsattningar-for-digitala-nationella-prov/fidus
[3] https://www.skolverket.se/om-oss/var-verksamhet/skolverkets-prioriterade-omraden/digitalisering/digitala-nationella-prov
[4] https://www.sunet.se/services/identifiering/swamid
[5] https://skolfederation.se/
[6] https://en.wikipedia.org/wiki/Mutual_authentication
[7] https://datatracker.ietf.org/doc/draft-halen-fed-tls-auth/
[8] https://skolfederation.se/nyheter/2022/03/11/kontosynk-blir-moa/
[9] https://wiki.federationer.internetstiftelsen.se/pages/viewpage.action?pageId=20545581

Krav på tillit till inloggningen i provtjänsten regleras i huvudsak av Diggs tillitsramverk för Svensk E-legitimation genom ett antal beslutsunderlag som upprättas. Dessa beslutsunderlag ställer krav på tillitnivå utifrån Diggs tillitsramverk, baserat på regulatoriska krav, informationssäkerhetskrav och verksamhetskrav.

Det finns i nuläget inte något motsvarande beslutsunderlag som ställer krav på tillitsnivå för åtkomst till provisioneringstjänsten.

## Tänkbara certifikat för provisioneringstjänsten

Certifikatbaserad inloggning med korrekt utfärdade certifikat säkerställer korrekt identitet på den som ansluter sig.

Det enklaste sättet att identifiera och autentisera en juridisk person är att uttrycka organisationsnumret i certifikatet. Detta krav kan begränsa antalet möjliga utfärdare då formatet på de standardcertifikat som stämplas ofta är strikt fördefinierat.

Certifikaten för mTLS måste också ha OID: Client Authentication (1.3.6.1.5.5.7.3.2) vilken möjliggör för huvudmännen att autentisera sig med certifikatet.

## Alternativ: Federerad TLS - Certifikat från en federation som ingår i Fidus

För de aktörer som ingår i en federation som medverkar i Fidus interfederation så behövs inte certifikat från externa utgivare. Genom att använda mTLS med federering (FedTLS) och certifikat från aktörerna inom de anslutna federationerna kan autentisering göras inom ramen för Fidus. Det kräver dock att Fidus interfederationsramverk korrigeras något för att inkludera FedTLS för ändamålet. Eftersom alla skolhuvudmän inte är anslutna till en federation inom Fidus så behövs en alternativ lösning i form av mTLS med lämpliga certifikat.

## Alternativ: CA/Browser Forum

Merparten av aktörerna på internet (i form av t.ex. webbläsarleverantörer) litar på de utfärdarorganisationer som ingår i CA/Browser Forum[10] (CAB Forum) genom att dessa organisationer och deras tillhörande rotcertifikat ofta anses betrodda i standardprodukter och tjänster.

För att få vara med i CAB Forum måste organisationen ha genomgått en lyckad revision mot en eller flera av följande standarder:

- WebTrust for CA:s

[10] https://cabforum.org/

- ETSI EN 319 411-1
- ETSI TS 102 042
- ETSI TS 101 456.

En lyckad revision och ett medlemskap ger en objektiv grund för att lita på utfärdaren. För närvarande ingår 55[11] olika utfärdare i organisationen. Försäkringskassans E-identitet för offentlig sektor (EFOS)[12] är betrodda av CAB Forum. Dock får inte Försäkringskassan ställa ut certifikat till andra organisationer än myndigheter vilket gör att skolhuvudmän inte är en målgrupp som kan använda EFOS.

Beroende på vilka kontroller[13] som görs av den utfärdande parten kan certifikaten vara:

- OV – Organization Validated
- DV – Domain Validated
- EV – Extended Validation

En DV-validering är en enklare validering av att domänen är under beställarens kontroll vilken inte är relevant i detta sammanhang.

En OV-validering går något längre, den inkluderar bl.a. kontroll av att beställaren är ett legitimt företag och företagets namn och adress verifieras.

En EV-validering inkluderar flera olika säkerhetskontroller varav den viktigaste är att en verifiering görs av att den som beställer certifikatet är anställd i den aktuella organisationen. Detta är sannolikt den lägsta nivån för att möta Skolverkets krav.

Få medlemmar i CAB Forum ger ut klientcertifikat som inkluderar ett organisationsnummer. Det är också tydligt uttryck att WebPKI-komponenten inte är tänkt för mTLS. Även om kraven och samarbetet i CAB Forum har fokus på servercertifikat är medlemskapet en kvalitetsstämpel för organisationen, vilket är relevant även när de stämplar organisationscertifikat. Att kräva ett medlemskap i CAB Forum kan därför vara ett sätt att bestämma en miniminivå på accepterade utfärdare.

## Alternativ: Qualified website authentication certificate

Kvalificerade certifikat för autentisering av webbplatser (Qualified website authentication certificate, QWAC) är en av flera typer av certifikat som regleras genom eIDAS-förordnignen.

[11] https://cabforum.org/members/
[12] https://www.efos.se/
[13] https://cabforum.org/info-for-consumers/

Trots namnet används QWAC-certifikat inte enbart för serverautentisering. I samband med Europaparlamentets och rådets direktiv (EU) 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden (Payment Services Directive, PSD2) ställs det krav på att använda QWAC-certifikat för kund/klientautentisering via mTLS.

I eIDAS definieras ett *certifikat för autentisering av webbplatser* som ett intyg som gör det möjligt att autentisera en webbplats och koppla webbplatsen till den fysiska eller juridiska person som certifikatet utfärdats för. För att ett certifikat för autentisering av webbplatser ska vara kvalificerat (ett QWAC) ska certifikatet utfärdas av en kvalificerad tillhandahållare av betrodda tjänster (Qualified Trust Service Provider, QTSP) och uppfylla kraven i bilaga IV till förordningen enligt följande:

a) En uppgift, åtminstone i en form som lämpar sig för automatiserad behandling, om att certifikatet har utfärdats som ett kvalificerat certifikat för autentisering av webbplatser.
b) En uppsättning uppgifter som otvetydigt avser den kvalificerade tillhandahållare av betrodda tjänster som utfärdar de kvalificerade certifikaten, inbegripen uppgift om åtminstone vilken medlemsstat tillhandahållaren är etablerad i, samt
   - för juridiska personer: namn och, i tillämpliga fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar,
   - för fysiska personer: personens namn.
c) För fysiska personer: åtminstone namnet på den person som certifikatet utfärdats för eller en pseudonym. Om en pseudonym används ska detta tydligt anges.
   För juridiska personer: åtminstone namnet på den juridiska person som certifikatet utfärdats för och, i förekommande fall, registreringsnummer i enlighet med vad som uppgetts i officiella handlingar.
d) Adressuppgifter, inbegripet åtminstone stad och stat, för den fysiska eller juridiska person som certifikatet utfärdats för och, i förekommande fall, i enlighet med vad som uppgetts i officiella handlingar.
e) Det eller de domännamn som drivs av den fysiska eller juridiska person som certifikatet utfärdats för.
f) Detaljerade uppgifter om när certifikatet börjar respektive upphör att gälla.
g) Certifikatets identifieringskod, som måste vara unik för den kvalificerade tillhandahållaren av betrodda tjänster.
h) Den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln för den kvalificerade tillhandahållare av betrodda tjänster som utfärdar certifikatet.
i) Uppgift om var det certifikat som stöder den avancerade elektroniska underskriften eller den avancerade elektroniska stämpeln som avses i led h finns tillgängligt kostnadsfritt.

j) Uppgift om var de tjänster är lokaliserade som kan användas för att göra förfrågningar om det kvalificerade certifikatets giltighet.

Detta torde vara rimliga krav att ställa utifrån Skolverkets behov. Genom kraven som ställs på utfärdande av QWAC i eIDAS och de standarder som blir tillämpliga genom regleringen (däribland ETSI EN 319 411) har QWAC en tillförlitlighet som minst motsvarar EV-certifikat.

Reglerna och standarderna i eIDAS-ekosystemet leder till att QTSP:er i olika EU-medlemsländer följer samma regler och ramverk. Därigenom har eIDAS skapat väldigt goda förutsättningar för att hänsyn inte ska behöva tas till vilket EU-medlemsland en QTSP är etablerad i när tjänster ska upphandlas. För närvarande är 58[14] organisationer godkända utfärdare av QWAC-certifikat. I skrivande stund finns ingen svensk utfärdarorganisation.

QWAC har ännu inte fått någon stor utbredning i svenska myndighetstjänster, men exempelvis Naturvårdsverket[15] har nyligen lanserat en tjänst som förlitar sig på EU:s trusted lists (medlemsstaternas nationella förteckningar över de företag som i ett land har statusen kvalificerade tillhandahållare av betrodda tjänster) för QWAC.

## Alternativ: Övriga utfärdare

Utfärdare som inte inryms i CAB Forum eller QWAC och som återfinns i myndighetstjänster är exempelvis Expisoft (fd Steria) och SITHS.

Certifikat från Expisoft (fd Steria) har varit en de facto-standard under en lång period för anslutning till myndighets API:er. Detta beror troligen på en kombination av hög tillit och att de erbjuder ”Server-stämpellegitimationer” där organisationsnumret skrivs in i attributet ”Serialnumber”. Det har gjort det enkelt för myndigheterna att identifiera organisationen.

Tilltron till Expisoft vilar i dag på det faktum att certifikaten i så hög grad redan accepteras inom myndighetssfären. Dåvarande Sterias CA (Steria AB EID CA) skapades i enlighet med Statskontorets upphandlade ramavtal ”6678/04” (EID 2004).

Exempel på andra statliga tjänster som uttryckligen kräver Expisoft-certifikat är Statens Personadressregister (SPAR), Spridnings- och hämtningssystemet (SHS), Skatteverket, Försäkringskassan, E-hälsomyndigheten, Bolagsverket med flera.

---

[14] https://eidas.ec.europa.eu/efda/tl-browser/#/screen/search/type/3?searchCriteria=eyJjb3VudHJpZXMiOlsiQVQiLCJCRSIsIkJHIiwiQ1kiLCJDWiIsIkRFIiwiREsiLCJFRSIsIkVMIiwiRVMiLCJGSSIsIkZSIiwiSFIiLCJIVSIsIklFIiwiSVMiLCJJVCIsIkxJIiwiTFQiLCJMVSIsIkxWIiwiTVQiLCJOTCIsIk5PIiwiUEwiLCJQVCIsIlJPIiwiU0UiLCJTSSIsIlNLIiwiVUsiXSwicVNlcnZpY2VUeXBlcyI6WyJRV0FDIl19

[15] https://www.naturvardsverket.se/vagledning-och-stod/avfall-farligt-avfall/rapportera-till-avfallsregistret/rapportera-till-avfallsregistret-via-api/

Vid en genomgång av Expisoft (fd Steria) utfärdarpolicy kan konstateras att de liknar de kontroller som görs vid en EV-validering.

# Frågeställning – val av certifikat för provisioneringstjänsten

Inom ramen för detta underlag har ett flertal olika vägval beskrivits. Nedan motiveras det vägval som ligger till grund för beslutstexten.

## Använda FedTLS – Utökning av Fidus

Med FedTLS löses autentiseringen till provisioneringstjänsten helt inom interfederationen och inga externa leverantörer av certifikat behöver anlitas eftersom certifikat kan utges inom ramen för de federationer som är anslutna till Fidus. För att federerad autentisering ska kunna användas som beskrivet ovan krävs att Fidus interfederationsramverk modifieras något för att tillåta FedTLS.

Den nuvarande lydelsen för interfederationsramverket i Fidus under rubriken Om Fidus lyder:

2. En metadatafil som innehåller:
    a. Tjänster som kan nyttjas av de anslutna federationernas medlemmar (Service Providers – SP)
    b. Metadata om varje enskild medlems inloggningstjänst (Identity Provider – IDP).

Punkt 2 i medlemskapsdeklaration föreslås därför att ändras till:

2. En metadatafil

Ändringen innebär att interfederationen inte begränsas till Service Providers (SP) och Identity Providers (IdP)

Eftersom alla som behöver autentisera sig till provisioneringstjänsten inte är anslutna till en federation inom Fidus så behövs en alternativ lösning i form av mTLS med lämpliga certifikat.

## Kompletterande alternativ 1: Förlita sig på eIDAS-förordningen

En lågt hängande frukt är att inte utöka Fidus ramverk med nya detaljkrav på certifikat utan bara uttrycka att Skolverket följer kraven som följer av eIDAS-förordningen och kan då lita på EU:s trusted lists för QWAC-certifikat.

Utöver exemplet med Naturvårdsverkets avfallregister är det ännu inte utbrett i myndighetssverige att förlita sig på QWAC. Samtidigt är det ett uttryckligt krav för dem som exempelvis berörs av betaltjänstdirektivet att förlita sig på QWAC-certifikat vilket innebär att det inte är obruten mark.

Tillsynsansvaret för betrodda tjänster inom EU regleras inom ramen för eIDAS-förordningen varför Skolverket inte behöver utöva någon egen tillsyn här.

### Kompletterande alternativ 2: Förlita sig på CAB Forum

CAB Forum är huvudsakligen inriktade på serversidan. Alla medlemmar tillhandahåller inte certifikat för mTLS och de är heller inte likformade på samma sätt som QWAC varför detta kan anses vara en mycket riskabel väg att gå.

### Kompletterande alternativ 3: Historiska certifikat

Om Skolverket vill göra som flera andra myndigheter hittills gjort, dvs. att peka ut ett antal utfärdare som de själva anser är betrodda, exempelvis Expisoft (fd Steria) och SITHS, behöver Skolverket ta fram en kravbild som kan motivera valet av dessa, utan att stänga ute leverantörer som kan anses leva upp till objektivt ställda krav. Frågan har ställts till ett antal organisationer hur kravbilden för valet av exempelvis Expisoft (fd Steria) och SITHS utformats, men det har inte resulterat i någon konkret återkoppling. Den 20 år gamla kravställningen från Statskontorets upphandlade ramavtal ”6678/04” är kanske den som lever vidare?

Om det här alternativet väljs måste Skolverket även bestämma hur de utvalda aktörerna revideras och följs upp över tid.

EFOS är en utfärdare som också återfinns i det här sammanhanget men de är betrodda av CAB Forum så de revideras återkommande mot det ramverket. Som tidigare känt kan inte Försäkringskassan utfärda EFOS funktionscertifikat till andra än myndigheter.

Expisoft (fd Steria) och SITHS revideras inte mot något ramverk ur ett mTLS-perspektiv. SITHS revideras däremot mot DIGG:s tillitsramverk för Svensk e-legitimation. SITHS funktionscertifikat får utfärdas till kommuner.

## Konsekvenser

Genom att använda den etablerade interfederationen Fidus även för autentisering av mTLS-anslutningar med FedTLS för provisioneringstjänsten så utnyttjas en befintlig struktur av tillit som innebär att certifikaten kan ges ut av aktörerna i federationerna som ingår i Fidus. Inga kostnader för anskaffning av certifikat från externa leverantörer uppstår. Kraven på aktörerna som ingår i Fidus innebär att ingen ytterligare granskning av säkerhetsnivå eller utformning skulle behövas.

Alternativet till FedTLS som kan användas i andra hand för mTLS innebär att tillit för certifikaten måste säkerställas på annat sätt, men genom att uttrycka att Skolverket följer kraven som följer av eIDAS-förordningen så kan Skolverket då lita på EU:s trusted lists för QWAC-certifikat. Att formulera ytterligare detaljer kring certifikatens säkerhetsnivå och utformning blir inte nödvändigt, utöver att certifikaten ska fungera för klientautentisering och innehålla

organisationsnummer. Formatet för organisationsnummer är standardiserat[16]. De extra attributen i certifikatet som krävs för att använda QWAC-certifikat i PSD2-sammanhang är inte nödvändiga, vilket kan vara värt att påpeka.

Tillsynsansvaret för betrodda tjänster inom EU regleras inom ramen för eIDAS-förordningen varför Skolverket inte behöver utöva någon egen tillsyn här. Den behöriga nationella myndigheten för tillsyn av betrodda tjänster enligt eIDAS är Post- och telestyrelsen.

Genom att välja QWAC för autentisering för mTLS i provisioneringstjänsten kommer Skolverket att använda en lösning med ett befintligt ramverk som stöds av standarder och är regulatoriskt harmoniserad inom EU. Processen för att bli en kvalificerad betrodd utgivare av sådana certifikat är transparent och harmoniseringen innebär att dessa aktörer kan finnas i hela EU och bedriver sin verksamhet på lika villkor.

## Förslag till diskussionsfrågor utifrån vägval under arbetsprocessen

- Hur lång ska en övergångsperiod för historiska certifikat vara?
- 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.

[16] Se ETSI EN 319 412-1