

FAQ - Underskriftstjänsten

Fråga 1: Fråga 1: Behövs det separata stödtjänster per e-tjänst på en och samma organisation?

- Nej, sätt upp en lokal stödtjänst som servrar fler e-tjänster, dock om de ska ha olika "Display Names" så måste detta separeras i olika profiler i stödtjänsten.

Fråga 2: Fråga 2: Kan applikationen (stödtjänsten) köras i container/Docker?

- Ja, det är möjligt.

Fråga 3: Fråga 3: Visst finns det certifikat i lösningen som måste underhållas?

- Ja, på samma sätt som Metadata mellan SP och IdP så finns det certifikat som signerar meddelanden mellan Stödtjänsten och Underskriftstjänsten som måste livscykelhanteras.

Fråga 4: Fråga 4: Finns det fler certifikat än det för Stödtjänsten?

- Ja om man vill ha mTLS-autentisering på API:et mellan e-tjänst och Stödtjänsten så behövs det. Detta rekommenderats för annars så är det fritt fram för de som kan prata med Stödtjänsten och dess API att initiera en signatur.

Fråga 5: Fråga 5: Kommer man behöva någon brandväggsöppning från stödtjänsten till någon tjänst utanför vår organisation?

- Ja, eftersom funktionen för validering av signerade dokument finns i Stödtjänsten så måste den kunna ladda ner CRL-filer från Cn som signerar dokumenten.
- Denna CDP (CRL Distribution point) är publicerad på internet från CGI:s sida och laddas ner via port 80.
- Ingen externt utgående trafik behövs.

Fråga 6: Fråga 6: Vilka andra externa tjänster behöver Stödtjänsten?

- Korrekt tid är ett krav, dvs ni måste se till att Stödtjänstens servrar går korrekt och synkroniserar mot en säker tids-källa (NTP), och att servertiden inte drar sig.
- Kopplingen till en Redis-databas som antingen sätts upp av er själva eller med hjälp av CGI, om ni inte redan har en som kan användas.

Fråga 7: Fråga 7: Hur pratar e-tjänsten med Stödtjänsten?

- Ett SOAP-API över mTLS.

Fråga 8: Fråga 8: Vad är det vanligaste felet som kan uppstå?

- I och med att Google Chrome 80 ändrade säkerheten med kakor så orsakar att e-tjänster tappar användarnas session från det de sänder requesten till den centrala miljön och sedan tar tillbaka den.
- En signatur slutförs inte korrekt om e-tjänsten inte har koll på användarens inloggade session och sedan ger tillbaka den via API:et till stödtjänsten.

Fråga 9: Fråga 9: Vilka miljöer finns det av Underskriftstjänsten?

- Systemtest (SIT) – kan också benämnas bara test, Integration test, dev integrations test osv Funktion är 100% lik produktion, dock ej kapaciteten och klustringen.
- Acceptanstest (AT) – Kan benämnas som stage eller QA eftersom denna är 100% lik produktion i uppbyggnad och kapacitet.
- Produktion (Prod)

Fråga 10: Fråga 10: Går det att skapa organisationsstämplar?

- Nej, enligt eIDAS så är en stämpel kopplad till Juridisk person och Sverige och Sweden connect saknas idag e-legitimations-scheman för eID:n utställda till en juridisk person.
- Tekniskt så skulle tjänsten kunna skapa en organisationsstämpel om det fanns ett eID-schema för juridisk person.
- Tillsvare så skapar tjänsten signaturer utställda till enbart fysiska personer, men eller utan organisationstillhörighet (läs mer om [Underskriftsprofiler](#)).

Fråga 11: Fråga 11: Kan min organisations IdP användas för legitimering för elektronisk underskrift?

- Nej, endast Ineras IdP kan användas i detta syfte. Däremot kan den egna IdP:n användas för autentisering. Se [denna sida](#) för mera information.