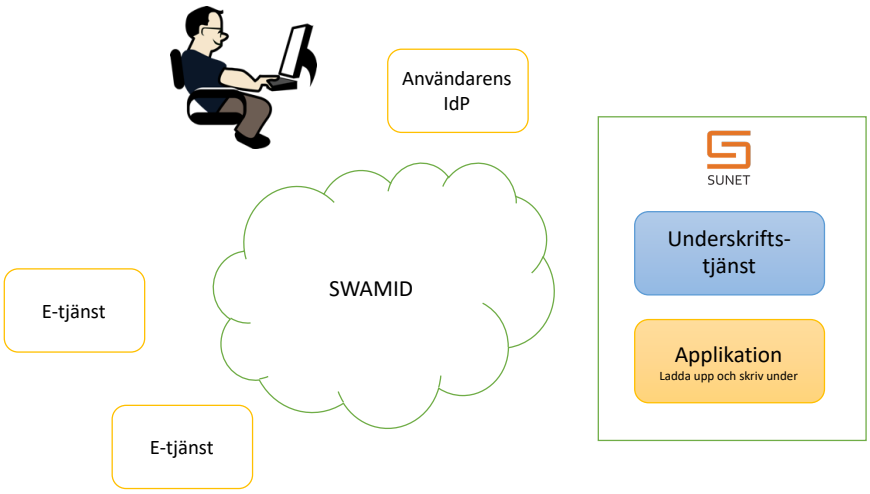
Designbeskrivning
Underskriftstjänst i SWAMID

Bakgrund

Detta dokument beskriver en grundläggande arkitektur för en underskriftstjänst i SWAMID som gör det möjligt för användare som har ett SWAMID eID att kunna skriva under elektroniska dokument. Underskriftstjänsten kan betjäna en eller flera e-tjänster som på ett enkelt sätt kan låta användare skriva under elektroniska handlingar i e-tjänsten. En första e-tjänst för test tillhandahålls av SUNET genom vilken användare kan ladda upp och skriva under valfria dokument.

Grundläggande arkitektur

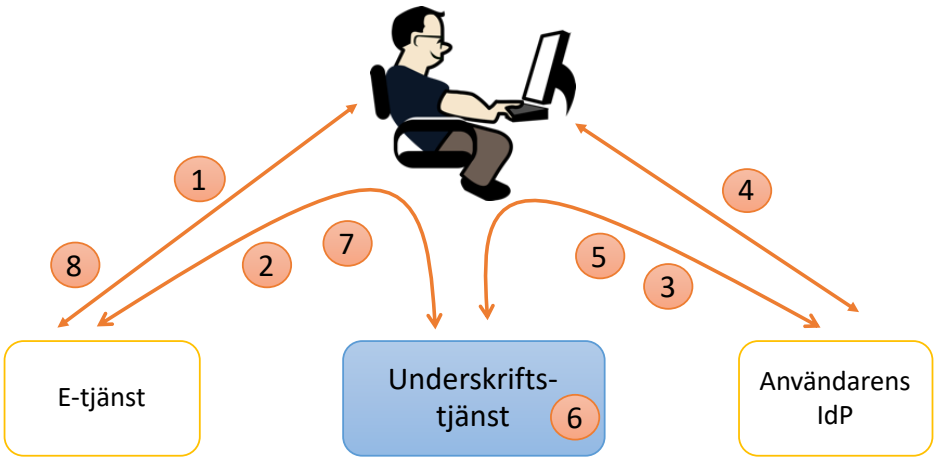


Underskriftstjänsten är en resurstjänst kopplad till SWAMID-federationen som kan nyttjas av e-tjänster enligt ungefär samma principer som när en e-tjänst använder en legitimeringstjänst (IdP) för inloggning enligt följande jämförelse.

- Vid legitimering skickar e-tjänsten användaren till en IdP med en begäran om legitimering (authentication request). Efter fullbordad legitimering återvänder användaren tillbaka till e-tjänsten med ett intyg om styrkt (autentiserad) identitet (authentication response).
- Vid underskrift skickas användaren till underskriftstjänsten med begäran om underskrift (sign request). Vid fullbordad underskrift återvänder användaren till e-tjänsten med en motsvarande sign response som innehåller den de underskrifter som användaren skapat i tjänsten.

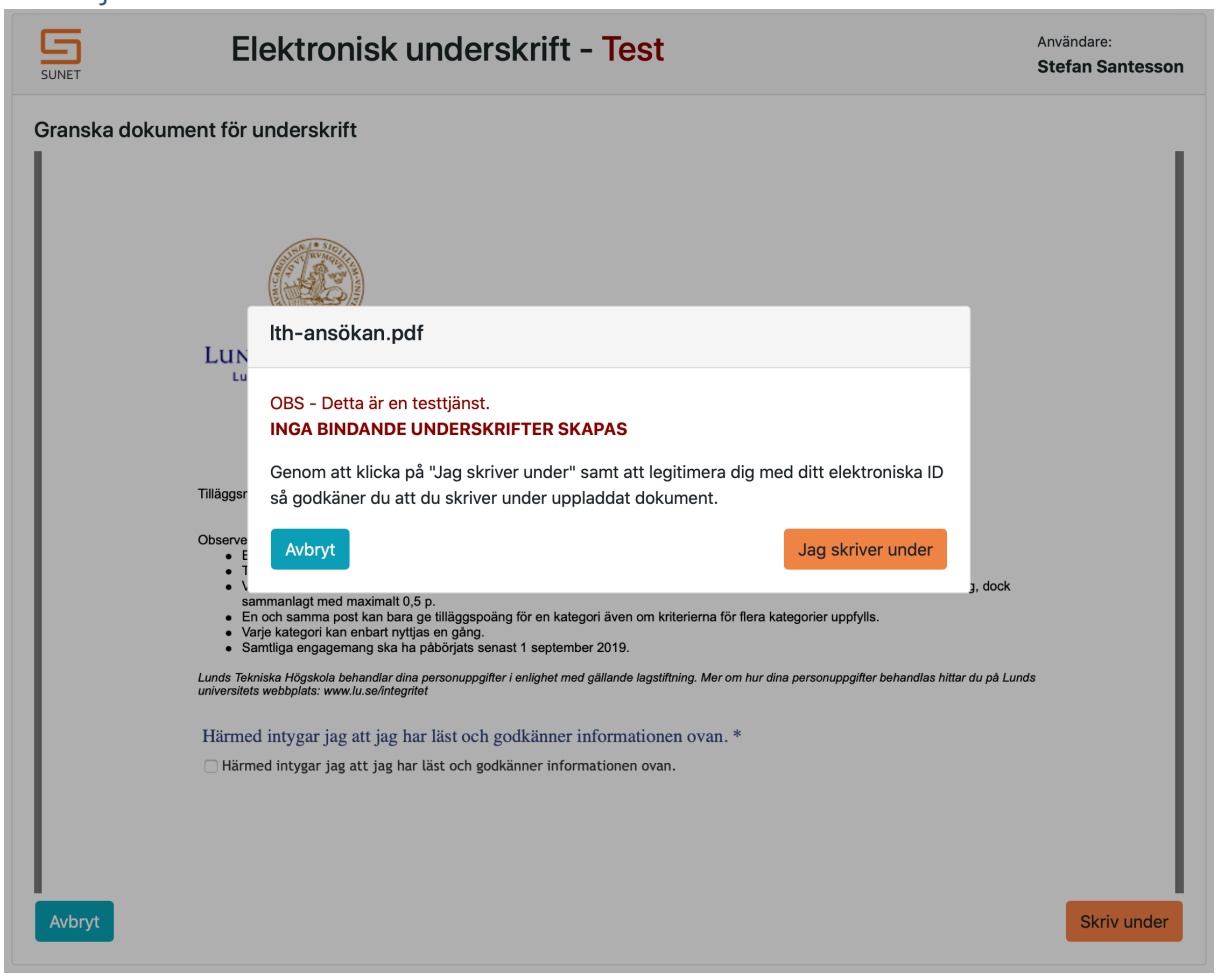
I legitimeringsfallet används protokollet SAML och I underskriftsfallet är protokollet istället DSS från OASIS med tillägg som definieras av Sweden Connect tekniska ramverk.

När väl användaren överförts till underskriftstjänsten med begäran om underskrift legitimeras användaren med lämplig IdP för att godkänna underskriften. Hela processen att skriva under kan därför beskrivas i följande steg:



1. Användaren besöker en e-tjänst och väljer här att skriva under en elektronisk handling.
2. E-tjänsten överför användaren till underskriftstjänsten tillsammans med en sign request som specificerar vad som skall skrivas under och hur.
3. Underskriftstjänsten skickar användaren vidare till sin legitimeringstjänst (IdP) med en SAML request för legitimering.
4. Användaren godkänner underskrift genom att legitimera sig med sitt elektroniska ID mot sin IdP.
5. IdP returnerar användaren till underskriftstjänsten med styrkt identitet i en SAML response.
6. Underskriftstjänsten verifierar användarens identitet samt att alla villkor för underskrift har uppfyllts och skapar därefter användarens underskrift.
7. Användaren returneras till e-tjänsten tillsammans med underskriften.
8. E-tjänsten bekräftar på lämpligt sätt att användaren skrivit under.

Test tjänst



En e-tjänst för test tillhandahålls för att demonstrera underskriftstjänsten för test och för att ge e-tjänster en första möjlighet att testa underskriftstjänsten med enklaste form av integration. Denna tjänst låter användaren ladda upp och skriva under ett PDF eller ett XML dokument. Bilden ovan illustrerar hur användaren godkänner underskrift av uppladdat dokument.

Denna tjänst kan användas för enklaste möjliga integration med en e-tjänst enligt följande principiella upplägg.

1. E-tjänsten tillhandahåller ett dokument som användaren behöver skriva under.
2. Användaren laddar upp dokumentet i test-tjänsten (ovan) och skriver under dokumentet.
3. Användaren laddar upp det underskrivna dokumentet i den första e-tjänsten.

Test-tjänsten är tillgänglig på följande URL: https://sig.idsec.se/sigdemo/secure/main och kräver att användaren loggar in med SWAMID för att kunna ladda upp och skriva under ett dokument.

Dokument för underskrift

Underskriftstjänsten kan skapa underskrifter för XML och PDF dokument. Vid varje underskriftstillfälle kan underskriftstjänsten skapa underskrifter på ett eller flera dokument. Det är e-tjänsten som begär underskrift som i sin underskriftsbegäran (sign request) tillhandahåller underlag för de dokument som skall skrivas under. Dessa underlag innehåller all information som underskriftstjänsten behöver för att skapa underskrifterna men innehåller inte de fullständiga dokument som skall skrivas under. Istället bifogas endast dokumentens sk. ”hash summa” samt övriga parametrar enligt gällande signaturformat som krävs för att skapa underskriften. Detta förfaringssätt medför några viktiga grundläggande egenskaper/fördelar:

- Detta värnar om användarens integritet då den centrala underskriftstjänsten inte har någon kunskap om vad som skrivs under och därmed undviks en stor koncentrationspunkt för lagring av information om vad alla användare skriver under. Detta gör det även lättare för e-tjänster att låta användaren skriva under känslig information och att behålla kontroll över informationsspridning och eventuell radering.
- Protokollet för underskrift blir effektivare då dokumentet som skall skrivas under inte behöver skickas mellan tjänsterna via användarens webbläsare.
- Underskriftstjänsten blir mer generell genom att e-tjänsten behåller kontrollen över den slutliga utformningen av det underskrivna dokumentet. Aspekter såsom exempelvis var en underskrift skall placeras i det underskrivna dokumentet hanteras av e-tjänsten.

Identitet i underskrifter

Undertecknarens identitet i underskrivna dokument styrks av ett underskriftscertifikat. En ny underskriftsnyckel genereras för varje underskriftstillfälle och användarens identitet knyts till den publika verifieringsnyckeln i ett certifikat som även detta utfärdas vid underskriftstillfället. Om mer än ett dokument skrivs under vid samma utskriftsbegäran om underskrift, skrivs samtliga dokument under med samma nyckel och samma certifikat. Efter fullbordad underskrift raderas underskriftsnyckeln som därmed aldrig kan röjas eller komma på avvägar. Vid nästa underskriftstillfälle genereras ny nyckel med nytt certifikat.

Detta upplägg ger ett antal avgörande fördelar jämfört med traditionella underskriftstjänster som återanvänder underskriftsnycklar och certifikat:

- I och med att certifikatet utfärdas vid underskriftstilfället styrks därmed även tidpunkten för underskriften. Detta gör det lättare att bevisa när underskriften utfördes och eliminerar därmed behov av tidsstämpling.
- Underskriftscertifikatet är alltid färskt och är därmed giltigt under den tid som anses lämpligt vid underskriftstillfället.
- Användarens identitet i certifikatet kan anpassas efter behov. Vid varje underskriftstillfälle kan det specificeras vilka av användarens identitetsuppgifter som skall ingå i certifikatet.

- I och med att underskriftsnyckeln raderas och att användarens identitet styrks vid varje underskriftstillfälle, undanröjs i stort sett behovet av spärrtjänster.

Val av legitimeringstjänst och discovery

Det är e-tjänsten som i sign request anger vilken legitimeringstjänst som skall användas av underskriftstjänsten för att styrka användarens identitet och medgivande till underskrift. Tanken är att e-tjänsten i normalfallet redan har legitimerat användaren i e-tjänsten och därmed redan vet vilken IdP användaren valt att legitimera sig med. Genom att e-tjänsten informerar underskriftstjänsten om vilken IdP som skall användas, undviks behovet för användaren att välja IdP i underskriftstjänsten. Detta innebär också att underskriftstjänsten inte behöver integreras mot federationens discovery tjänst.

Om en e-tjänst inte har legitimerat användaren i förväg behöver e-tjänsten först låta användaren välja IdP innan sign request skapas då underskriftstjänsten saknar rutiner för att låta användaren välja IdP.

Säkerhetsnivåer

Underskrift med underskriftstjänst kan skapa såväl avancerade som kvalificerade underskrifter i enlighet med eIDAS förordningen i EU.

För att skapa en kvalificerad underskrift skall underskriftscertifikatet utfärdas som ett kvalificerat certifikat och underskriftsnyckeln skall skyddas i en s.k. kvalificerad enhet för signaturgenerering.

För underskrifter där användarens identitet styrks med SWAMID legitimering kan endast nivån ”avancerad underskrift” enligt eIDAS uppnås. Inom ramen för avancerade underskrifter kan det vidare uppnås olika säkerhetsnivåer vilka främst bestäms av den nivå med vilken användarens identitet styrkts (t.ex. en- eller tvåfaktorsautentisering). Information om säkerhetsnivå vid legitimering lagras i underskriftscertifikatet och därmed styrks underskriftens säkerhetsnivå vid validering av underskriften.

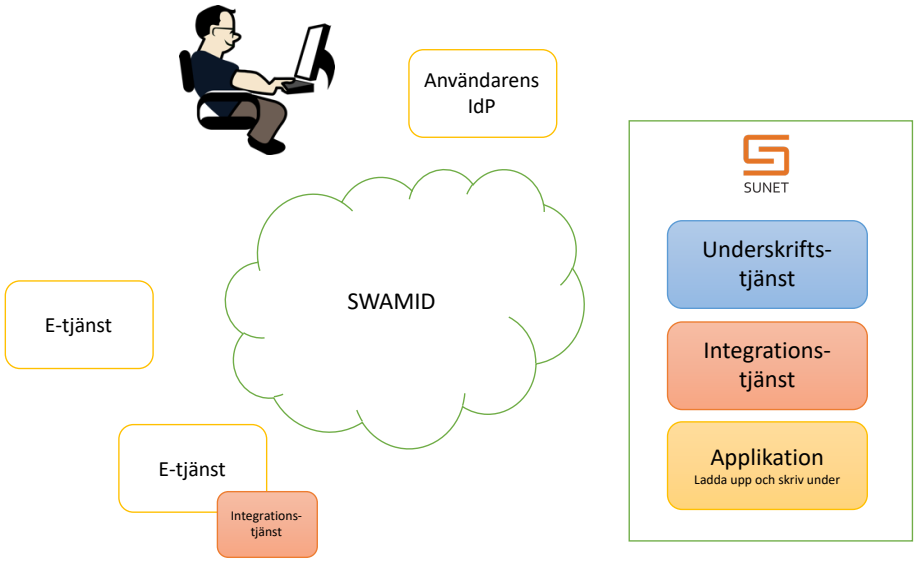
Integrationstjänst

Nästa steg vid integration av e-tjänster med underskriftstjänsten innefattar att e-tjänsten måste kunna skapa en egen sign request för de underskrift av de dokument som användaren skall skriva under i e-tjänsten (ex vid underskrift av ansökan, prov eller liknande). E-tjänsten skall även kunna ta emot och behandla sign response från underskriftstjänsten och använda detta för att foga samman den slutliga underskrivna handlingen.

För att underlätta denna integration används en integrationstjänst som tillhandahåller denna funktionalitet till e-tjänster via ett enkelt och funktionellt API.

Integrationstjänsten kan tillhandahållas på 3 huvudsakliga sätt:

- Som en molntjänst hos SUNET.
- Som en lokal tjänst som driftsätts i e-tjänstens egna IT-miljö
- Som ett java bibliotek med JAVA – API



Fördelen med en molntjänst är att det medger enklare integration för e-tjänsten, men nackdelen är en lägre grad av säkerhet och exponering av information då dokument som skall skrivas under måste delas med integrationstjänsten.

I testinfrastrukturen för underskrift kommer SUNET i nästa stega att tillhandahålla en molntjänst för integration med underskriftstjänsten.