

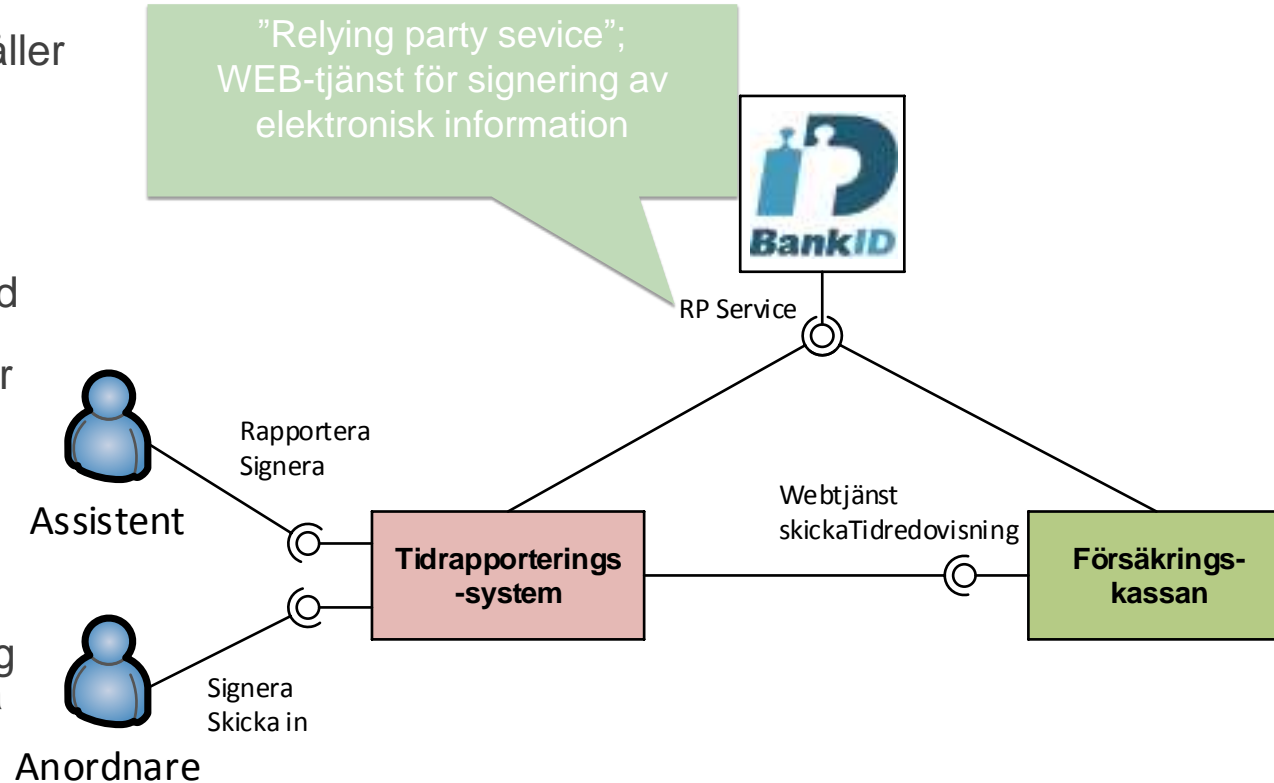
Nytt IT-stöd Assistansersättning

Elektronisk tidredovisning

Presentation av gränssnitt mot tidrapporteringsystem

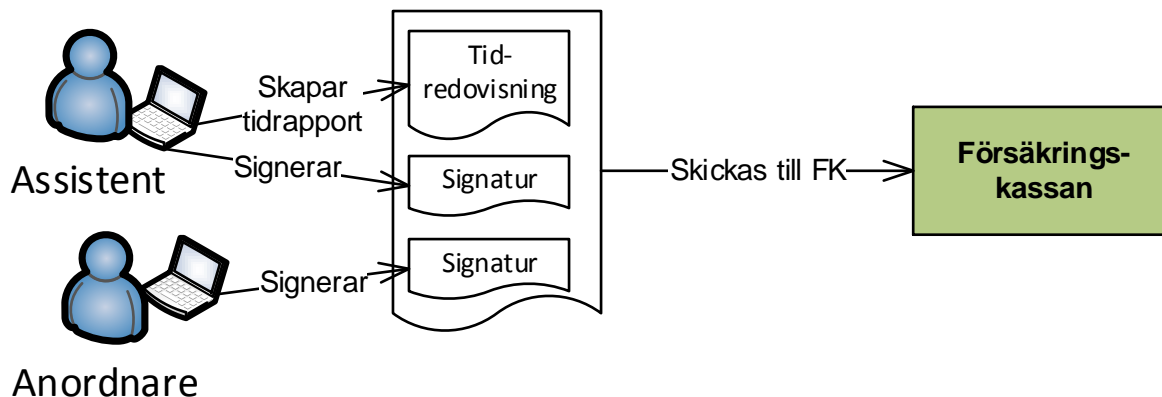
Tekniskt gränssnitt för tidredovisning

- Försäkringskassan tillhandhåller ett Webtjänstegränssnitt (SOAP) för att ta emot signerade Tidredovisningar "skickaTidredovising"
- Webtjänst sker över TLS med certifikat utställt av Försäkringskassan MCA eller Steria.
- Lösningen baseras på PKI signering för att skydda informationens integritet
- BankID används för signering av Tidredovisningar i externa tidrapporteringsystem.



Signering av tidredovisning

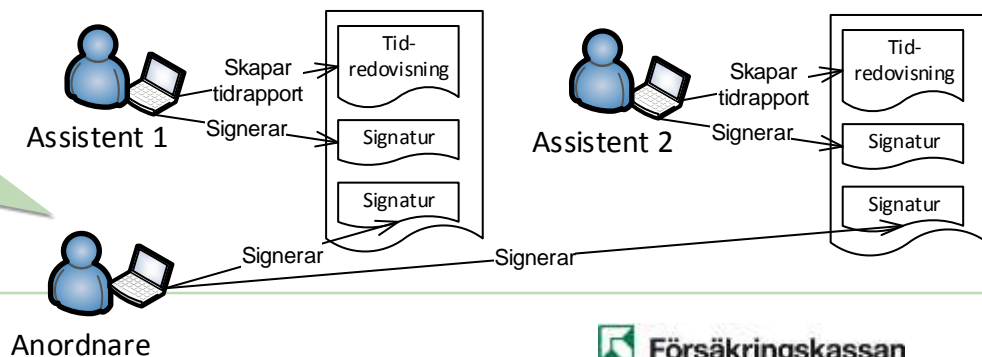
- Varje tidsrapport signeras av assistent och anordnare med BankID eller Mobilt BankID
- Format på tidredovisning / SOAP-meddelanden specificeras i XML-Schema av Försäkringskassan
- Försäkringskassan kommer att utföra kontroller av signaturer samt formatkontroll av innehåll. Felmeddelanden kommer att returneras och anropet kan komma att avvisas vid avvikelser



Anordnares multipla signatur

- Anordnaren tillåts signera flera tidredovisningar med en och samma signatur. Detta möjliggörs genom att inkludera informationen från alla de tidredovisningar som skall signeras i form av listor. Signaturen kopieras sedan in i alla tidredovisningar som avses med signaturen.
- Detta betyder att för en specifik tidredovisning kommer checksummor för alla tidredovisningar som signerades samtidigt att finnas med.

Anordnare kan signera flera tidredovisningar samtidigt genom att inkludera alla rapporternas checksummor i samma signatur och bifoga den i alla inskickade meddelanden



Signaturprocedur

- Tidrapporteringsystemen behöver använda den av BankID rekommenderade signeringsproceduren "Method Sign".
Proceduren är enligt följande:
 1. Presentera dokumentet som skall signeras för användaren.
 2. Beräkna en checksumma av en binär representation av dokumentet.
 3. Skapa en översikt av dokumentet.
 4. Använd "Method Sign" med "userVisibleData" satt till översikten av dokumentet och "nonUserVisibleData" satt till den beräknade checksumman.

Se "*BankID Relying Party Guidline*" för mera detaljer kring BankIDs webbtjänstegränssnitt:
<https://www.bankid.com/assets/bankid/rp/bankid-relying-party-guidelines-v2.10.pdf>

Använd BankIDs "MethodSign" för signering

- "MethodSign" baseras på kryptering av en för den som signerar synlig informationsdel, och en del som inte visas för den som signerar, `userVisibleData` och `userNonVisibleData`.
- Utifrån resultatet från signeringen är det två parametrar vi är intresserade av för att kunna verifiera signaturer:
 - "signature" XML-signaturen
 - "ocspResponse" OCSP-svaret som är kopplat till signaturen.

Tillämpning av BankIDs "Method Sign"

- Då dokumentet som skall signeras är en XML-struktur så anses "checksumma av en binär representation" avse en checksumma av en kanonisk form av den avsedda XML-strukturen enligt c14n-specifikationen.
Följande version skall användas:
Canonicalizer.ALGO_ID_C14N_EXCL_WITH_COMMENTS
- `userVisibleData` är en översikt av det dokument som skall signeras och innehåller tillräcklig information för att det ska vara uppenbart vilket dokument som signeras.
- `userNonVisibleData` innehåller ovan nämnda checksumma för att garantera dokumentets integritet efter signering.

Assistentens signatur

Assistenten behöver signera varje enskild tidsredovisning och följande information signeras i samband med detta:

- **userVisibleData:**

Jag intygar idag <år-månad-dag> klockan: <timmar : minuter> att uppgifterna om utförd assistans för <Personens namn och personnummer> under tiden < år-månad-dag> till <år-månad-dag> om totalt: <timmar:minuter aktiv tid> aktiv tid, <timmar:minuter väntetid> väntetid och <timmar:minuter beredskapstid> beredskapstid är riktiga.

- **userNonVisibleData:**

<TidrapportID>,<SHA-256 checksumma>

UUID enligt schema
tidredovisning_extern_v1.xsd

Checksumma av den
c14n formaterade
tidredovisningen

Anordnarens signatur

- **userVisibleData**

Jag intygar idag <år-månad-dag> klockan: <timmar : minuter> att alla uppgifterna i följande tidredovisningar om utförd assistans är riktiga:

Assistenten <Asistentens namn och personnummer> för <Personens namn och personnummer> under tiden < år-månad-dag> till <år-månad-dag> om totalt: <timmar:minuter aktiv tid> aktiv tid, <timmar:minuter väntetid> väntetid och <timmar:minuter beredskapstid> beredskapstid.

Assistenten <Asistentens namn och personnummer> för <Personens namn och personnummer> under tiden < år-månad-dag> till <år-månad-dag> om totalt: <timmar:minuter aktiv tid> aktiv tid, <timmar:minuter väntetid> väntetid och <timmar:minuter beredskapstid> beredskapstid.

- **userNonVisibleData**

<TidrapportID>,<SHA-256 checksumma>;
<TidrapportID>,<SHA-256 checksumma>

Lista med tidrapportID och checksummeapar.

Webtjänst ”skickaTidredovisning”

Tjänsteanropet innehåller 5 delar. De 4 nedersta erhålls vid anrop till signeringstjänsten mot BankID.

- Tidredovisning i XML format enligt XML-Schema
- Assistentens signatur
- OCSP-svaret som hör till assistentens signatur
- Anordnarens signatur
- OCSP-svaret som hör till anordnarens signatur

Den information som ska signeras. Måste vara i exakt det format som den var när den signerades

De fem delarna i anropet har typen `xmlmime base64Binary`. UTF-8 skall användas som teckenencoding för Tidredovisnings. För övriga skickas svaret från BankID som det är

Webtjänst ”skickaTidredovisningResponse”

Tjänsteresponsen

- Transaktions ID
- Felhantering via SOAP fault med två typer av felmeddelanden:
 - ”XmlValidationError”: Vid fel i tidrapporten.
 - ”signatureValidationError: Vid fel i signaturen.

Transaktions ID kan vara bra att logga för att använda i felsöknings syfte. FK kan med hjälp av detta söka rätt på tidredovisningar mottagna i transaktionen

Specifikationer för Webtjänst

- Schema för Tidredovisningen
 - tidredovisning_extern_v1.xsd
- Tjänsten skickaTidredovisning
 - SkickaTidrapportInteraction_1.0_shsbp10.wsdl
 - SkickaTidrapportResponder_1.0.xsd
 - xmlmime.xsd