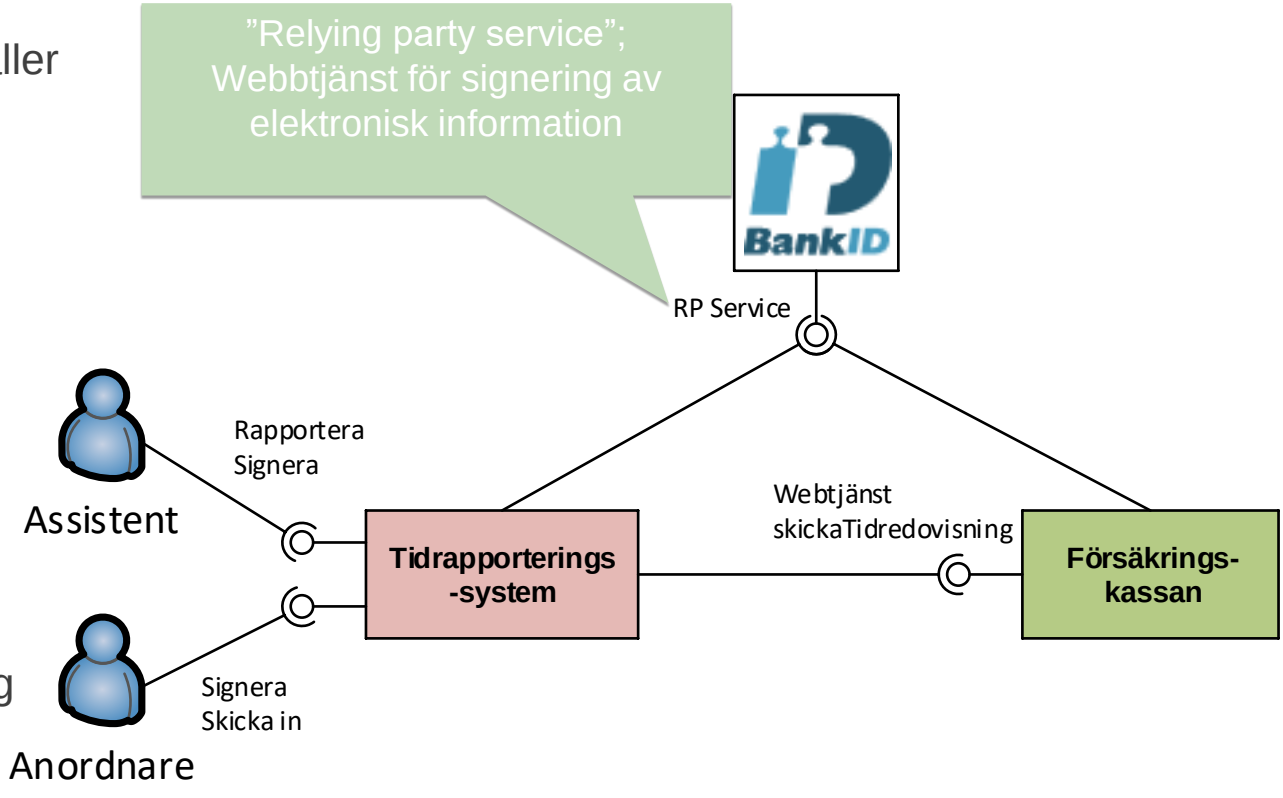
Elektronisk tidredovisning

Presentation av gränssnitt mot tidrapporteringssystem

Tekniskt gränssnitt för tidredovisning

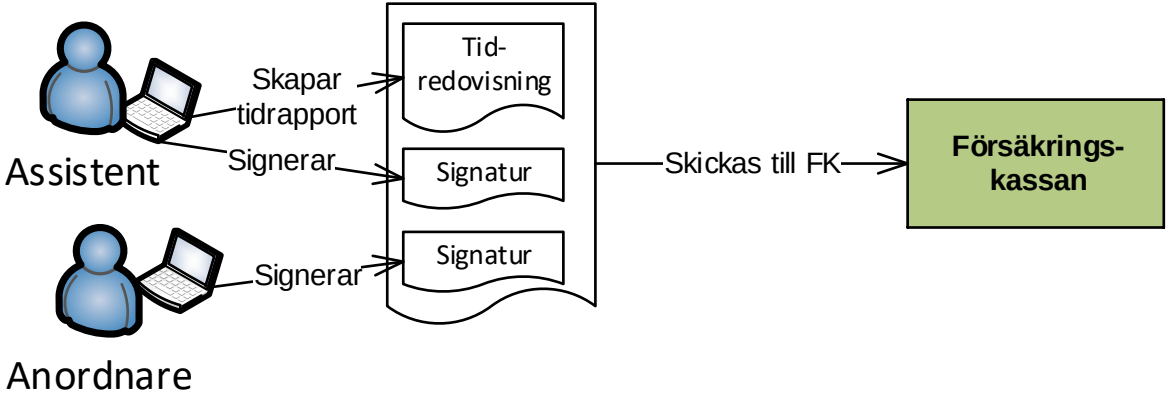
- Försäkringskassan tillhandhåller ett webbtjänstegränssnitt (SOAP) för att ta emot signerade tidredovisningar ”skickaTidredovisning”
- Webbtjänsten sker över TLS med certifikat.
- Lösningen baseras på PKI-signering för att skydda informationens integritet.
- Bank-id används för signering av tidredovisningar i externa tidrapporteringssystem.



Försäkringskassan

Signering av tidredovisning

- Varje tidrapport signeras av assistent och anordnare med bank-id eller mobilt bank-id.
- 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.

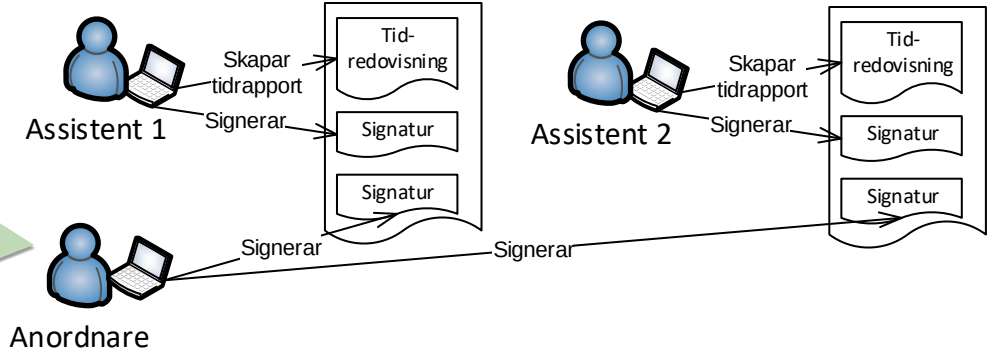


Försäkringskassan

Anordnares multipla signatur

- Anordnaren tillåts signera flera tidredovisningar med en och samma signatur. Detta möjliggörs genom att inkludera informationen från alla de tidredovisningar som ska 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



Försäkringskassan

Signaturprocedur

- Tidrapporteringssystemen behöver använda den av BankID rekommenderade signeringsproceduren ”Method Sign”. Proceduren är enligt följande:

1. Presentera dokumentet som ska 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.

”MethodSign”

Använd BankID:s ”MethodSign” för signering.

- ”MethodSign” baseras på kryptering av en för den som signerar synlig informationsdel, userVisibleData, och en del som inte visas för den som signerar, 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”

- Eftersom dokumentet som ska 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 ska användas:
  Canonicalizer.ALGO_ID_C14N_EXCL_WITH_COMMENTS
- userVisibleData är en översikt av det dokument som ska 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 tidredovisning 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 <Assistentens 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 <Assistentens 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 checksummepar.

Webtjänst ”skickaTidredovisning”

Tjänsteanropet innehåller fem delar. De fyra 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. Den måste vara i exakt det format som den var när den signerades.

De fem delarna i anropet har typen xmlmime base64Binary.
UTF-8 ska användas som tecken-encoding för tidredovisning. För övriga skickas svaret från BankId som det är.

Webbtjänst ”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. Försäkringskassan kan med hjälp av detta söka rätt på tidredovisningar mottagna i transaktionen.

Specifikationer för webbtjänst

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