25.11.2022

OP tjänsten för förmedling av identifiering

Innehåll

25.11.2022

1 Allmän beskrivning

Du kan använda OP Tjänsten för förmedling av identifiering för stark autentisering i din nättjänst eller applikation. Hos OP får du identifieringsverktyg för stark autentisering i olika identifieringstjänster med ett enda avtal och en enda teknisk integration.

Tjänsten är en del av det nationella förtroendenätet, som består av leverantörer av Identifieringstjänster som ger ut identifieringsverktyg för stark autentisering samt leverantörer av tjänster för identifieringsförmedling. OP är en leverantör av en tjänst för förmedling av identifiering i Förtroendenätet.

Lägg till en länk till OP Tjänsten för förmedling av identifiering i din elektroniska tjänst. Länken måste byggas upp med ett OIDC-gränssnittsanrop i enlighet med integrationsinstruktionerna.

Den som använder den elektroniska tjänsten klickar på knappen till den valda identifieringstjänsten. Till buds står de identifieringstjänster som ingår i Förtroendenätet och som beskrivs på sidan om OP Tjänsten för förmedling av identifiering på op.fi.

Identifieringen sker i den identifieringstjänst som användaren har valt och som omdirigerar användaren tillbaka till förmedlingstjänsten.

Förmedlingstjänsten omdirigerar användaren från identifieringstjänsten tillbaka till den elektroniska tjänsten.

Den identifierade användarens identifieringsuppgifter förmedlas till den elektroniska tjänsten. Om ett fel inträffar, förmedlas en uppgift om felet.

I tjänsterna och gränssnitten iakttar vi Traficoms föreskrift 72b om elektroniska identifieringstjänster och betrodda elektroniska tjänster. Detaljerna i föreskriften https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/reglering-och-tillsyn/elektronisk-identifiering.

OP Tjänsten för förmedling av identifiering baserar sig på OIDC-specifikationer (OpenID Connect). Vi behandlar endast finländska identifieringsverktyg i tjänsten. En identifieringstransaktion som innehåller icke-obligatoriska attribut behandlas som om den inte innehöll sådana. De icke-obligatoriska attributen räknas upp i Traficoms föreskrift.

För att kunna använda OP Tjänsten för förmedling av identifiering måste du ingå ett avtal om tjänsten med andelsbanken och godkänna användarvillkoren. Du kan börja använda förmedlingstjänsten när du har ingått avtalet. Tjänsten ska tas i bruk i enlighet med den här tjänstebeskrivningen.

2 Krav på programvara

2.1 Användargränssnitt

Du kan integrera OP Tjänsten för förmedling av identifiering i din elektroniska tjänst på två olika sätt.

1) Användargränssnitt som tillhandahålls av OP

Lägg i din elektroniska tjänst till en länk som gör ett OIDC-gränssnittsanrop och dirigerar användaren till det webbläsarbaserade responsiva användargränssnitt som OP tillhandahåller. Användargränssnittet kan användas på svenska, finska och engelska. Användaren väljer en identifieringstjänst. Från den omdirigeras användaren identifierad tillbaka till den elektroniska tjänsten. Om ett fel inträffar i identifieringstjänsten, dirigeras användaren tillbaka till OP:s användargränssnitt.

I förmedlingstjänsten är det också möjligt att visa en vy där användaren kan kontrollera sina personuppgifter innan användaren dirigeras tillbaka till den elektroniska tjänsten.

2) Användargränssnitt inbäddat i den elektroniska tjänsten

Den elektroniska tjänsten gör ett OIDC-gränssnittsanrop. Som svar sänder OP Tjänsten för förmedling av identifiering identifieringsknapparna (länkar och bilder) till identifieringstjänsterna, som den elektroniska tjänsten bäddar in i sitt användargränssnitt. Om ett fel inträffar i identifieringstjänsten, dirigeras användaren tillbaka till den elektroniska tjänstens användargränssnitt.

När en elektronisk tjänst konstruerar ett inbäddat användargränssnitt ska den uppge att tjänsten för förmedling av identifiering tillhandahålls av OP. Kunden ska också informeras om att personbeteckningen och namnet förmedlas till tjänsteleverantören vid identifieringen. Dessutom ska det läggas till en länk till dataskyddsbeskrivningen för tjänsten för förmedling av identifiering. Alla de här uppgifterna kommer också från gränssnittet.

Uppgifterna ska anges i följande form i den elektroniska tjänsten:

Vid identifieringen förmedlas följande uppgifter till tjänsteleverantören: personbeteckning, namn. **Dataskyddsbeskrivning** OP Tjänsten för förmedling av identifiering tillhandahålls av OP Gruppens andelsbanker och OP Företagsbanken Abp.

Hyperlänk till dataskyddsbeskrivningen: https://isb.op.fi/privacy-info?lang=fi. Språkkoder som stöds: sv, fi och en.

2.2 Webbläsare som stöds

OP Tjänsten för förmedling av identifiering fungerar med alla de vanligaste webbläsarna. Vi rekommenderar att du använder de senaste versionerna av webbläsarna. För att fungera kräver tjänsten att du tillåter sessionscookies (http session cookies) och JavaScript i webbläsaren.

OP:s användargränssnitt har byggts upp så att det är tillgängligt för så många kunder som möjligt, bland annat med hjälp av assisterande teknik.

Information om webbläsare som stöds och anvisningar om användningen av cookies och JavaScript finns på op.fi, på sidan Användningen av nättjänster.

3 Avtal

Då du avtalar om användning av OP Tjänsten för förmedling av identifiering ska du välja för vilket ändamål du kommer att använda stark autentisering. Utöver för identifiering kan

tjänsten användas för att sammankoppla identifikatorer, det vill säga antingen för att bevilja identifikatorer för stark autentisering (tillgängliga endast för medlemmar i Förtroendenätet) eller för att bevilja egna identifikatorer för svag autentisering i den elektroniska tjänsten. De här tre användningsändamålen behandlas i den här beskrivningen som avtalstyper: identifiering, sammankoppling av identifikatorer för stark autentisering och sammankoppling av identifikatorer för svag autentisering.

3.1 Avtalsändringar

Följande ändringar kräver en avtalsändring. Om du vill:

- lägga till eller ta bort en sammankoppling av identifikatorer för stark autentisering eller en sammankoppling av identifikatorer för svag autentisering.
- lägga till en begränsning för identifieringsverktyg.
- ta bort en begränsning för identifieringsverktyg.

Vi meddelar i op.fi om i OP Tjänsten för förmedling av identifiering tas med nya leverantörer av stark autentisering.

4 Steg vid ibruktagandet

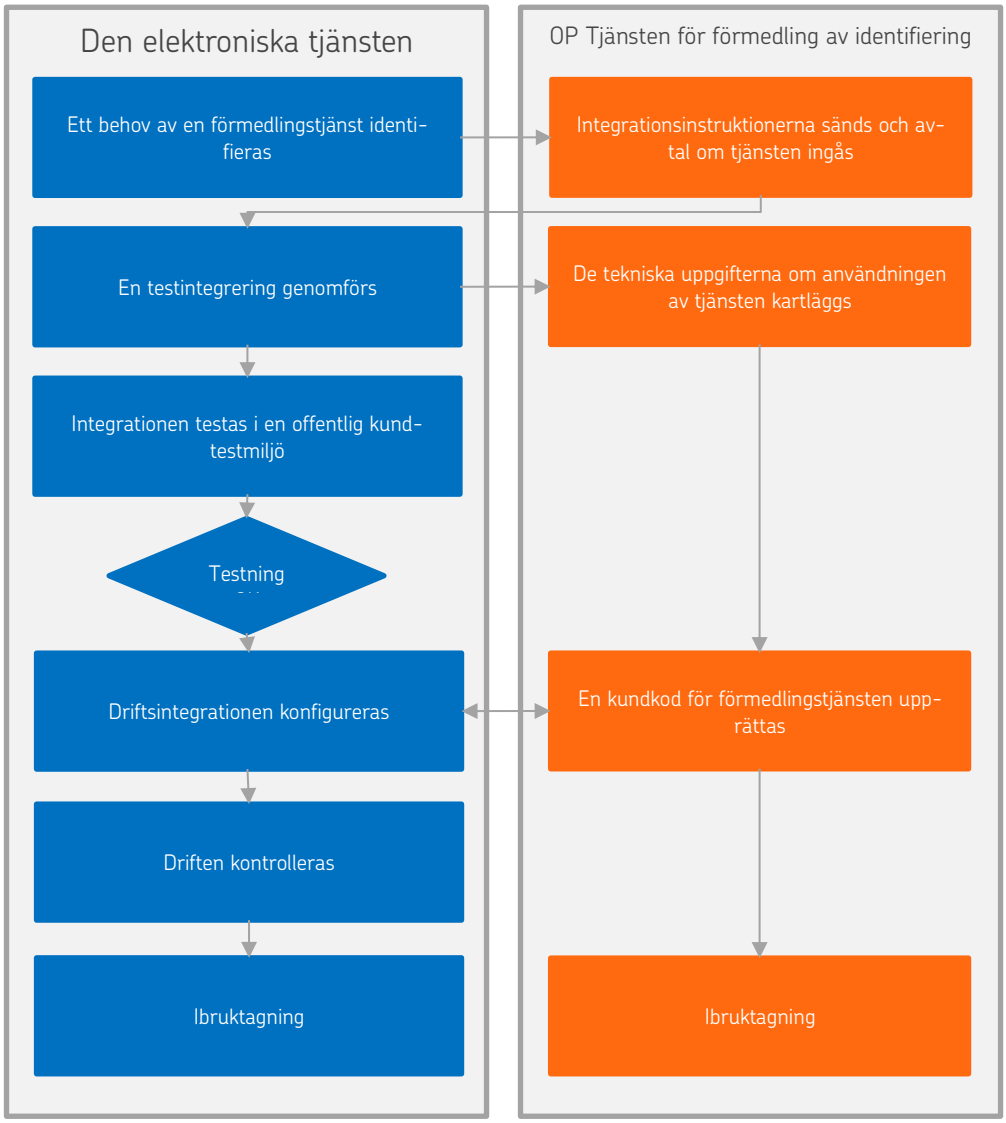
Integrera den elektroniska tjänsten och OP Tjänsten för förmedling av identifiering i enlighet med de offentliga integrationsanvisningarna. Innan du inleder integreringen rekommenderar vi att du kontaktar andelsbanken för att ingå ett avtal.

Du kan testa integrationen mellan den elektroniska tjänsten och OP Tjänsten för förmedling av identifiering i en offentlig kundtestmiljö (Sandbox), där alla elektroniska tjänster kan integreras med samma offentliga testidentifikator.

Ingå ett avtal om användning av tjänsten innan den sätts i drift. Vi kartlägger de tekniska uppgifterna om användningen av tjänsten och ger den elektroniska tjänsten en kundkod (Client ID), med vilken den elektroniska tjänsten identifieras i gränssnittsanrop vid integreringen.

En mer detaljerad gränssnittsbeskrivning med exempel finns under OP Developer: https://github.com/op-developer/Identity-Service-Broker-API

25.11.2022



4.1 Lämnande av tekniska uppgifter

För ibruktagningen behöver vi följande uppgifter:

- Företagets namn
- Företagets FO-nummer
- OpenID entity statement
- Som ytterligare information behöver vi valbara andra namn som kan användas om tjänsten (SP name i den tekniska beskrivningen)

Meddela oss e-postadressen till en kontaktperson för den elektroniska tjänsten, så att vi kan sända blanketten för lämnande av uppgifter till kontaktpersonen. Vi sänder blanketten i ett krypterat e-postmeddelande. Den elektroniskt ifyllda blanketten ska returneras genom att svara på det krypterade e-postmeddelandet.

Samtidigt ger vi den elektroniska tjänstens kundkod (Client ID) till kontaktpersonen. Med kundkoden identifieras den elektroniska tjänsten i gränssnittsanrop vid integreringen.

4.2 Byte av krypteringsnycklar

OP Tjänsten för förmedling av identifiering byter regelbundet gränssnittets krypterings-nycklar. Den elektroniska tjänsten får de gällande krypteringsnycklarna automatiskt från gränssnittet signed_jwks, och det ska kontrolleras minst en gång per dygn. Vid kontrollen ska den elektroniska tjänsten också kontrollera TLS-certifikatet för OP Tjänsten för för-medling av identifiering och underskriften i gränssnittet signed_jwks.

Den elektroniska tjänstens egna OICD-nycklar ska bytas regelbundet, nycklarna på med-delandenivå minst vartannat år. OP Tjänsten för förmedling av identifiering får automatiskt de gällande krypteringsnycklarna från den elektroniska tjänstens gränssnitt signed_jwks. Då en gammal nyckel tas ur bruk, ska den först tas bort från den elektroniska tjänstens gräns-snitt signed_jwks minst ett dygn innan nyckeln slutar fungera.

Ditt företag bär ansvaret för att följa upp giltigheten för den elektroniska tjänstens TLS-certifikat och att förnya certifikatet i tid. Den rekommenderade giltighetstiden för certifikatet är ett år, och ditt företag ansvarar för att förnya det. Certifikatet ska vara utfärdat av en allmänt tillförlitlig leverantör av certifikatstjänster.

4.3 Testning av Tjänsten för förmedling av identifiering

Du kan först testa integrationen mellan OP Tjänsten för förmedling av identifiering och den elektroniska tjänsten i en offentlig kundtestmiljö (Sandbox). Identifieringstjänsternas test-miljöer har integrerats i kundtestmiljön, och det går inte att identifiera sig med riktiga iden-tifieringsverktyg i den.

4.4 Kontroll av driften

Då driften sätts igång ska integrationens funktion kontrolleras i driftsmiljön med riktiga identifieringstjänster och identifieringsverktyg.

5 Kontaktinformation

Kontaktinformation för OP Tjänsten för förmedling av identifiering:

- Företags- och betalningsrörelsetjänster 0100 05151 eller
- e-post verkkopainikkeet@op.fi

I avtalsärenden kontakta din andelsbank.

Om ditt företags kontaktpersoner eller uppgifter ändras, ska du anmäla ändringarna till OP:s kontaktperson.