TJÄNSTEBESKRIVNING FÖR IDENTIFIERINGSTJÄNST OIDC

TJÄNSTEBESKRIVNING OCH TILLÄMPNINGSANVISNING

29.6.2022

INNEHÅLL

1 ALLMÄNT

I den här tjänstebeskrivningen definieras förutsättningarna för införande av identifieringstjänsten för tjänsteleverantören samt beskrivs dataposterna med anknytning till införandet av identifieringstjänsten. I S-Bankens identifieringstjänst identifierar banken på ett tillförlitligt sätt på tjänsteleverantörens vägnar de kunder som uträttar ärenden elektroniskt. Identifieringstjänsten har tagits fram i enlighet med det Förtroendenät-protokoll som Transport- och kommunikationsverket har definierat och som baseras på OpenID Connect-protokollet. Identifieringstjänsten är avsedd för leverantörer av elektroniska identifieringsförmedlingstjänster samt leverantörer av ärendehanteringstjänster, nedan kunden. Gränssnittet för identifieringstjänsten har genomförts baserat på 12 a § 2 mom. i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009) samt Transport- och kommunikationsverkets gränssnittsrekommendationer för OpenID Connect 1.0.

2 ALLMÄN BESKRIVNING

Den kod som S-Banken ger är unik och den är bunden till såväl ifrågavarande tjänsteleverantörs tjänstetransaktion som kunden. Kunden identifieras med samma bankkoder som kunden använder för S-Bankens egna tjänster. När tjänsteleverantören har ett behov av att identifiera sin kund, skickar tjänsteleverantören en begäran om identifiering till kunden, som går till S-Bankens identifieringstjänst genom att klicka på bankens identifieringsknapp.

Tjänsteleverantörens begäran om identifiering förmedlas från kunden till S-Bankens identifieringstjänst, som efter identifiering skickar kunden ett svarsmeddelande. Kunden kontrollerar uppgifterna i svarsmeddelandet och kan efter att ha godkänt dem gå tillbaka till tjänsteleverantörens tjänst. Vid behov kan kunden avbryta eller förkasta identifieringstransaktionen antingen före identifiering eller efter att kunden granskat svarsmeddelandet. Om kunden avbryter identifieringstransaktionen kommer uppgifterna inte att förmedlas till tjänsteleverantören.

De identifieringsuppgifter som förmedlas via identifieringstjänsten kan även användas som en del av en elektronisk underskrift om kunden som vill identifiera sig och tjänsteleverantören kommer överens om detta. S-Banken ombesörjer dock endast identifiering av kunden på det sätt som beskrivs i tjänstebeskrivningen och svarar inte för hur bindande rättshandlingen mellan kunden och tjänsteleverantören är och inte heller för dess innehåll.

Identifieringstjänsten kan användas 24 timmar under alla veckodagar, frånsett avbrott som beror på underhåll, uppdatering eller motsvarande orsaker.

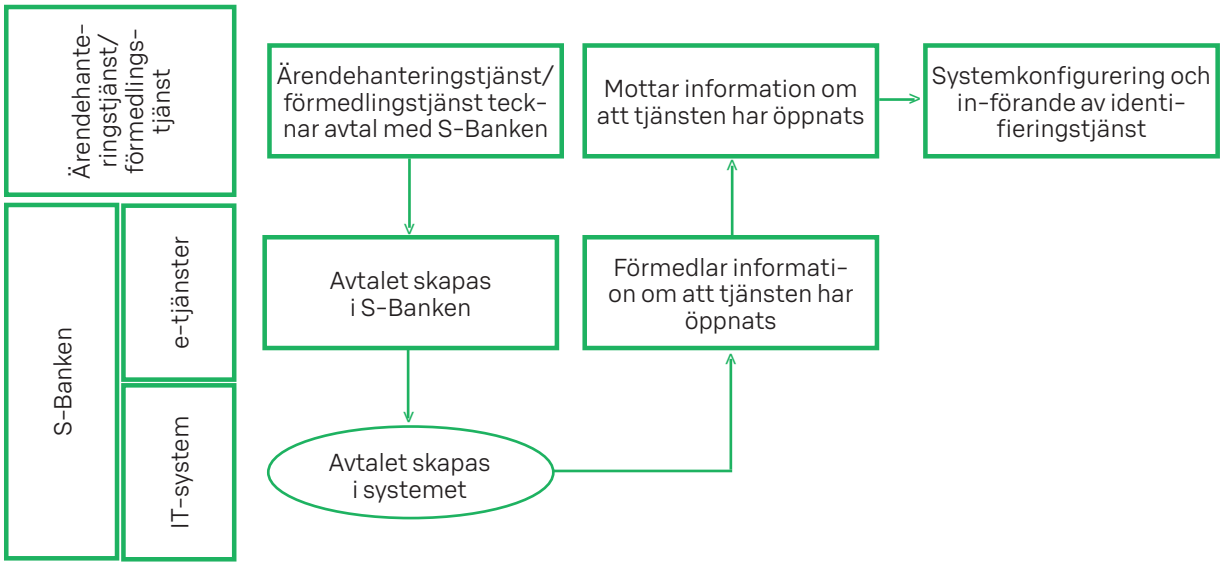
När man identifierar sig med bankkoder i andra än S-Bankens tjänster, omfattas koderna av kraven på stark autentisering enligt lagen om stark autentisering och betrodda elektroniska tjänster samt av Trafik- och kommunikationsverkets bestämmelser som utfärdats med stöd av lagen. Trafik- och kommunikationsverket har som uppgift att övervaka att nämnda lag följs.

Förutsättningar för att ta i bruk tjänsten:
1) tecknande av tjänsteavtal med S-Banken
2) utbyte av offentliga nycklar för underskrift och kryptering
3) konfigurering av tjänsten i systemen för identifieringsförmedlingstjänsten eller ärendehanteringstjänsten

Användningen av identifieringstjänsten sker i enlighet med standarden OpenID Connect.

Identifiering med OpenID Connect sker stegvis:
1. Begäran om identifiering startar identifieringsprocessen
2. Identifiering av innehavaren av identifieringsverktyget
3. Begäran om auktorisering för att begära identifieringsuppgifterna

Bild 1: Införande av identifieringstjänsten



Med hjälp av standarden OpenID Connect lägger man till en identitet på protokollet OAuth 2.0. Protokollet OAuth 2.0 erbjuder tjänster förknippade med auktorisering. Identifiering med OpenID Connect görs via gränssnittet HTTPS REST.

Mer information om konfigurering av det tekniska gränssnittet e-palvelut@s-pankki.fi

3 AVTAL

Tjänsteleverantören ska teckna ett skriftligt avtal om användningen av identifieringstjänsten med S-Banken. Tjänsteleverantörens uppgifter registreras i banken och ett krypterat e-postmeddelande med krypterings- och underskriftsnycklarna skickas till den kontaktperson som angetts i avtalet.

Tjänsteleverantören svarar för att denne enligt EU:s allmänna dataskyddsförordning (GDPR) har en grund att behandla personers namn, födelsetider och personbeteckningar.

Tjänsteleverantören ska informera S-Banken om dennes tjänst eller uppgifter förändras. S-Banken kompletterar vid behov avtalet med de förändrade uppgifterna.

4 S-BANKENS KNAPP SOM ANVÄNDS I IDENTIFIERINGSTJÄNSTEN

I tjänsteleverantörens webbtjänst ska användningen av identifieringstjänsten anges med S-Bankens märke för webbtjänster och det ska vara enkelt att se. Märket i fråga används som funktionsknapp.

Bildfilen med S-Bankens knapp för identifieringstjänsten kan hämtas på S-Bankens webbplats. Storleken eller färgerna på knappen får inte redigeras, skapas själva eller formas. Knappbilden får inte användas för annat ändamål än vad som avtalats i avtalet mellan tjänsteleverantören och S-Banken.

I S-Bankens tjänst är namnet identifieringstjänst (tunnistuspalvelu). S-Bankens namn får inte heller redigeras eller delas upp på flera rader.

5 UTBYTE AV OPENID CONNECT-KRYPTERINGS- OCH UNDERSKRIFTSNYCKLAR

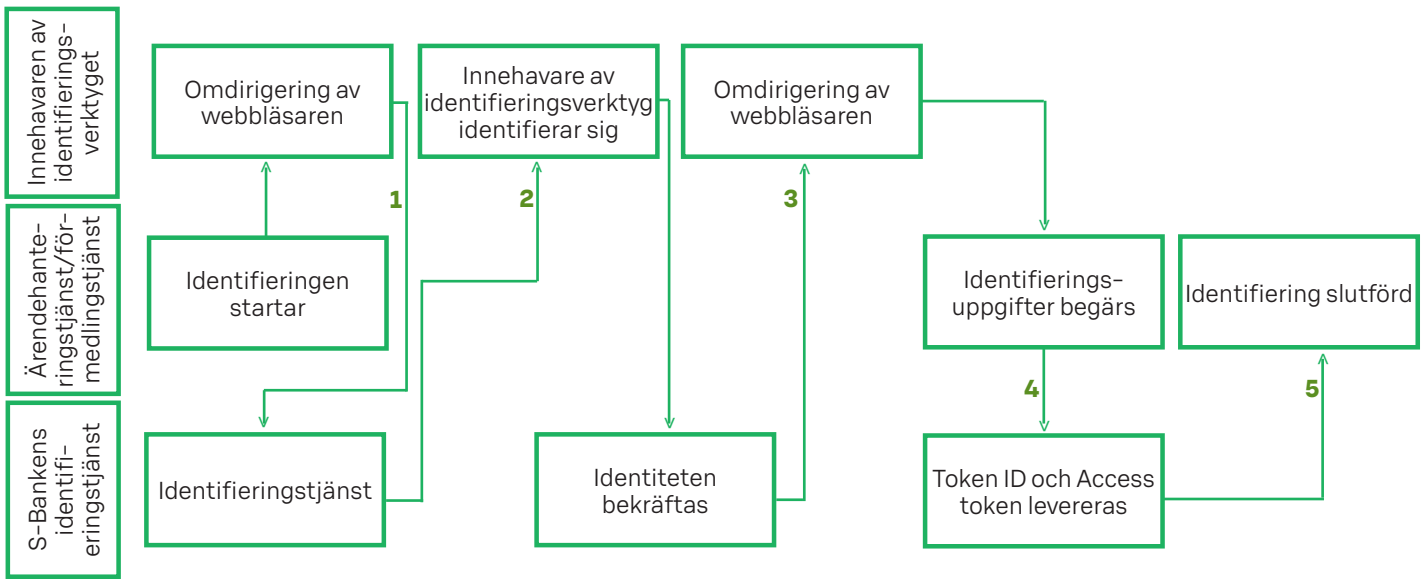
Tjänsteleverantören ska skapa en krypteringsnyckel och skicka den offentliga delen av nyckeln (public key) i pem-format i ett krypterat e-postmeddelande till S-Banken. S-Bankens kommunikation sker via e-postadressen e-palvelut@s-pankki.fi. S-Banken skapar en underskriftsnyckel och skickar den offentliga delen av nyckeln i ett krypterat e-postmeddelande till tjänsteleverantören.

6 KONFIGURERING AV TJÄNSTEN I SYSTEMEN FÖR IDENTIFIERINGSFÖRMEDLINGSTJÄNSTEN ELLER ÄRENDEHANTERINGSTJÄNSTEN

Kunden mottar de OpenID Connect-konfigurationsuppgifter som är förknippade med användningen av identifieringstjänsten i samma krypterade e-postmeddelande som de nycklar som nämnts i stycket ovan och som behövs för att använda identifieringstjänsten. Kunden ska konfigurera de givna uppgifterna i sitt system för att kunna använda S-Bankens identifieringstjänst.

Bild 2 visar skedena i identifieringstransaktionen:
1. Begäran om identifiering undertecknad (authorization request)
2. Identifiering
3. Identifieringskod (authorization code)
4. Begäran om kod för identifieringstransaktionen (token request)
5. ID token undertecknad/krypterad med identifieringsuppgifterna

Bild 2: Identifieringstransaktion



7 BEGÄRAN OM IDENTIFIERING (OIDC AUTHORIZATION REQUEST)

Begäran om identifiering är ett HTTPS REST authorization request-meddelande i enlighet med protokollet OpenID Connect, och det skickas till identifieringsadressen (authorization endpoint): https://online.s-pankki.fi/ftn/authorize

Ärendehanteringstjänsten eller förmedlingstjänsten omdirigerar med givna parametrar webbläsaren hos innehavaren av identifieringsverktyget till den adress som motsvarar identifieringsadressen. När adressen öppnas, startas identifieringsprocessen av innehavaren av identifieringsverktyget i S-Bankens identifieringstjänst.

I S-Bankens identifieringstjänst omdirigeras webbläsaren hos innehavaren av identifieringsverktyget efter lyckad identifiering till omdirigeringsadressen (redirect URI) för ärendehanteringstjänsten eller förmedlingstjänsten. Omdirigeringsanropet inkluderar som parameter en auktoriseringskod (authorization code) som beviljats av identifieringstjänsten och som ärendehanteringstjänsten eller förmedlingstjänsten kan använda för att hämta identifieringsuppgifterna från S-Bankens identifieringstjänst via begäran om auktorisering (token request). Begäran om identifiering undertecknas alltid med ärendehanteringstjänstens eller förmedlingstjänstens privata nycklar.

8 BEGÄRAN OM AUKTORISERING (OIDC TOKEN REQUEST)

Begäran om auktorisering är ett token request-meddelande som uppfyller protokollet OpenID Connect eller som förmedlingstjänsten skickar till auktoriseringsadressen (token endpoint) som ett direkt HTTPS REST-meddelande. Som parameter i meddelandet ansluts den auktoriseringskod (authorization code) som mottagits till följd av begäran om identifiering och som svar mottas en identifieringskod (ID token) och accesskod (access token).

Meddelanden förmedlas i enlighet med standarden JSON Web Token (IETF RFC 7519). JWT definierar JSON-dataöverföringsmetoden mellan två aktörer. Identifieringskoden (ID token) är en base64-kodad, undertecknad och krypterad JWE (JSON Web Encryption), som innehåller identifieringsuppgifterna (claims) om innehavaren av identifieringsverktyget. Elementen är separerade med punkt och base64-kodade.

Den mottagna identifieringskoden ska alltid valideras i enlighet med OpenID Connect-specifikationen. Begäran om auktorisering undertecknas alltid med ärendehanteringstjänstens eller förmedlingstjänstens privata nycklar. Begäran om auktorisering undertecknas alltid med privata nycklar från S-Bankens identifieringstjänst och krypteras med ärendehanteringstjänstens eller förmedlingstjänstens nycklar.

9 KUNDUPPGIFTER

UserInfo-slutpunkten är en OAuth 2.0-skyddad resurs som återställer kraven gällande en verifierad slutanvändare. För att få de begärda kraven gällande slutanvändaren lämnar kunden en begäran till UserInfo-slutpunkten genom att använda den användarbehörighet som erhållits genom OpenID Connect-verifiering.

UserInfo-slutpunkten är inte obligatorisk, den är en av de tillgängliga slutpunkterna som en del av FTN-utförandet. De kunder som använder FTN-utförandet ska besluta om de vill använda denna slutpunkt.

10 TEST AV IDENTIFIERINGSTJÄNSTEN

I det säkerhetsmeddelande som skickas till kunden när avtalet tecknas får kunden anvisningar för test av identifieringstjänsten.

11 UNDANTAGSSITUATIONER

Tjänsteleverantören ska förbereda sig på undantagssituationer som till exempel:

1. Kunden avbryter identifieringstransaktionen. Kunden kan avbryta transaktionen antingen innan koden förmedlas till S-Bankens identifieringstjänst eller efter att koden har skapats genom att klicka på avbryt.
2. Verifiering av kunden misslyckas antingen på grund av att de identifieringsuppgifter som kunden gett är felaktiga eller om kunden har begärt verifiering via fel bank. Kunden går tillbaka till tjänsteleverantörens tjänst genom att klicka på avbryt.
3. S-Banken observerar ett fel i begäran om identifiering. S-Banken observerar ett fel i begäran om identifiering innan kunden har verifierats. Kunden går tillbaka till tjänsteleverantörens tjänst.
4. Tjänsteleverantören observerar ett fel i koden. Felet kan bero på ett fel i meddelandets innehåll eller på att koden inte motsvarar de personuppgifter som kunden uppgett. Tjänsteleverantören ska förse kunden med ett meddelande som motsvarar situationen.
5. Inget svar kommer. Orsaken till avbrottet kan vara ett kommunikationsavbrott, annat tekniskt fel, att kunden lämnar sessionen på hälft eller att en timeout sker i kundens session.
6. Samma svar skickas flera gånger.

12 RÅDGIVNING OCH TEKNISK SUPPORT

Teknisk support för identifieringstjänsten
e-palvelut@s-pankki.fi

13 LÄNKAR

Finnish Trust Network OpenID Connect 1.0 Protocol Profile version 1.0
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ftn_oidc_profile_v1.0_ficora_rec_213_2018_s.pdf

OpenID Connect –protokolla
https://openid.net/connect/

OpenID Connect 1.0
https://openid.net/specs/openid-connect-core-1_0.html

JSON Web Tokens
http://jwt.io

6/2022 S-Banken