Hightrust.id rajapintakuvaus

Hightrust.id (HTID) tarjoaa luottamusverkoston rajapinnan Kyberturvallisuuskeskuksen tarjoaman OpenID Connect (OIDC) suosituksen mukaisesti. Noudatettu “OIDC Authorization Code flow” käyttää PKCE:ta, jolloin osapuolten on toimitettava kutsuissa vastaavat parametrit. HTID tukee suosituksen mukaisia pakollisia parametreja ja attribuutteja.

Luottamuksen perustaminen

Luottamussuhde perustetaan jakamalla Entity Stament molemminpuolisesti, jonka jälkeen se aktivoidaan manuaalisesti. Tässä yhteydessä jaetaan myös OIDC:n client_id, redirect_uri sekä audience parametrit. HTID Entity Statement sisältää metatiedossaan myös “token endpoint” URI:n, josta haetaan ID Token.

Authentication request

OIDC:n mukainen “authentication request” on sisällettävä kaikki suosituksen mukaiset pakolliset parametrit. Tämän lisäksi pyynnön on sisällettävä parametrit audience sekä PKCE:n mukaiset code_challenge ja code_challenge_method=S256.
Koska HTID:n LoA-taso on tällä hetkellä korotettu, tuetaan vain acr_values arvoa “http://ftn.ficora.fi/2017/loatest2”.

ID Token Request

Token endpoint pyyntö autentikoidaan private_key_jwt-menetelmällä käyttäen suosituksen mukaista RS256 algoritmia. Lisäksi välitetään PKCE:n mukainen code_verifier parametri. Autentikointiin käytettävä JWT token (client_assertion) on sisällettävä seuraavat parametrit:

- iss: *client_id*
- exp: *5m*
- aud: *AUTH_ENV_URL/oauth2/token*
- sub: *client_id*
- jti: *uuid*

, missä *AUTH_ENV_URL* on joko testi- tai tuotantoympäristön OpenID Connect palvelun url, joka saadaan ympäristöä vastaavan Entity Statementin metatiedon issuer-kentän arvosta.

Vastauksena ID token pyyntöön palautuu allekirjoitettu ja salattu ID Token. Allekirjoituksessa käytetty algoritmi on suosituksessa esitetty RS256 ja salauksessa RSA-OAEP.

ID Token sisältää seuraavat käyttäjän attribuutit:

- urn:oid:1.2.246.21 (HETU)
- urn:oid:1.3.6.1.5.5.7.9.1 (DateOfBirth)
- urn:oid:1.2.246.575.1.14 (FirstNames)
- urn:oid:2.5.4.4 (FamilyName)

Tämän lisäksi ID token sisältää muita varmenteen tietoja kuten issuer, subject ja notAfter FTN-kontekstin ulkopuolelta.

Erillistä “User Info”- API:a ei ole käytössä.

Testausjärjestelyt

Tuotannon kanssa identtinen testiympäristö on tarjolla, jonka asetukset saadaan jaettavasta Entity Statementista, kun testauksesta on sovittu osapuolten kesken. Testi clientin asetukset tehdään tämän dokumentin mukaisesti ja noudattaen Kyberturvallisuuskeskuksen tarjoaman OpenID Connect (OIDC) suositusta.