

Logout

Introductie

Op [deze](#) en [deze](#) pagina's vind je meer informatie over de gebruikte specificaties. Deze specificaties zijn leidend, de tekst hieronder geldt als een versimpelde **conceptuele** uitleg. Deze tekst moet niet gebruikt worden als leidraad voor een implementatie. Daarvoor verwijzen we naar de eerder genoemde specificaties.

Beknopte uitleg

Net zoals bij SAML2.0 Single Logout is het met OpenID Connect mogelijk om vanuit een Relying Party (RP) en vanuit een OpenID Provider (OP) uit te loggen.

Voor het gemak beschrijven we deze implementaties als **Relying Party initiated Logout** en **OpenID Provider initiated Logout** en noemen we de OpenID Provider (OP) een Identity Provider (IdP).

Relying Party initiated Logout (specificatie: OpenID Connect RP-Initiated Logout 1.0)

1. De browser stuurt een uitlog verzoek naar de Relying Party.
2. De Relying Party stuurt de browser van de gebruiker door naar de uitlogpagina van de Identity Provider.
3. De Identity Provider beëindigd de gebruikerssessie en stuurt het uitlogverzoeken naar andere Relying Party's en leidt de browser optioneel door naar de uitlogpagina van de Relying Party.

OpenID Provider initiated Logout (specificatie: OpenID Connect Front-Channel Logout 1.0)

1. De browser stuurt het uitlogverzoek naar de Identity Provider.
2. De Identity Provider toont een uitlogpagina met één of meerdere **<iframe>** elementen met de logout URI's van de Relying Party's waarmee de eindgebruiker een sessie heeft.
3. De browser roept alle **<iframe>** elementen aan en initieert per Relying Party één uitlogverzoek.
4. De Relying Party ontvangt het uitlogverzoek en beëindigen de sessie met de gebruiker.

In tegenstelling tot SAML2.0 Single Logout (m.u.v. een asynchrone logout) is er bij bovengenoemde implementaties geen garantie dat de sessie bij de Relying Party beëindigd is.

Implementatie

Een aantal factoren waar een beheerder en/of ontwikkelaar van een Relying Party rekening mee moet houden zijn:

- Het gebruik van security headers t.b.v. **<iframe>** elementen zoals (maar niet uitsluitend): X-Frame-Options, Content-Security-Policy, etc. op de uitlogpagina (frontchannel_logout_uri).
- Het verschil tussen een frontchannel_logout_uri en post_logout_redirect_uri.
- Het vermelden van de frontchannel_logout_session_required indien de waarde 'true' is.
- Bij het gebruik van een post_logout_redirect_uri is een id_token_hint verplicht.

Testen

Het Identity Provider /.well-known/openid-configuration endpoint adverteert ondersteuning voor onderstaande instellingen. Dit houdt in dat als jouw applicatie deze instellingen automatisch inleest er mogelijk onbedoeld gebruik gemaakt wordt van de mogelijkheid om uit te kunnen loggen. Om een correcte werking van de OpenID Connect implementatie te garanderen doen wij een dringend verzoek om dit te controleren.

Via een TOPdesk melding kan verzocht worden om jouw geregistreerde applicatie op de Identity Provider te voorzien van tenminste een logout_redirect_uri en optioneel een post_logout_redirect_uri.

Onderstaande elementen zijn t.o.v. de productie omgeving toegevoegd aan het /.well-known/openid-configuration endpoint:

- end_session_endpoint: https://login.<acc>.uu.nl/nidp/oauth/v1/nam/end_session
- frontchannel_logout_session_supported: true
- frontchannel_logout_supported: true

Revision #22

Created 27 June 2023 13:31:54 by Haas, T.P.R. de (Tom)

Updated 18 October 2023 12:08:54 by Schmidt, M.S. (Mick)