

Table 13.1 Claims inside an ID token

Claim Name	Claim Description
iss	The <i>issuer</i> of the token; URL of the IdP.
sub	The <i>subject</i> of the token, a stable and unique identifier for the user at the IdP. This is usually a machine-readable string and shouldn't be used as a username.
aud	The <i>audience</i> of the token; must contain the client ID of the RP.
exp	The <i>expiration</i> timestamp of the token. All ID tokens expire, and usually pretty quickly.
iat	The timestamp of <i>when the token was issued</i> .
auth_time	The timestamp of <i>when the user authenticated to the IdP</i> .
nonce	A string sent by the RP during the authentication request, used to mitigate replay attacks similar to the <i>state</i> parameter. It must be included if the RP sends it.
acr	The <i>authentication context reference</i> , which indicates an overall categorization of the authentication that the user performed at the IdP.
amr	The <i>authentication method reference</i> , which indicates how the user authenticated to the IdP.
azp	The <i>authorized party</i> for this token; must contain the client ID of the RP if it's included.
at_hash	Cryptographic hash of the access token.
c_hash	Cryptographic hash of the authorization code.