Chapter 6

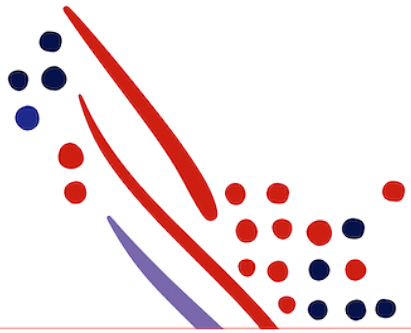
Step 5: Validate ID Token

from Understanding the End-User App Authorization Process

Published on
Nov 12, 2019, 10:11 PM

Last modified
Jul 17, 2024, 03:40 PM

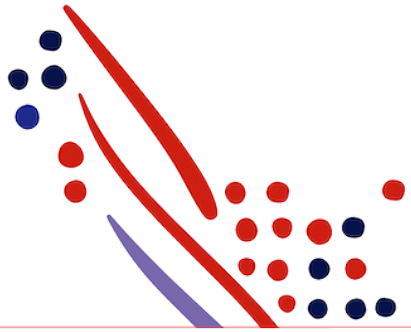
Always Designing for People™



ADP Copyright Information

Published on
Nov 12, 2019, 10:11 PM

Published on
Jul 17, 2024, 03:40 PM



Chapter Contents

Chapter 6

Step 5: Validate ID Token

An identity token is an assertion of the authentication of the end-user by the OpenID Connect identity provider. The assertion is provided as a JSON Web Token (JWT) object in the id_token parameter of the JSON object returned on a successful authorization code exchange.

A JWT contains three binhex encoded sections separated by dots ("."): a header, a set of asserted claims, and the signature of the header and the claims. Your consumer application must decode and validate the JWT.

The encoded claims section of the id_token decodes to the following JSON object.


```
{ "iss":"https://accounts.adp.com",
  "sub":"https://accounts.adp.com/user/G123123123123213/G456783748392999",
  "exp":1412793735,
  "iat":1412786535,
  "auth_time":1412786535,
  "nonce":"163141324",
  "azp":"c5348fb0-efd6-4632-a359-d6c2f5ab04f6",
  "c_hash":"2oYJkgWbM3jgT5QjuSfNaQ",
  "name":"Anthony Albright",
  "given_name":"Anthony",
  "family_name":"Albright",
  "email":"Anthony.Albright@blah.com"
}
```


Parameter	Description
iss	The issuer of the authentication assertion. In this case, theADP OpenID Connect Provider contains the following value: https://accounts.adp.com.
sub	The subject of the assertion. A unique identifier associated with the end-user authenticating with ADP.
aud	The party to which the id_token was issued. The value is your consumer application's client_id.
exp	The expiration time of the assertion. Your consumer application should not accept expired assertions.
iat	The time the assertion was issued. Your consumer application can use this parameter to determine the age of the assertion.
auth_time	The time when the end-user authentication occurred.
nonce	Returned if your consumer application provided this parameter in the authorize request. This parameter mitigates replay attacks.
azp	The party to which the id_token was issued. The value is your consumer application's client_id.
c_hash	Authorization code hash value. It is the binhex encoding of the left-most half of the authorization. The hash algorithm is the algorithm specified in the header section.

Normally, it is critical that you validate an ID token before you use it, but since you are communicating directly with ADP over an HTTPS channel and using your client credentials and signed certificate to authenticate yourself to ADP, you can be confident that the token you receive really comes from ADP and is valid. If your server passes the ID token to other components of your app, it is extremely important that the other components validate the token before using it.

Your consumer application may decode and minimally validate the id_token as follows:

- Validate the signature of the JWT.
- Validate that the value of the nonce parameter matches the value provided in the authorize request if your consumer application provided one.
- Validate that the value of the iss (Issuer) parameter matches https://accounts.adp.com.

- Validate that the "aud" (audience) parameter contains the client_id assigned to your consumer application.
- Validate that the "azp" (authorized party) parameter contains the client_id assigned to your consumer application.
- Validate that the id_token has not expired or that the current time is before the value specified in the "exp" parameter.
- Validate that the c_hash parameter matches the authorization code provided by the result of the authorization request to the ADP Authorization Service.