1. Access Token

inside.Docupedia Export

Author: BAI Hongyin (AA/SWS3-CN)
Date: 02-Mar-2022 04:39

Table of Contents

1 Overview

In order to make authorized calls e.g to the OpenId Connect (OIDC) Userinfo Endpoint or other APIs, a **Client Application must first obtain an Access Token on behalf of a user**. This access token is sent to the API as credential. The passed token informs the API that the bearer of the token has been authorized to access the API and perform specific actions specified by the scope that was granted during authorization. The scopes defined by the token issuer control and limit the set of data which the requesting application is allowed to request or create.

2 Example


```
{
"iss":"https://identity.bosch.com.cn/",
"aud":"https://identity.bosch.com.cn/resources",
"exp":1500646946,
"client_id":"ciamids_0815",
"scope":
[
"openid",
"profile",
"phone",
"offline_access"
],
"sub":"S-1-5-21-3923742794-3248341794-1582090486-xxxx",
"auth_time":1495462946,
"idp":"identityserver",
"amr":
[
"external"
]
}
```

3 Header Claims

Tokens

4 Payload Claims

Claim Name	JSON Value Type	Claim Syntax	Claim Description
aud	string	StringAndURI	The aud (audience) claim identifies the **recipients that the JWT is intended for**. Each principal intended to process the JWT MUST identify itself with a value in the audience claim. If the principal processing the claim does not identify itself with a value in the aud claim when this claim is present, then the JWT MUST be rejected. In the general case, the aud value is an array of case-sensitive strings, each containing a StringOrURI value.
iss	string	StringAndURI	The iss (issuer) claim identifies the **principal that issued the JWT**. The processing of this claim is generally application specific. The iss value is a case-sensitive string containing a StringOrURI value.
exp	integer	IntDate	The exp (expiration time) claim identifies the **expiration time on or after which the JWT MUST NOT be accepted for processing**. The processing of the exp claim requires that the current date/time MUST be before the expiration date/time listed in the exp claim.
client_id	string	StringOrGUID	The “client_id” value represents the **registered OpenID Connect Client ID** and is required to identify the requesting and targeting client application.
scope	string	String / JSON Array String	The "scope" value defines what kind of pre-defined set of **user attributes** the client is allowed to request.
sub	string	objectSID	The "sub" (subject) claim is the **unique Bosch ID of a user**.
auth_time	string	Timestamp ISO8601	**Time of authorization** when the user logged in.
idp	string	String	The "idp" value defines which **IdP** was used for identifying the Users.

Claim Name	JSON Value Type	Claim Syntax	Claim Description
amr	string	String / JSON Array String	The Authentication Methods References "amr" value represents a **JSON array of strings that are identifiers for authentication methods** used in the authentication.

5 Scope Handling

In oAuth2.0 / Open ID Connect scopes are used to **specify access privileges** when issuing an access token to an application. The scopes you as an application are requesting in the authorization and the token request will be **delivered in the access token you get from CIAM**.

5.1 Default scopes

CIAM uses the following standard scopes:

Scope	Required?
openid	yes
phone	no
email	no
profile	no
offline_access	(yes) Scope offline_access is **required to get a refresh token**