`"ver": 1,`

"jti": "AT.PhSunKerSs9hLp7SoFu74hhN4xGd7fgHjDmx-OFo-K4",

{

Header

"alg": "RS256"

`"exp": 1744848072,`

}

```
"aud": "api://default",
```

"scp": [

"cid": "0oao9o802iZ9VZLTY5d7",

"openid",

```
"iss": "https://dev-83916648.okta.com/oauth2/default",
```

```
"uid": "00uo8z7jp14kNa6qZ5d7",
```

"profile",

```json
"kid": "O7foVO74iGyRDL7ho4CfUj5ZODUlgDdSVR6C2aCZDdw",
```

```
"iat": 1744844472,
```

`"auth_time": 1744843464,`

"sub": "semona.igama+32@okta.com"

],

"read:messages"

Anatomy of an access token

Minimum claims to validate

Depends on the resources

Two ways to validate a token

- Local

- Up-to-date info

- the token is sent to the authorization server for validation

- App performs the validation itself

- Remote (/introspect endpoint)

- Keys are fetched dynamically from the JWKS endpoint (/keys endpoint)