**Table 11.1 Standard JSON web token claims**

| Claim Name | Claim Description |
|---|---|
| `iss` | The *issuer* of the token. This is an indicator of *who created this token*, and in many OAuth deployments this is the URL of the authorization server. This claim is a single string. |
| `sub` | The *subject* of the token. This is an indicator of *who the token is about*, and in many OAuth deployments this is a unique identifier for the resource owner. In most cases, the subject needs to be unique only within the scope of the issuer. This claim is a single string. |
| `aud` | The *audience* of the token. This is an indicator of *who is supposed to accept the token*, and in many OAuth deployments this includes the URI of the protected resource or protected resources that the token can be sent to. This claim can be either an array of strings or, if there's only one value, a single string with no array wrapping it. |
| `exp` | The *expiration* timestamp of the token. This is an indicator of *when the token will expire*, for deployments where the token will expire on its own. This claim is an integer of the number of seconds since the UNIX Epoch, midnight on January 1, 1970, in the Greenwich Mean Time (GMT) time zone. |
| `nbf` | The *not-before* timestamp of the token. This is an indicator of *when the token will begin to be valid*, for deployments where the token could be issued before it becomes valid. This claim is an integer of the number of seconds since the UNIX Epoch, midnight on January 1, 1970, in the GMT time zone. |
| `iat` | The *issued-at* timestamp of the token. This is an indicator of *when the token was created*, and is commonly the system timestamp of the issuer at the time of token creation. This claim is an integer of the number of seconds since the UNIX Epoch, midnight on January 1, 1970, in the GMT time zone. |
| `jti` | The *unique identifier* of the token. This is a value *unique to each token created by the issuer*, and it's often a cryptographically random value in order to prevent collisions. This value is also useful for preventing token guessing and replay attacks by adding a component of randomized entropy to the structured token that would not be available to an attacker. |