End user — **Consumer** — **SP** — **OP**

Request Cons to use SP data.

Request <u>unauthorized request token</u>.

(Unauthorized) request token

Redirect to SP.

(Unauthorized) request token

SP obtaining user authorization.

User authorization.

(Authorized) request token

Request access token.

Access Token and Token key

OAuth

End user	Consumer	SP	OP

Send user's OpenID identifier.

Association Request.

Association Response.

Claimed Identifier

Authentication Request.

Redirect user to OP.

Obtaining user authentication.

Authentication.

Authentication Response.

Assertion

OpenID

End user | Consumer | SP | OP

Request Cons to use SP data.

Send user's OpenID identifier.

Request unauthorized request token.

(Unauthorized) request token

Redirect to SP.

(Unauthorized) request token

Association Request.

Association Response.

Claimed Identifier

Authentication Request.

Redirect user to OP.

Obtaining user authentication.

Authentication.

If the user have already signed in this OP, these interaction will be skipped.

Authentication Response.

Assertion

SP obtaining user authorization.

User authorization.

(Authorized) request token

Request access token.

Access Token and Token key

OpenID+OAuth

End user   Consumer   SP   OP

Request Cons to use SP data.

Send user's OpenID identifier.

Request unauthorized request token / Association Request.

(Unauthorized) request token

Association Response.

Authentication Request.
Redirect to SP.

(Unauthorized) request token   Claimed Identifier

Obtaining user authentication and authorizarion at the same time.

Authentication and authorization.

Assertion   (Authorized) request token

Authentication Response.

Request access token.

Access Token and Token key

OpenID+OAuth
Superimposed in case OP
and SP are same