IETF 90 OAuth WG

Request by JWS ver.1.0 for OAuth 2.0

draft-sakimura-oauth-requrl-05

2014/7/24

Nat Sakimura

Nomura Research Institute

In the begging, was the "application/x-www-form-urlencoded” response.

- But it was replaced by JSON in draft-ietf-oauth-v2-09 (June 29, 2010)
- Request remained form-urlencoded.

- There was a parallel proposal to make the request JSON as well:
  - http://tools.ietf.org/html/draft-sakimura-oauth-requrl-00 (June 17, 2010)
  - Idea was to replace the form-urlencoded request with a (optionally signed) JSON.
  - Further, as the name indicates, assign a URL to it and send the URL instead and have the server pull it.
- Had some support, but was put on hold until the main spec is done.

Advantage of using JWT/JWS/JWE

1. The request may be signed so that integrity check may be implemented. If a suitable algorithm is used for the signing, then non-repudiation property may be obtained in addition.
2. The request may be encrypted so that end-to-end confidentiality may be obtained even if in the case TLS connection is terminated at a gateway or a similar device.

Advantage of using references

1. When it is detected that the User Agent dose't suport long URLs - It is entirely possible that some extensions may extend the URL. For example, the client might want to send a public key with the request.
2. Static signature: The client may make a signed Request Object and put it on the client. This may just be done by a client utility or other process, so that the private key does not have to reside on the client, simplifying programming.
3. When the server wants the requests to be cacheable - The request_uri may include a sha256 hash of the file, as defined in FIPS180-2 [FIPS180-2], the server knows if the file has changed without fetching it, so it does not have to re-fetch a same file, which is a win as well.
4. When the client wants to simplify the implementation without compromising the security. If the request parameters go through the Browser, they may be tampered in the browser even if TLS was used. This implies we need to have signature on the request as well. However, if HTTPS "request_uri" was used, it is not going to be tampered, thus we now do not have to sign the request. This simplifies the implementation.

After that …

- Subsequently, OpenID Connect adopted it for finer grained claims request etc.
- This can be generally useful outside of OpenID Connect.
- Should we push this forward within the WG?