OAuth Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 16, 2016

N. Sakimura, Ed.
Nomura Research Institute
J. Bradley
Ping Identity

October 14, 2015

OAuth 2.0 JWT Authorization Request
draft-ietf-oauth-jwsreq-06

Abstract

The authorization request in RFC6749 utilizes query parameter serialization. This specification defines the authorization request using JWT serialization. The request is sent by value through "request" parameter or by reference through "request_uri" parameter that points to the JWT, allowing the request to be optionally signed and encrypted.

Status of This Memo

This Internet-Draft will expire on April 16, 2016.

Copyright Notice

Table of Contents

1. Introduction

The parameters "request" and "request_uri" are introduced as additional authorization request parameters for the OAuth 2.0 [RFC6749] flows. The "request" parameter is a JSON Web Token (JWT) [RFC7519] whose JWT Claims Set holds the JSON encoded OAuth 2.0 authorization request parameters. The JWT [RFC7519] can be passed to the authorization endpoint by reference, in which case the parameter "request_uri" is used instead of the "request".

Using JWT [RFC7519] as the request encoding instead of query parameters has several advantages:

1. The request can be signed so that an integrity check can be implemented. If a suitable algorithm is used for the signing, then it will provide verification of the client making the request.

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.

3. The request may be signed by a third party attesting that the authorization request is compliant to certain policy. For example, a request can be pre-examined by a third party that all the personal data requested is strictly necessary to perform the process that the end-user asked for, and statically signed by that third party. The client would then send the request along with dynamic parameters such as state. The authorization server then examines the signature and show the conformance status to the end-user, who would have some assurance as to the legitimacy of the request when authorizing it. In some cases, it may even be desirable to skip the authorization dialogue under such circumstances.

There are a few cases that request by reference are useful such as:

1. When it is detected that the User Agent does not support long URLs: 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 can make a signed Request Object and put it at a place that the Authorization Server can access. 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 SHA-256 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.

This capability is in use by OpenID Connect [OpenID.Core].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Terminology

For the purposes of this specification, the following terms and definitions apply.

2.1. Request Object

JWT [RFC7519] that holds an OAuth 2.0 authorization request as JWT Claims Set

2.2. Request Object URI

Absolute URI from which the Request Object (Section 2.1) can be obtained

3. Request Object

A Request Object (Section 2.1) is used to provide authorization request parameters for an OAuth 2.0 authorization request. It contains OAuth 2.0 [RFC6749] authorization request parameters including extension parameters. It is a JSON Web Signature (JWS) [RFC7515] signed JWT [RFC7519] . The parameters are represented as the JWT claims. Parameter names and string values MUST be included as JSON strings. Numerical values MUST be included as JSON numbers. It MAY include any extension parameters. This JSON [RFC7159] constitutes the JWT [RFC7519] Claims Set.

The Request Object MAY be signed or be an Unsecured JWS. When it is an unsecured JWS, this is indicated by use of the "none" algorithm JWA [RFC7518] in the JWS header. If signed, the Authorization Request Object SHOULD contain the Claims "iss" (issuer) and "aud" (audience) as members, with their semantics being the same as defined in the JWT [RFC7519] specification.

The Request Object MAY also be encrypted using JWE [RFC7516] and MAY be encrypted without also being signed. If both signing and encryption are performed, it MUST be signed then encrypted, with the result being a Nested JWT, as defined in JWT [RFC7519].

The Authorization Request Object MAY alternatively be sent by reference using the "request_uri" parameter.

REQUIRED OAuth 2.0 Authorization Request parameters that are not included in the Request Object MUST be sent as a query parameter. If a required parameter is not present in neither the query parameter nor the Request Object, it forms a malformed request.

"request" and "request_uri" parameters MUST NOT be included in Request Objects.

If the parameter exists in both the query string and the Authorization Request Object, the values in the Request Object takes precedence. This means that if it intends to use a cached request object, it cannot include such parameters like "state" that is expected to differ in every request. It is fine to include them in the request object if it is going to be prepared afresh every time.

The following is a non-normative example of the Claims in a Request Object before base64url encoding and signing. Note that it includes extension variables such as "nonce", "userinfo", and "id_token".

```
  {
   "iss": "s6BhdRkqt3",
   "aud": "https://server.example.com",
   "response_type": "code id_token",
   "client_id": "s6BhdRkqt3",
   "redirect_uri": "https://client.example.org/cb",
   "scope": "openid",
   "state": "af0ifjsldkj",
   "nonce": "n-0S6_WzA2Mj",
   "max_age": 86400,
   "claims":
    {
     "userinfo":
      {
       "given_name": {"essential": true},
       "nickname": null,
       "email": {"essential": true},
       "email_verified": {"essential": true},
       "picture": null
      },
     "id_token":
      {
       "gender": null,
       "birthdate": {"essential": true},
       "acr": {"values": ["urn:mace:incommon:iap:silver"]}
      }
    }
  }
```

Signing it with the "RS256" algorithm results in this Request Object value (with line wraps within values for display purposes only):

```
eyJhbGciOiJSUzI1NiIsImtpZCI6ImsyYmRjIn0.ew0KICJpc3MiOiAiczZCaGRSa3
F0MyIsDQogImF1ZCI6ICJodHRwczovL3NlcnZlci5leGFtcGxlLmNvbSIsDQogInJl
c3BvbnNlX3R5cGUiOiAiY29kZSBpZF90b2tlbiIsDQogImNsaWVudF9pZCI6ICJzNk
JoZFJrcXQzIiwNCiAicmVkaXJlY3RfdXJpIjogImh0dHBzOi8vY2xpZW50LmV4YW1w
bGUub3JnL2NiIiwNCiAic2NvcGUiOiAib3BlbmlkIiwNCiAic3RhdGUiOiAiYWYwaW
Zqc2xka2oiLA0KICJub25jZSI6ICJuLTBTNl9XekEyTWoiLA0KICJtYXhfYWdlIjog
ODY0MDAsDQogImNsYWltcyI6IA0KICB7DQogICAidXNlcmluZm8iOiANCiAgICB7DQ
ogICAgICJnaXZlbl9uYW1lIjogeyJlc3NlbnRpYWwiOiB0cnVlfSwNCiAgICAgIm5p
Y2tuYW1lIjogbnVsbCwNCiAgICAgImVtYWlsIjogeyJlc3NlbnRpYWwiOiB0cnVlfS
wNCiAgICAgImVtYWlsX3ZlcmlmaWVkIjogeyJlc3NlbnRpYWwiOiB0cnVlfSwNCiAg
ICAgInBpY3R1cmUiOiBudWxsDQogICAgfSwNCiAgICJpZF90b2tlbiI6IA0KICAgIH
sNCiAgICAgImdlbmRlciI6IG51bGwsDQogICAgICJiaXJ0aGRhdGUiOiB7ImVzc2Vu
dGlhbCI6IHRydWV9LA0KICAgICAiYWNyIjogeyJ2YWx1ZXMiOiBbInVybjptYWNlOm
luY29tbW9uOmlhcDpzaWx2ZXIiXX0NCiAgICB9DQogIH0NCn0.nwwnNsk1-Zkbmnvs
F6zTHm8CHERFMGQPhos-EJcaH4Hh-sMgk8ePrGhw_trPYs8KQxsn6R9Emo_wHwajyF
KzuMXZFSZ3p6Mb8dkxtVyjoy2GIzvuJT_u7PkY2t8QU9hjBcHs68PkgjDVTrG1uRTx
0GxFbuPbj96tVuj11pTnmFCUR6IEOXKYr7iGOCRB3btfJhM0_AKQUfqKnRlrRscc8K
ol-cSLWoYE9l5QqholImzjT_cMnNIznW9E7CDyWXTsO70xnB4SkG6pXfLSjLLlxmPG
iyon_-Te111V8uE83IlzCYIb_NMXvtTIVc1jpspnTSD7xMbpL-2QgwUsAlMGzw
```

The following RSA public key, represented in JWK format, can be used to validate the Request Object signature in this and subsequent Request Object examples (with line wraps within values for display purposes only):

```
{
 "kty":"RSA",
 "kid":"k2bdc",
 "n":"y9Lqv4fCp6Ei-u2-ZCKq83YvbFEk6JMs_pSj76eMkddWRuWX2aBKGHAtKlE5P
      7_vn__PCKZWePt3vGkB6ePgzAFu08NmKemwE5bQI0e6kIChtt_6KzT5OaaXDF
      I6qCLJmk51Cc4VYFaxgqevMncYrzaW_50mZ1yGSFIQzLYP8bijAHGVjdEFgZa
      ZEN9lsn_GdWLaJpHrB3ROlS50E45wxrlg9xMncVb8qDPuXZarvghLL0HzOuYR
      adBJVoWZowDNTpKpk2RklZ7QaBO7XDv3uR7s_sf2g-bAjSYxYUGsqkNA9b3xV
      W53am_UZZ3tZbFTIh557JICWKHlWj5uzeJXaw",
 "e":"AQAB"
}
```

4. Authorization Request

The client constructs the authorization request URI by adding the following parameters to the query component of the authorization endpoint URI using the "application/x-www-form-urlencoded" format:

request REQUIRED unless "request_uri" is specified. The Request Object (Section 3) that holds authorization request parameters stated in the section 4 of OAuth 2.0 [RFC6749].

request_uri REQUIRED unless "request" is specified. The absolute URL that points to the Request Object (Section 3) that holds authorization request parameters stated in the section 4 of OAuth 2.0 [RFC6749].

state RECOMMENDED. OAuth 2.0 [RFC6749] state.

The client directs the resource owner to the constructed URI using an HTTP redirection response, or by other means available to it via the user-agent.

For example, the client directs the end-user's user-agent to make the following HTTPS request (line breaks are for display purposes only):

```
GET /authorize?request_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1
Host: server.example.com
```

The authorization request object MAY be signed AND/OR encrypted.

When the "request" parameter is used, the OAuth 2.0 request parameter values contained in the JWT supersede those passed using the OAuth 2.0 request syntax. However, parameters MAY also be passed using the OAuth 2.0 request syntax even when a Request Object is used; this would typically be done to enable a cached, pre-signed (and possibly pre-encrypted) Request Object value to be used containing the fixed request parameters, while parameters that can vary with each request, such as state and nonce, are passed as OAuth 2.0 parameters.

4.1. Passing a Request Object by Value

The Client sends the Authorization Request as a Request Object to the Authorization Endpoint as the "request" parameter value.

The following is a non-normative example of an Authorization Request using the "request" parameter (with line wraps within values for display purposes only):

```
  https://server.example.com/authorize?
    response_type=code%20id_token
    &client_id=s6BhdRkqt3
    &redirect_uri=https%3A%2F%2Fclient.example.org%2Fcb
    &scope=openid
    &state=af0ifjsldkj
    &nonce=n-0S6_WzA2Mj
    &request=eyJhbGciOiJSUzI1NiIsImtpZCI6ImsyYmRjIn0.ew0KICJpc3MiOiA
    iczZCaGRSa3F0MyIsDQogImF1ZCI6ICJodHRwczovL3NlcnZlci5leGFtcGxlLmN
    vbSIsDQogInJlc3BvbnNlX3R5cGUiOiAiY29kZSBpZF90b2tlbiIsDQogImNsaWV
    udF9pZCI6ICJzNkJoZFJrcXQzIiwNCiAicmVkaXJlY3RfdXJpIjogImh0dHBzOi8
    vY2xpZW50LmV4YW1wbGUub3JnL2NiIiwNCiAic2NvcGUiOiAib3BlbmlkIiwNCiA
    ic3RhdGUiOiAiYWYwaWZqc2xka2oiLA0KICJub25jZSI6ICJuLTBTNl9XekEyTWo
    iLA0KICJtYXhfYWdlIjogODY0MDAsDQogImNsYWltcyI6IA0KICB7DQogICAidXN
    lcmluZm8iOiANCiAgICB7DQogICAgICJnaXZlbl9uYW1lIjogeyJlc3NlbnRpYWw
    iOiB0cnVlfSwNCiAgICAgIm5pY2tuYW1lIjogbnVsbCwNCiAgICAgImVtYWlsIjo
    geyJlc3NlbnRpYWwiOiB0cnVlfSwNCiAgICAgImVtYWlsX3ZlcmlmaWVkIjogeyJ
    lc3NlbnRpYWwiOiB0cnVlfSwNCiAgICAgInBpY3R1cmUiOiBudWxsDQogICAgfSw
    NCiAgICJpZF90b2tlbiI6IA0KICAgIHsNCiAgICAgImdlbmRlciI6IG51bGwsDQo
    gICAgICJiaXJ0aGRhdGUiOiB7ImVzc2VudGlhbCI6IHRydWV9LA0KICAgICAiYWN
    yIjogeyJ2YWx1ZXMiOiBbInVybjptYWNlOmluY29tbW9uOmlhcDpzaWx2ZXIiXX0
    NCiAgICB9DQogIH0NCn0.nwwnNsk1-ZkbmnvsF6zTHm8CHERFMGQPhos-EJcaH4H
    h-sMgk8ePrGhw_trPYs8KQxsn6R9Emo_wHwajyFKzuMXZFSZ3p6Mb8dkxtVyjoy2
    GIzvuJT_u7PkY2t8QU9hjBcHs68PkgjDVTrG1uRTx0GxFbuPbj96tVuj11pTnmFC
    UR6IEOXKYr7iGOCRB3btfJhM0_AKQUfqKnRlrRscc8Kol-cSLWoYE9l5QqholImz
    jT_cMnNIznW9E7CDyWXTsO70xnB4SkG6pXfLSjLLlxmPGiyon_-Te111V8uE83Il
    zCYIb_NMXvtTIVc1jpspnTSD7xMbpL-2QgwUsAlMGzw
```

4.2. Passing a Request Object by Reference

The "request_uri" Authorization Request parameter enables OAuth authorization requests to be passed by reference, rather than by value. This parameter is used identically to the "request" parameter, other than that the Request Object value is retrieved from the resource at the specified URL, rather than passed by value.

When the "request_uri" parameter is used, the OAuth 2.0 authorization request parameter values contained in the referenced JWT supersede those passed using the OAuth 2.0 request syntax. However, parameters MAY also be passed using the OAuth 2.0 request syntax even when a "request_uri" is used; this would typically be done to enable a cached, pre-signed (and possibly pre-encrypted) Request Object value to be used containing the fixed request parameters, while parameters

that can vary with each request, such as "state" and "nonce", are passed as OAuth 2.0 parameters.

Servers MAY cache the contents of the resources referenced by Request URIs. If the contents of the referenced resource could ever change, the URI SHOULD include the base64url encoded SHA-256 hash as defined in FIPS180-2 [FIPS180-2] of the referenced resource contents as the fragment component of the URI. If the fragment value used for a URI changes, that signals the server that any cached value for that URI with the old fragment value is no longer valid.

The entire Request URI MUST NOT exceed 512 ASCII characters. There are three reasons for this restriction.

1. Many WAP / feature phones do not accept large payloads. The restriction are typically either 512 or 1024 ASCII characters.

2. The maximum URL length supported by Internet Explorer is 2083 ASCII characters.

3. On a slow connection such as 2G mobile connection, a large URL would cause the slow response and using such is not advisable from the user experience point of view.

The contents of the resource referenced by the URL MUST be a Request Object. The scheme used in the "request_uri" value MUST be "https", unless the target Request Object is signed in a way that is verifiable by the Authorization Server. The "request_uri" value MUST be reachable by the Authorization Server, and SHOULD be reachable by the Client.

The following is a non-normative example of the contents of a Request Object resource that can be referenced by a "request_uri" (with line wraps within values for display purposes only):

```
eyJhbGciOiJSUzI1NiIsImtpZCI6ImsyYmRjIn0.ew0KICJpc3MiOiAiczZCaGRSa3
F0MyIsDQogImF1ZCI6ICJodHRwczovL3NlcnZlci5leGFtcGxlLmNvbSIsDQogInJl
c3BvbnNlX3R5cGUiOiAiY29kZSBpZF90b2tlbiIsDQogImNsaWVudF9pZCI6ICJzNk
JoZFJrcXQzIiwNCiAicmVkaXJlY3RfdXJpIjogImh0dHBzOi8vY2xpZW50LmV4YW1w
bGUub3JnL2NiIiwNCiAic2NvcGUiOiAib3BlbmlkIiwNCiAic3RhdGUiOiAiYWYwaW
Zqc2xka2oiLA0KICJub25jZSI6ICJuLTBTNl9XekEyTWoiLA0KICJtYXhfYWdlIjog
ODY0MDAsDQogImNsYWltcyI6IA0KICB7DQogICAidXNlcmluZm8iOiANCiAgICB7DQ
ogICAgICJnaXZlbl9uYW1lIjogeyJlc3NlbnRpYWwiOiB0cnVlfSwNCiAgICAgIm5p
Y2tuYW1lIjogbnVsbCwNCiAgICAgImVtYWlsIjogeyJlc3NlbnRpYWwiOiB0cnVlfS
wNCiAgICAgImVtYWlsX3ZlcmlmaWVkIjogeyJlc3NlbnRpYWwiOiB0cnVlfSwNCiAg
ICAgInBpY3R1cmUiOiBudWxsDQogICAgfSwNCiAgICJpZF90b2tlbiI6IA0KICAgIH
sNCiAgICAgImdlbmRlciI6IG51bGwsDQogICAgICJiaXJ0aGRhdGUiOiB7ImVzc2Vu
dGlhbCI6IHRydWV9LA0KICAgICAiYWNyIjogeyJ2YWx1ZXMiOiBbInVybjptYWNlOm
luY29tbW9uOmlhcDpzaWx2ZXIiXX0NCiAgICB9DQogIH0NCn0.nwwnNsk1-Zkbmnvs
F6zTHm8CHERFMGQPhos-EJcaH4Hh-sMgk8ePrGhw_trPYs8KQxsn6R9Emo_wHwajyF
KzuMXZFSZ3p6Mb8dkxtVyjoy2GIzvuJT_u7PkY2t8QU9hjBcHs68PkgjDVTrG1uRTx
0GxFbuPbj96tVuj11pTnmFCUR6IEOXKYr7iGOCRB3btfJhM0_AKQUfqKnRlrRscc8K
ol-cSLWoYE9l5QqholImzjT_cMnNIznW9E7CDyWXTsO70xnB4SkG6pXfLSjLLlxmPG
iyon_-Te111V8uE83IlzCYIb_NMXvtTIVc1jpspnTSD7xMbpL-2QgwUsAlMGzw
```

4.2.1. URL Referencing the Request Object

The Client stores the Request Object resource either locally or remotely at a URL the Server can access. This URL is the Request URI, "request_uri".

If the Request Object includes requested values for Claims, it MUST NOT be revealed to anybody but the Authorization Server. As such, the "request_uri" MUST have appropriate entropy for its lifetime. It is RECOMMENDED that it be removed if it is known that it will not be used again or after a reasonable timeout unless access control measures are taken.

The following is a non-normative example of a Request URI value (with line wraps within values for display purposes only):

```
https://client.example.org/request.jwt#
  GkurKxf5T0Y-mnPFCHqWOMiZi4VS138cQO_V7PZHAdM
```

4.2.2. Request using the "request_uri" Request Parameter

The Client sends the Authorization Request to the Authorization Endpoint.

The following is a non-normative example of an Authorization Request using the "request_uri" parameter (with line wraps within values for display purposes only):

```
  https://server.example.com/authorize?
    response_type=code%20id_token
    &client_id=s6BhdRkqt3
    &request_uri=https%3A%2F%2Fclient.example.org%2Frequest.jwt
    %23GkurKxf5T0Y-mnPFCHqWOMiZi4VS138cQO_V7PZHAdM
    &state=af0ifjsldkj
```

4.2.3. Authorization Server Fetches Request Object

Upon receipt of the Request, the Authorization Server MUST send an HTTP "GET" request to the "request_uri" to retrieve the referenced Request Object, unless it is already cached, and parse it to recreate the Authorization Request parameters.

Note that the client SHOULD use a unique URI for each request utilizing distinct parameters, or otherwise prevent the Authorization Server from caching the "request_uri".

The following is a non-normative example of this fetch process:

```
  GET /request.jwt HTTP/1.1
  Host: client.example.org
```

5. Validating JWT-Based Requests

5.1. Encrypted Request Object

The Authorization Server MUST decrypt the JWT in accordance with the JSON Web Encryption [RFC7516] specification. The result MAY be either a signed or unsigned (plaintext) Request Object. In the former case, signature validation MUST be performed as defined in Section 5.2.

The Authorization Server MUST return an error if decryption fails.

5.2. Signed Request Object

To perform Signature Validation, the "alg" Header Parameter in the JOSE Header MUST match the value of the "request_object_signing_alg" set during Client Registration or a value that was pre-registered by other means. The signature MUST be validated against the appropriate key for that "client_id" and algorithm.

The Authorization Server MUST return an error if signature validation fails.

5.3. Request Parameter Assembly and Validation

The Authorization Server MUST assemble the set of Authorization Request parameters to be used from the Request Object value and the OAuth 2.0 Authorization Request parameters (minus the "request" or "request_uri" parameters). If the same parameter exists both in the Request Object and the OAuth Authorization Request parameters, the parameter in the Request Object is used. Using the assembled set of Authorization Request parameters, the Authorization Server then validates the request as specified in OAuth 2.0 [RFC6749].

6. Authorization Server Response

Authorization Server Response is created and sent to the client as in Section 4 of OAuth 2.0 [RFC6749] .

In addition, this document defines additional error values as follows:

invalid_request_uri	The "request_uri" in the Authorization Request returns an error or contains invalid data.
invalid_request_object	The request parameter contains an invalid Request Object.
request_not_supported	The Authorization Server does not support the use of the "request" parameter.
request_uri_not_supported	The Authorization Server does not support use of the "request_uri" parameter.

7. IANA Considerations

The request_object_signing_alg OAuth Dynamic Client Registration Metadata is pending registration by OpenID Connect Dynamic Registration specification.

8. Security Considerations

In addition to the all the security considerations discussed in OAuth 2.0 [RFC6819], the following security considerations SHOULD be taken into account.

When sending the authorization request object through "request" parameter, it SHOULD be signed with then considered appropriate

algorithm using [RFC7515]. The "alg=none" SHOULD NOT be used in such a case.

If the request object contains personally identifiable or sensitive information, the "request_uri" MUST be of one-time use and MUST have large enough entropy deemed necessary with applicable security policy. For higher security requirement, using [RFC7516] is strongly recommended.

9. Acknowledgements

Follwoing people contributed to the creation of this document in OAuth WG.

Michael B. Jones (Microsoft), Axel Nenker(DT), Sergey Beryozkin, Jim Manico, (add yourself).

Following people contributed to creating this document through the OpenID Connect 1.0 [OpenID.Core].

Breno de Medeiros (Google), Hideki Nara (TACT), Ryo Itou (Yahoo! Japan), George Fletcher (AOL), Justin Richer (MITRE), Edmund Jay (Illumila), Michael B. Jones (Microsoft), (add yourself).

In addition following people contributed to this and previous versions through The OAuth Working Group.

David Recordon (Facebook), Luke Shepard (Facebook), James H. Manger (Telstra), Marius Scurtescu (Google), John Panzer (Google), Dirk Balfanz (Google), (add yourself).

10. Revision History

-06

- Added explanation on the 512 chars URL restriction.

- Updated Acknowledgements.

-05

- More alignment with OpenID Connect.

-04

- Fixed typos in examples. (request_url -> request_uri, cliend_id -> client_id)

- Aligned the error messages with the OAuth IANA registry.

- Added another rationale for having request object.

-03

- Fixed the non-normative description about the advantage of static signature.

- Changed the requirement for the parameter values in the request itself and the request object from 'MUST MATCH" to 'Req Obj takes precedence.

-02

- Now that they are RFCs, replaced JWS, JWE, etc. with RFC numbers.

-01

- Copy Edits.

11. References

11.1. Normative References

[FIPS180-2]
U.S. Department of Commerce and National Institute of Standards and Technology, "Secure Hash Signature Standard", FIPS 180-2, August 2002.

Defines Secure Hash Algorithm 256 (SHA256)

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <http://www.rfc-editor.org/info/rfc6749>.

[RFC6819] Lodderstedt, T., Ed., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", RFC 6819, DOI 10.17487/RFC6819, January 2013, <http://www.rfc-editor.org/info/rfc6819>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <http://www.rfc-editor.org/info/rfc7159>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <http://www.rfc-editor.org/info/rfc7515>.

[RFC7516] Jones, M. and J. Hildebrand, "JSON Web Encryption (JWE)", RFC 7516, DOI 10.17487/RFC7516, May 2015, <http://www.rfc-editor.org/info/rfc7516>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <http://www.rfc-editor.org/info/rfc7518>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <http://www.rfc-editor.org/info/rfc7519>.

11.2. Informative References

[OpenID.Core] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0", February 2014.

Authors' Addresses

Nat Sakimura (editor)
Nomura Research Institute
1-6-5 Marunouchi, Marunouchi Kitaguchi Bldg.
Chiyoda-ku, Tokyo 100-0005
Japan

Phone: +81-3-5533-2111
Email: n-sakimura@nri.co.jp
URI: http://nat.sakimura.org/

John Bradley
Ping Identity
Casilla 177, Sucursal Talagante
Talagante, RM
Chile

Phone: +44 20 8133 3718
Email: ve7jtb@ve7jtb.com
URI: http://www.thread-safe.com/