Introduction to the FAPI Read & Write OAuth Profile

2018-05-15

Nat Sakimura(@_nat_en)

OpenID® Foundation
Chairman of the board

NRI
Research Fellow

• OpenID® is a registered trademark of the OpenID Foundation.
• *Unless otherwise noted, all the photos and vector images are licensed by GraphicStocks.
OAuth is a framework – needs to be profiled

This framework was designed with the clear expectation that future work will define prescriptive profiles and extensions necessary to achieve full web-scale interoperability.

The OAuth 2.0 Authorization Framework

Abstract

The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction
Which OAuth?
<table>
<thead>
<tr>
<th>Draft name</th>
<th>Rev.</th>
<th>Dated</th>
<th>Status</th>
<th>Obsoleted by/(Updated by)</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-oauth- jwt-bcp</td>
<td>-00</td>
<td>2017-07-19</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-mtls</td>
<td>-04</td>
<td>2017-10-12</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-security-topics</td>
<td>-03</td>
<td>2017-09-10</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-token-binding</td>
<td>-05</td>
<td>2017-10-27</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-token-exchange</td>
<td>-09</td>
<td>2017-07-03</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-pop-key-distribution</td>
<td>-03</td>
<td>2017-02-24</td>
<td>Expired</td>
<td></td>
</tr>
<tr>
<td>IESG Processing:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-discovery</td>
<td>-07</td>
<td>2017-09-07</td>
<td>Waiting for Writeup</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-jwsreq</td>
<td>-15</td>
<td>2017-07-21</td>
<td>IESG Evaluation: AD Followup</td>
<td></td>
</tr>
</tbody>
</table>

Published:

<table>
<thead>
<tr>
<th>Draft name</th>
<th>Rev.</th>
<th>Dated</th>
<th>Status</th>
<th>Obsoleted by/(Updated by)</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-oauth-amc-values</td>
<td>-08</td>
<td>2017-03-13</td>
<td>RFC 8176</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-assertions</td>
<td>-18</td>
<td>2014-10-21</td>
<td>RFC 7521</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-dyn-reg</td>
<td>-30</td>
<td>2015-05-28</td>
<td>RFC 7591</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-dyn-reg-management</td>
<td>-15</td>
<td>2015-05-05</td>
<td>RFC 7592</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-introspection</td>
<td>-11</td>
<td>2015-07-04</td>
<td>RFC 7662</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth- jws-token</td>
<td>-32</td>
<td>ipr 2014-12</td>
<td>RFC 7519</td>
<td>(RFC 7797)</td>
</tr>
<tr>
<td>draft-ietf-oauth-jwt-bearer</td>
<td>-12</td>
<td>2014-11-12</td>
<td>RFC 7523</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-native-apps</td>
<td>-12</td>
<td>2017-06-09</td>
<td>RFC 8252</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-proof-of-possession</td>
<td>-11</td>
<td>2015-12-19</td>
<td>RFC 7800</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-revocation</td>
<td>-11</td>
<td>2013-07-13</td>
<td>RFC 7069</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-saml2-bearer</td>
<td>-23</td>
<td>2014-11-12</td>
<td>RFC 7522</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-sptop</td>
<td>-15</td>
<td>2015-07-10</td>
<td>RFC 7636</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-urn-sub-ns</td>
<td>-06</td>
<td>2012-07-16</td>
<td>RFC 6755</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-v2</td>
<td>-31</td>
<td>ipr 2012-08</td>
<td>RFC 6749</td>
<td>(RFC 8252)</td>
</tr>
<tr>
<td>draft-ietf-oauth-v2-bearer</td>
<td>-23</td>
<td>ipr 2012-08</td>
<td>RFC 6750</td>
<td></td>
</tr>
<tr>
<td>draft-ietf-oauth-v2-threatmodel</td>
<td>-08</td>
<td>2012-10-06</td>
<td>RFC 6819</td>
<td></td>
</tr>
</tbody>
</table>
That creates specification to take care of medium to high risk API access security.

<table>
<thead>
<tr>
<th>Value of the resource</th>
<th>Environment control level</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

- **Closed circuit Factory application**: Basic choices ok.
- **Financial API – Read & Write**: Basic choices NOT OK
- **Financial API – Read only**: Basic choices NOT OK
- **Social sharing**: Basic choices ok.

No need to satisfy all the security requirements by OAuth
That can serve all financial transactions including PSD2, but not limited to.
FAPI Security Profile is a general purpose higher security API protection mechanism based on OAuth framework.
It has been adopted by Open Banking UK

Open Banking forms collaboration with OpenID Foundation

The Open Banking Implementation Entity (OBIE), the organisation responsible for the open API banking standard, today announces its collaboration with the OpenID Foundation’s Financial API Working Group.

CMA Appoints New Trustee for Open Banking Implementation Entity

The Competition & Markets Authority (‘CMA’) has, today, announced that Imran Gulamhuseinwala will become the new trustee for the Open Banking Implementation Entity (the ‘IE’).
9 Major banks in UK went live on January, 2018

(Source) Chris Mitchel, “Banking is now more open”, Identify 2017

(OB Roadmap)

Australia adopting the same profile
It is also recommended by the Japanese Banker’s association

US FS-ISAC aligning their security requirements
... and major IAM vendors are implementing it
Submit to ISO/TC 68 and is a part of the forthcoming technical specification
We have issued two implementer's drafts.

- **Closed circuit Factory application**
- **Financial API**
  - Read & Write
- **Financial API**
  - Read only
- **Social sharing**

Basic choices ok.
Which are redirect approach

- **Part 1: Read Only Security Profile**
- **Part 2: Read and Write Security Profile**

Redirect Approach
Decoupled Approach
Embedded Approach
While RFC6749 is not complete with source, destination, and message authentication,

<table>
<thead>
<tr>
<th></th>
<th>Sender AuthN</th>
<th>Receiver AuthN</th>
<th>Message AuthN</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthZ Req</td>
<td>Indirect</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>AuthZ Res</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Token Req</td>
<td>Weak</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Token Res</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
</tbody>
</table>

© 2017 by Nat Sakimura. CC-BY-SA.
FAPI Part 2 is complete with source, destination, and message authentication.

- By using OpenID Connect’s Hybrid Flow and Request Object, you are pretty well covered.

<table>
<thead>
<tr>
<th></th>
<th>Sender AuthN</th>
<th>Receiver AuthN</th>
<th>Message AuthN</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthZ Req</td>
<td>Request Object</td>
<td>Request Object</td>
<td>Request object</td>
</tr>
<tr>
<td>AuthZ Res</td>
<td>Hybrid Flow</td>
<td>Hybrid Flow</td>
<td>Hybrid Flow</td>
</tr>
<tr>
<td>Token Req</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Token Res</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
</tr>
</tbody>
</table>
Tokens are Sender Constrained instead of being bearer

<table>
<thead>
<tr>
<th>Security Levels</th>
<th>Token Types</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sender Constrained Token</td>
<td>Only the entity that was issued can use the token.</td>
</tr>
<tr>
<td></td>
<td>Bearer Token</td>
<td>Stolen tokens can also be used</td>
</tr>
</tbody>
</table>
These are in the form of check lists.

5.2 Read and Write API Security Provisions

5.2.1 Introduction

Read and Write access carries higher financial risk; therefore the protection level required is higher than Read-Only access.

As a profile of The OAuth 2.0 Authorization Framework, this document mandates the following for the Read and Write API of the FAPI.

5.2.2 Authorization Server

The authorization server shall support the provisions specified in clause 5.2.2 of Financial API - Part 1: Read-Only API Security Profile.

In addition, the authorization server, for the Write operation,

1. shall require the request or request_uri parameter to be passed as a JWS signed JWT as in clause 6 of OIDC;
2. shall require the response_type values code id_token or code id_token token;
3. shall return ID Token as a detached signature to the authorization response;
4. shall include state hash, s_hash, in the ID Token to protect the state value;
5. shall only issue holder of key authorization code, access token, and refresh token for write operations;
6. shall support OAuth or MTLS as a holder of key mechanism;
7. shall support user authentication at LoA 3 or greater as defined in X.1254;
8. shall support signed ID Tokens; and
9. should support signed and encrypted ID Token.

(source) https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_002.md

© 2017 by Nat Sakimura. CC-BY-SA.
8.5 TLS Considerations

As confidential information is being exchanged, all interactions shall be encrypted with TLS (HTTPS).

Section 7.1 of Financial API - Part 1: Read Only API Security Profile shall apply, with the following additional requirements:

1. Only the following 4 cipher suites shall be permitted:
   - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

8.6 JWS Algorithm Considerations

JWS signatures shall use the PS256 or ES256 algorithms for signing.

(source) https://bitbucket.org/openid/fapi/src/master/Financial_API_WD_002.md
And now working on the decoupled approach ...

CIBA (client initiated backchannel authentication) profile.

https://bitbucket.org/openid/fapi/src/master/Financial_API WD_CIBA.md
Embedded Approach

- Giving bearer credentials to a third party is a bad idea.
- GDPR explicit consent for third party data transfer?
  - What would be the liability implications?
- Perhaps per app “password”?
We have other works as well…

E.g. The OpenBanking OpenID Dynamic Client Registration Specification
... and perhaps

**Intent registration endpoint**

Pushing the intent, e.g., to send $1,000 to Bob’s account

Intent ID

AuthZ Req w/Intent ID

AuthZ Response

Redirect URI

Client

Intent Registration EP

Authorization EP

Token EP

Server
How can we tell that the implementation conforms to the specification?
Once it passes the test, the implementer can self-certify and publish.

- That gets the implementers under the premise of the article 5 of the FTC Act.
- The log will be openly available so others can also find out false claims.

By the way
New Name for WG?
After all, there is nothing specifically “Financial”
It is a general purpose High Security API protection protocol
Some of the candidates …

- Fully Assured Protection Interoperable
- Fair Assurance Protection Interface
- Full Assurance Protection Interface
- Full Assurance Profile Interface (FAPI) WG
- Plus …