



OWASP

Open Web Application
Security Project

OWASP Portland Chapter

Welcome to OWASP Portland's
monthly chapter meeting!



OWASP

Open Web Application
Security Project

Twitter: @PortlandOWASP

Website: pdxowasp.org

Meetup: <https://www.meetup.com/OWASP-Portland-Chapter/>

Slack: [#chapter-pdx](https://owasp.slack.com)



OWASP

Open Web Application
Security Project

Next Chapter Meeting: Aug

Graph Theory for Security

Presented by Timothy Morgan

August 13th 2019 from 6–8pm

Hosted by: Simple 120 SE Clay St, Floor 2

Follow the Portland OWASP Meetup, Twitter, or email list for further details!



OWASP

Open Web Application
Security Project

Project Focus: Amass

- In-depth DNS Enumeration and Network Mapping!

Information Gathering Techniques Used

- DNS, Scraping, Certificates, APIs, Web Archives

https://www.owasp.org/index.php/OWASP_Amass_Project

<https://github.com/OWASP/Amass>



OWASP

Open Web Application
Security Project

Become A Member

- Support Web Application Security Education
- Get involved in OWASP Projects
- Direct Your Membership Dues to Your Home Chapter or Project You Care About

<https://www.owasp.org/index.php/Membership>

THE EASY (AND SECURE!) WAY TO BUILD JAVASCRIPT WEB APPS WITH OAUTH 2 & OIDC



Introduction

- Jake Feasel
- Developer Experience lead engineer at ForgeRock
- **AppAuthHelper** : <https://www.npmjs.com/package/appauthhelper>
- Wrapper for AppAuth for JS to assist with the full OAuth2 / OIDC token life-cycle.
- **OIDCSessionCheck**: <https://www.npmjs.com/package/oidcsessioncheck>
- JavaScript library to assist with binding sessions between an OIDC OP and RP



Context

- JavaScript or "Single Page" applications
- OAuth 2 client / OIDC relying party
- REST calls to Resource Server Endpoints
- Client app driven by the resource owner



Best Current Practices

Important security concerns for web clients



Which Grant to Use: Implicit or Authorization Code?

- <https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-3.1.2>
- *The implicit grant (response type "token") ... [is] vulnerable to access token leakage and access token replay...*
- *[C]lients SHOULD NOT use the implicit grant (response type "token")...*
- *Clients SHOULD instead use the response type "code" (aka authorization code grant type)*



PKCE for non-Mobile?

- <https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-3.1.1>
- *Clients utilizing the authorization grant type MUST use PKCE [RFC7636] in order to (with the help of the authorization server) detect and prevent attempts to inject (replay) authorization codes into the authorization response.*
- *Note: although PKCE so far was recommended as a mechanism to protect native apps, this advice applies to all kinds of OAuth clients, including web applications.*



Renewing tokens

- **HTTP/1.1 401 Unauthorized**
- WWW-Authenticate: Bearer realm="example",
- error="invalid_token",
- error_description="The access token expired"



Use a Refresh Token?

- Server side Clients Use These
- Why Not Front-End Apps?
- Refresh Tokens Live For a Long Time
- Less Is More
- You May Not Need It



Silent Authz Code Grant in iFrames

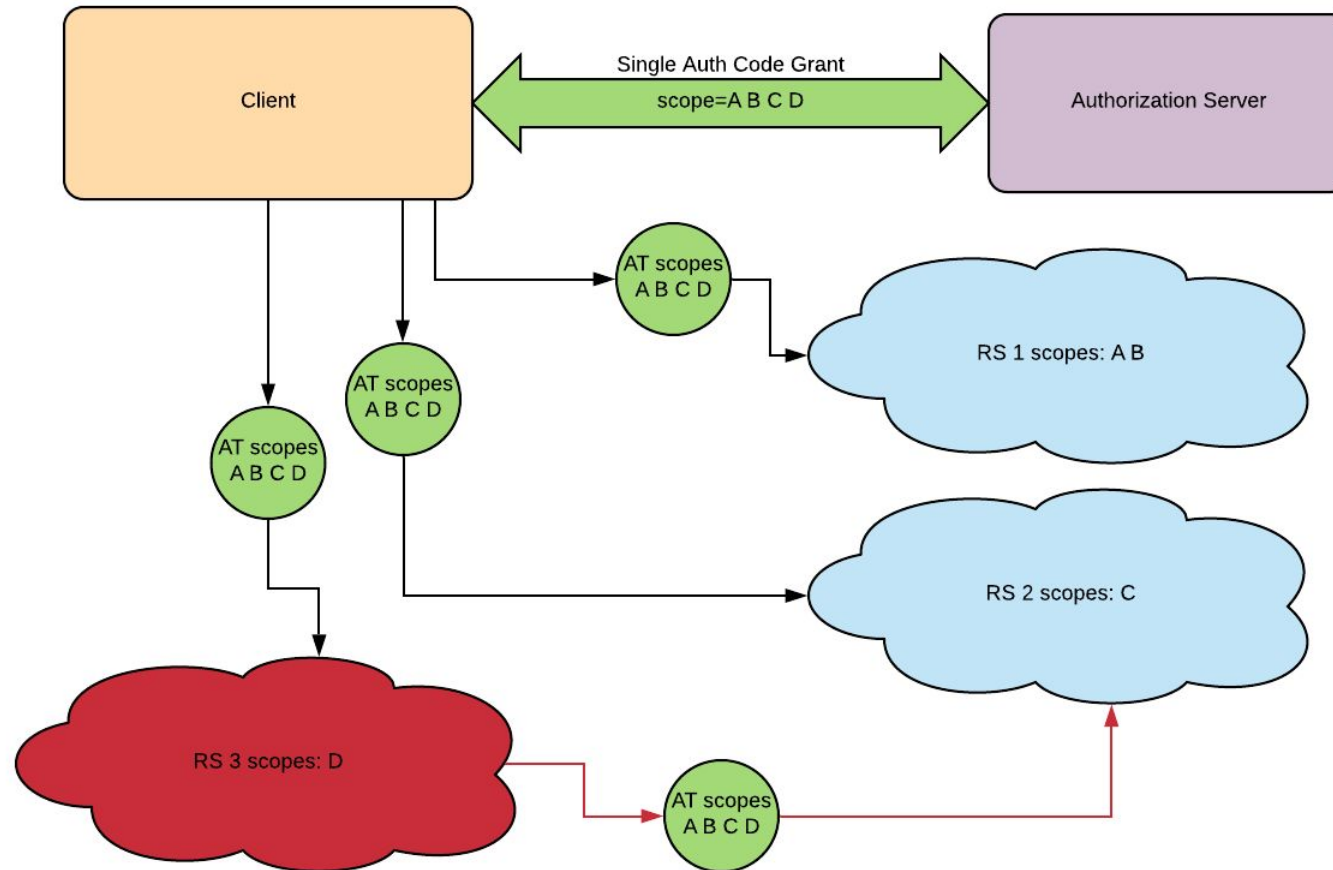
- Established session in the AS
- Scope consent has to have been saved
- Access token lifetime shorter than the AS session lifetime.
- Access-token-bearing requests in the same browser as the AS session cookie.
- Include `prompt=none` in the call to the authorization endpoint

Make the request in a hidden iFrame

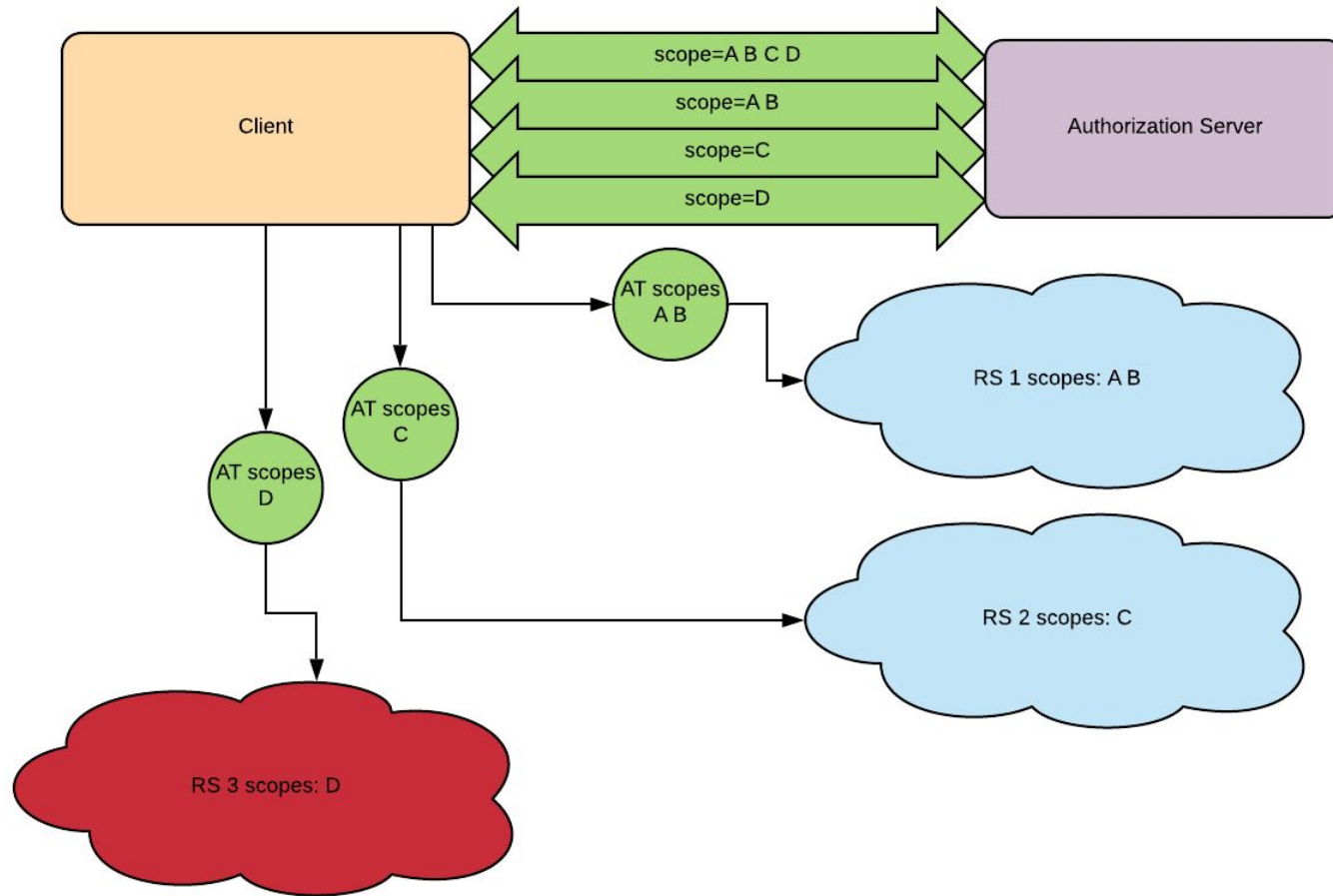


Access Token Leakage

- <https://tools.ietf.org/html/draft-ietf-oauth-security-topics-12#section-4.8>



Counter-measure for token leakage

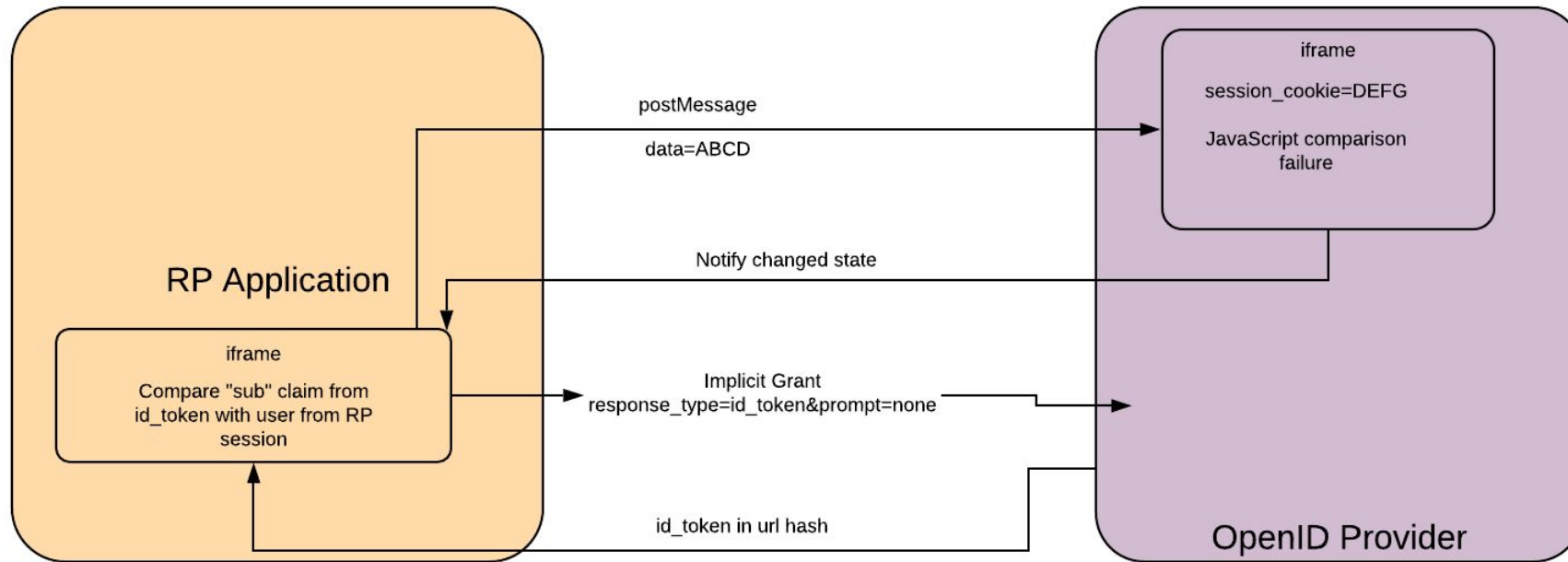


IDP-Initiated Logout

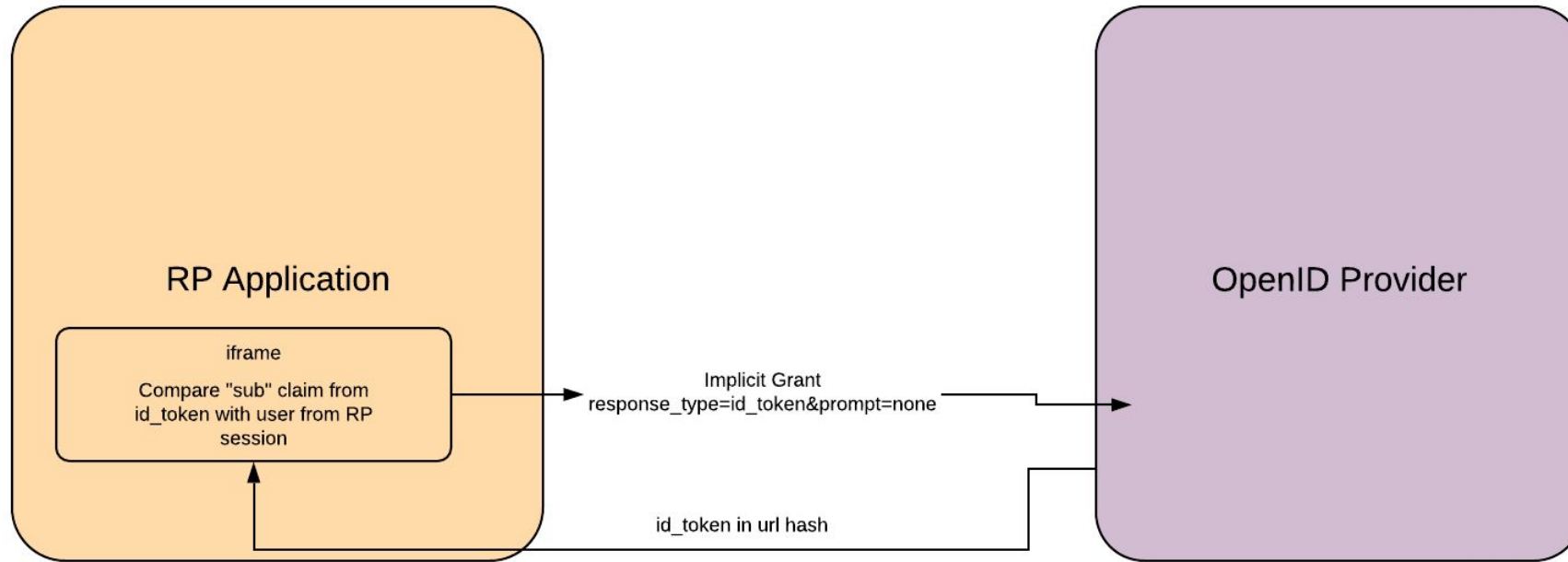
- https://openid.net/specs/openid-connect-session-1_0.html
- *To do so, it is **possible to repeat the Authentication Request with prompt=none**. However, this causes network traffic and this is **problematic on the mobile devices that are becoming increasingly popular**. Therefore, once the session is established with the Authentication Request and Response, it is desirable to be able to check the login status at the OP without causing network traffic by **polling a hidden OP iframe from an RP iframe with an origin restricted postMessage** as follows....*



OIDC Spec Session Monitoring Proposal



OIDC Session Monitoring Simplified



Libraries to make it easy

Tools you can use today



OIDCSessionCheck

- <https://www.npmjs.com/package/oidcsession>
- ```
var sessionCheck = new SessionCheck({
 clientId: "myClientId",
 opUrl: "https://login.sample.forgeops.com/oauth2/authorize",
 subject: claims.sub,
 invalidSessionHandler: function () {
 logout();
 },
 cooldownPeriod: 5
});

// check with every captured event
document.addEventListener("click", function () {
 sessionCheck.triggerSessionCheck();
});
document.addEventListener("keypress", function () {
 sessionCheck.triggerSessionCheck();
});
```



# AppAuth



## AppAuth

Native App SDK for OAuth 2.0 and  
OpenID Connect implementing modern  
best practices

[AppAuth for Android](#)

[AppAuth for iOS and macOS](#)

[AppAuth for JS](#)

- Open Source (Apache 2.0)
- Backed by Google
- PKCE
- JS version is generic (not just for browser apps)



# AppAuthHelper

- <https://www.npmjs.com/package/appauthhelper>
- ```
AppAuthHelper.init({  
  clientId: "appAuthClient",  
  authorizationEndpoint: "https://default.iam.example.com/am/oauth2/authorize",  
  tokenEndpoint: "https://default.iam.example.com/am/oauth2/access_token",  
  revocationEndpoint: "https://default.iam.example.com/am/oauth2/token/revoke",  
  endSessionEndpoint: "https://default.iam.example.com/am/oauth2/endSession",  
  resourceServers: {  
    "https://default.iam.example.com/am/oauth2/userinfo": "profile",  
    "https://default.iam.example.com/rs": "custom_scope1 custom_scope2"  
  },  
  tokensAvailableHandler: function (claims) {  
    // Start making RS requests  
    // fetch("https://default.iam.example.com/am/oauth2/userinfo").then(...)  
  }  
});  
AppAuthHelper.getTokens();
```



RS requests are easy, right?

```
• var deferred = $.ajax({  
•   url: "https://rs.example.com/me",  
•   headers: {  
•       "Authorization": "Bearer " + getAccessToken()  
•   }  
• });
```



What about expired tokens?

```
. var deferred = $.Deferred() ,  
.   requestDetails = function (token) {  
.     return {  
.       url: "https://rs.example.com/me",  
.       headers: {  
.         "Authorization": "Bearer " + getAccessToken()  
.       }  
.     };  
.   };  
  
. $.ajax(requestDetails()).then(deferred.resolve, function (jqXHR) {  
.   if (getAuthHeaderError(jqXHR) === "invalid_token") {  
.     refreshAccessToken().then(function () {  
.       $.ajax(requestDetails())  
.         .then(deferred.resolve, deferred.reject);  
.       }, deferred.reject);  
.   } else {  
.     deferred.reject(jqXHR);  
.   }  
. }
```

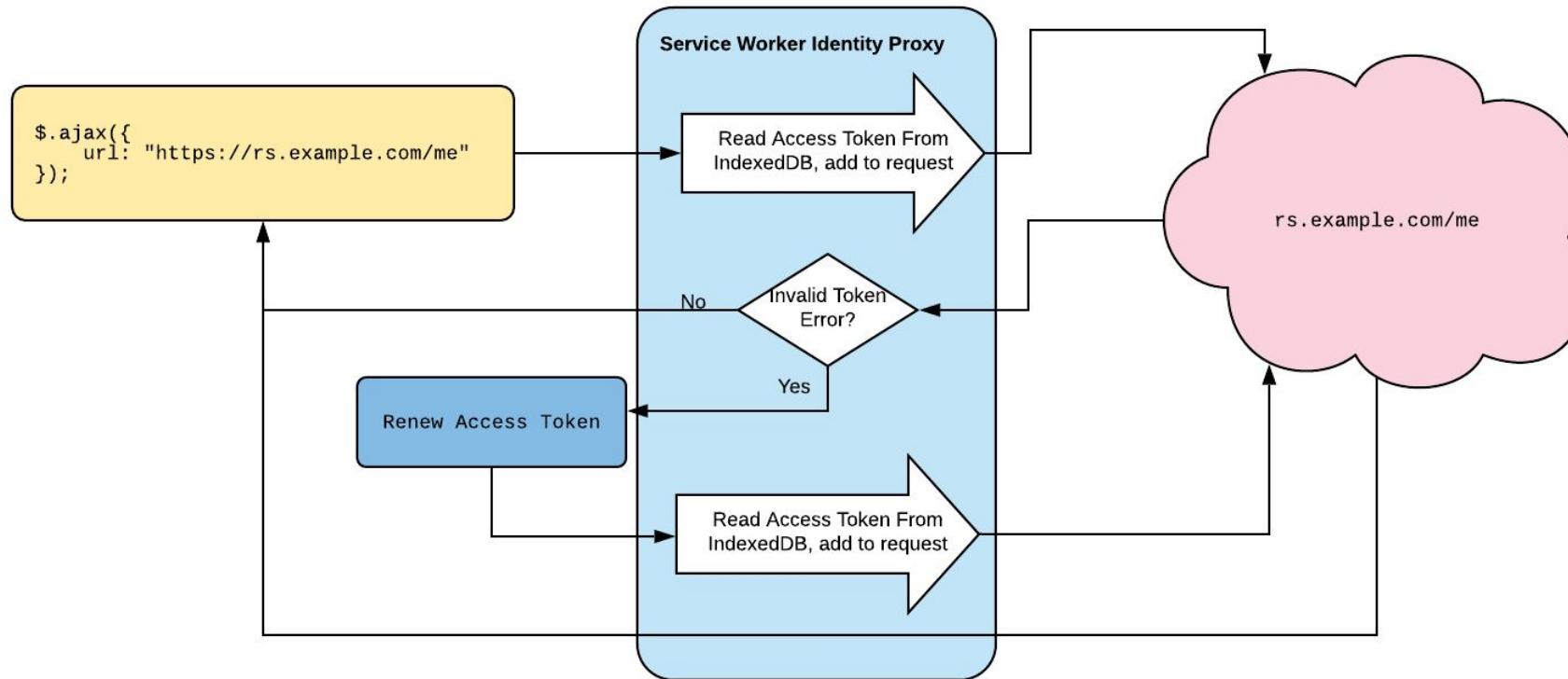


What if it wasn't your problem?

- `var deferred = $.ajax({`
- `url: "https://rs.example.com/me"`
- `});`



Service Worker as an Identity Proxy



```
resourceServers: {  
  "https://default.iam.example.com/am/oauth2/userinfo": "profile email",  
  "https://default.iam.example.com/me": "custom_scope1 custom_scope2"  
},
```



Service Worker Code Sample

```
self.addEventListener("fetch", (event) => {  
  if (self.appAuthConfig &&  
      typeof self.appAuthConfig.resourceServers === "object" &&  
      Object.keys(self.appAuthConfig.resourceServers).length) {  
    var resourceServer = Object.keys(self.appAuthConfig.resourceServers)  
      .filter((rs) => event.request.url.indexOf(rs) === 0)[0];  
    if (resourceServer) {  
      event.respondWith(new Promise((resolve, reject) => {  
        self.addAccessTokenToRequest(event.request, resourceServer)  
          .then((rsRequest) => fetch(rsRequest))  
          .then((resp) => {  
            // Watch for retry-able errors as described by https://tools.ietf.org/html/rfc6750#section-3  
            if (!resp.ok && self.getAuthHeaderDetails(resp.headers)["error"] === "invalid_token") {  
              let promise = self.waitForRenewedToken(resourceServer)  
                .then(() => self.addAccessTokenToRequest(event.request, resourceServer))  
                .then((freshRSRequest) => fetch(freshRSRequest));  
              self.messageChannel.postMessage({  
                "message": "renewTokens",  
                "resourceServer": resourceServer  
              });  
              return promise;  
            } else {  
              return resp;  
            }  
          })  
          .then(resolve, reject);  
        }  
      }  
    }  
  }  
  return resp;  
});
```



Demo

Walk-through of an example application




```
tokensAvailableHandler: function (claims) {
    Promise.all([
        fetch("https://rs.sample.forgeops.com/openidm/info/login").then((resp) => resp.json())
    ]).then((responses) => {
        document.getElementById('userDetails').innerText = JSON.stringify({
            "info/login": responses[0]
        }, null, 4);
    });
}
```

```
{
  "info/login": {
    "_id": "login",
    "authenticationId": "user.0",
    "authorization": {
      "component": "managed/user",
      "authLogin": false,
      "adminUser": "openig",
      "roles": [
        "internal/role/openidm-authorized"
      ],
      "ipAddress": "192.168.99.1",
      "authenticationId": "openig",
      "id": "c39ab2bc-346d-48e1-883e-7171af12567e",
      "moduleId": "STATIC_USER"
    }
  }
}
```

Status	Method	Domain	File
304	GET	localhost:8888	/
304	GET	localhost:8888	appAuthHelperBundle.js
404	GET	localhost:8888	favicon.ico
200	GET	localhost:8888	appAuthHelperRedirect.html
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js
302	GET	login.sample.forgeo...	authorize?redirect_uri=http://localhost:8888/appAuthHelperRedi...
200	GET	localhost:8888	appAuthHelperRedirect.html?code=zqJL4s7mf9kvPrbr_qZHL4Sv7...
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js
200	POST	login.sample.forgeo...	access_token
302	GET	login.sample.forgeo...	authorize?redirect_uri=http://localhost:8888/appAuthHelperRedi...
200	GET	localhost:8888	appAuthHelperRedirect.html?code=nAukxDj3Ulj2N5x286jOTAed...
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js
200	POST	login.sample.forgeo...	access_token
200	GET	rs.sample.forgeops....	login
200	GET	rs.sample.forgeops....	login



The screenshot shows the Chrome DevTools Network tab. A list of network requests is visible on the left, with the following details:

Sta	Me	Do...	File	Cause	Ty	Tra...	S	o ms
30	G...	L...	/	docu...	h...	cached	2.1	1 ms
30	G...	L...	appAuthHelperB...	script	js	cached	72	1 ms
40	G...	L...	favicon.ico	img	x...	cached	0	1
20	G...	L...	appAuthHelperR...	subd...	h...	cached	1.	1 ms
20	G...	L...	appAuthHelperF...	script	js	cached	0	1
30	G...	L...	authorize?redire...	subd...		621 B	0	27 ms
20	G...	L...	appAuthHelperR...	subd...	h...	1.58 ...	1.	1 ms
20	G...	L...	appAuthHelperF...	script	js	cached	0	1
20	P...	L...	access_token	fetch	j...	1.46 ...	1.	38 ms
30	G...	L...	authorize?redire...	subd...		621 B	0	12 ms
20	G...	L...	appAuthHelperR...	subd...	h...	1.58 ...	1.	1 ms
20	G...	L...	appAuthHelperF...	script	js	cached	0	1
20	P...	L...	access_token	fetch	j...	1.40 ...	1.	27 ms
20	G...	r...	login	fetch	j...	903 B	29	135 ms
20	G...	r...	login	fetch	j...	servi...	29	

The right pane shows the 'Params' tab for the selected request, displaying the following query string parameters:

- redirect_uri: http://localhost:8888/appAuthHelperRedirect.html
- client_id: appAuthClient
- response_type: code
- state: QrBVmglamY
- scope: openid profile openid
- prompt: none
- code_challenge: 6J_pYxU6Y-YJULwBLuDg9nOoWJxC0DqP4A8PGV578P0
- code_challenge_method: S256



Referrer Policy: no-referrer-when-downgrade

Filter headers

▼ Response headers (621 B)

```
HTTP/2.0 302 Found
server: nginx/1.15.9
date: Thu, 20 Jun 2019 20:32:53 GMT
content-length: 0
location: http://localhost:8888/appAuthHelperRedirect.html?code=zqJL4s7mf9kvPrbr_qZHl4Sv7Yk&iss=https%3A%2F%2F
x-frame-options: SAMEORIGIN
pragma: no-cache
cache-control: no-store
accept-ranges: bytes
vary: Accept-Charset, Accept-Encoding, Accept-Language, Accept
access-control-allow-origin: *
access-control-allow-methods: PUT,GET,POST,HEAD,PATCH,DELETE
access-control-allow-headers: authorization,x-requested-with
X-Firefox-Spdy: h2
```

▼ Request headers (855 B)

```
Host: login.sample.forgeops.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://localhost:8888/
Connection: keep-alive
Cookie: route=59372b3ea79657f7c765171526fdef07a57509; amlbcookie=01; iPlanetDirectoryPro=Qamslikf2RkZoZIVAPe
Upgrade-Insecure-Requests: 1
```



Sta	Me	Do...	File	Cause	Ty	Tra...	S	0 ms	Headers	Cookies	Params	Response	Timings	Sta
30	G...	l...	/	docu...	h...	cached	2.1	1 ms	Filter request parameters					
30	G...	l...	appAuthHelperB...	script	js	cached	72	1 ms	▼ Form data					
40	G...	l...	favicon.ico	img	x...	cached	0	l	grant_type: authorization_code					
20	G...	l...	appAuthHelperR...	subd...	h...	cached	1.		client_id: appAuthClient					
20	G...	l...	appAuthHelperF...	script	js	cached	0	l	redirect_uri: http://localhost:8888/appAuthHelperRedirect.html					
30	G...	l...	authorize?redire...	subd...			621 B	0 27 ms	code: zqJL4s7mf9kvPrbr_qZHL4Sv7Yk					
20	G...	l...	appAuthHelperR...	subd...	h...		1.58 ...	1. 1 ms	code_verifier: 7HDNRVYjLAsvID6LEdtX8it61uWqWv9jFliXtBUYyCK7xF9YGyPFRDts5T0cDjEllgNXYi					
20	G...	l...	appAuthHelperF...	script	js	cached	0	l						
20	P...	l...	access_token	fetch	j...		1.46 ...	1. 38 ms						
30	G...	l...	authorize?redire...	subd...			621 B	0 12 ms						
20	G...	l...	appAuthHelperR...	subd...	h...		1.58 ...	1. 1 ms						
20	G...	l...	appAuthHelperF...	script	js	cached	0	l						
20	P...	l...	access_token	fetch	j...		1.40 ...	1. 27 ms						
20	G...	r...	login	fetch	j...		903 B	29 135 ms						
20	G...	r...	login	fetch	j...	servi...	29							



Sta	Me	Do...	File	Cause	Ty	Tra...	S	0 ms	Headers	Cookies	Params	Response	Timings	Stack Trace	Sec
30	G...	L...	/	docu...	h...	cached	2	1 ms	Filter properties						
30	G...	L...	appAuthHelperB...	script	js	cached	72	1 ms	JSON						
40	G...	L...	favicon.ico	img	x...	cached	0								
20	G...	L...	appAuthHelperR...	subd...	h...	cached	1								
20	G...	L...	appAuthHelperF...	script	js	cached	0								
30	G...	L...	authorize?redire...	subd...		621 B	0	27 ms							
20	G...	L...	appAuthHelperR...	subd...	h...	1.58 ...	1	1 ms							
20	G...	L...	appAuthHelperF...	script	js	cached	0								
20	P...	L...	access_token	fetch	j...	1.46 ...	1	38 ms							
30	G...	L...	authorize?redire...	subd...		621 B	0	12 ms							
20	G...	L...	appAuthHelperR...	subd...	h...	1.58 ...	1	1 ms							

```

access_token: LAqelsVbc8sEF5B3OpEA4HG_vie
scope: openid profile
id_token: eyJ0eXAiOiJKV1QiLCJraWQoIj3VTNpZkLjYUxPVUFSZVJCL0ZHNmVNMVAXL
6ZXg2Z01EcDRod3M0SllCSHJGUStInN1Yil6lnVzZXluMCIslmF1ZGl0VHJhY2tpbi
YzU4ZTQxMTViMS00MjQ1IiwiaXNzIjoiaHR0cHM6Ly9sb2dpbi5zYW1wbGUuZm
mlkX3Rva2VuliwiZ2l2ZW5fbmFtZSI6IkFhY2NmliwiYXVkljoiYXBwQXV0aENsaW
WczMFEiLCJhY3IiOiIiwiaWib3JnLmZvcmdlcm9jay5vcGVuaWRjb25uZWN0Lm9wc
aW1lIjoxNTYxMDYyMzAxLCJyYW1lIjoiQWFiY2YgQW1hcilslJlYWxtIjoiLyIsImV
VG9rZW4iLCJmYW1pbHlfbmFtZSI6IkFtYXNzIjYXQoIjE1NjEwNj13NzN9.U5lgi!
MHR-E4aOC4bPBOPXUAi6mS6C5u-
uTK952tRCikC5GINRwVdCq_LDoy85Q3Ec84gBL9CaKp2L_QELZYO4y189pYLaLj.
zxG7X_XfJqp_yMqn5JwTMD7MENP7-
XEx8TKnVAJkRIASGffjTIWczj_hkA9FQAtAtMQCay1o_OdQ_9GNk8nrvAplS3_XX
m2sWUAzFxyiysQVHIU1JH36TrXRFgerpXgaN0ldHIU06ZUtP8g

token_type: Bearer
expires_in: 3599

```



St...	M...	Domain	File	Cause	Type	Transfe...	Siz	0 ms	▶	Headers	Cookies	Params	Respons
304	GET	local...	/	document	html	cached	2...	1 ms		Filter request parameters			
304	GET	local...	appAuthHelperBundle.js	script	js	cached	7...	1 ms		▼ Query string			
404	GET	local...	favicon.ico	img	x-icon	cached	0 B			redirect_uri: http://localhost:8888/appAuthHelper			
200	GET	local...	appAuthHelperRedirect.html	subdocu...	html	cached	1...			client_id: appAuthClient			
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B			response_type: code			
302	GET	login...	authorize?redirect_uri=http...	subdocu...		621 B	0 B	27 ms		state: fyUe7ZQBNV			
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms		scope: openid			
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B			prompt: none			
200	POST	login...	access_token	fetch	json	1.46 KB	1...	38 ms		code_challenge: vatuqoCcm1QuVtv75D4WhzmnC			
302	GET	login...	authorize?redirect_uri=http...	subdocu...		621 B	0 B	12 ms		code_challenge_method: S256			
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms					
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B						
200	POST	login...	access_token	fetch	json	1.40 KB	1...	27 ms					
200	GET	rs.sa...	login	fetch	json	903 B	2...	135 ms					
200	GET	rs.sa...	login	fetch	json	service ...	2...						



St...	M...	Domain	File	Cause	Type	Transfe...	Siz	0 ms	Headers	Cookies	Params	Response	Timings	Stack
304	GET	local...	/	document	html	cached	2...	1 ms	Filter properties					
304	GET	local...	appAuthHelperBundle.js	script	js	cached	7...	1 ms	JSON					
404	GET	local...	favicon.ico	img	x-icon	cached	0 B		access_token: e1ue6sWk82QQNHid7ZOCcTedT_w			scope: openid		
200	GET	local...	appAuthHelperRedirect.html	subdocu...	html	cached	1...		id_token: eyJ0eXAiOiJKV1QiLCJraWQiOiJ3VTNpZkLjYUxPVUFSZVJCL0ZlYjU0Q1BCb2NMVXlqdylsInN1YiI6InVzZXIuMCIsImF1ZGl0VHJhY2MjU4liwiaXNzIjoiaHR0cHM6Ly9sb2dpbi5zYW1wbGUuZm9yZ2VvQXV0aENsaWVudCIsImNfaGFzaCI6IlNxcF9DUTFoHkbnRmeIN2wcyI6IjRURkthRm8ya1VsTldMc0dSdThnMk52WGl1cyIsInF...					
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B		9RWF82ZmRvZmciLCJhenAiOiJhcHBhdXRoQ2xpZW50IiwiaXV0eINRva2VuVHlwZSI6IkpXVFRva2VuliwiaWF0IjoxNTYxMDYyNzczG1AXR7Qu0cggaJJjD5F3jc32IVb0o8LgUaAeoNGFP68Tkd1e0YNol					
302	GET	login....	authorize?redirect_uri=http...	subdocu...		621 B	0 B	27 ms	aU79e1F6f29t4BdKhrCruNUN95oMzr6pMHCu88DDVSsSLNMZtV					
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms	WGtbVTDCDxcZKhVudMVbZxNmIhEVdVwA4JJu7-_f4xWHStemu					
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B		token_type: Bearer			expires_in: 3599		
200	POST	login....	access_token	fetch	json	1.46 KB	1...	38 ms	Response payload					
302	GET	login....	authorize?redirect_uri=http...	subdocu...		621 B	0 B	12 ms	1					
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms	{ "access_token": "e1ue6sWk82QQNHid7ZOCcTedT_w", "scop					
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B							
200	POST	login....	access_token	fetch	json	1.40 KB	1...	27 ms						
200	GET	rs.sa...	login	fetch	json	903 B	2...	135 ms						
200	GET	rs.sa...	login	fetch	json	service ...	2...							



St...	M...	Domain	File	Cause	Type	Transfe...	Siz	0 ms	Headers	Cookies	Params	Response	Timings	Security
304	GET	local...	/	document	html	cached	2...	1 ms	Request URL: https://rs.sample.forgeops.com/openidm/info/login Request method: GET Remote address: 192.168.99.100:443 Status code: 200 OK ? Version: HTTP/2.0 Referrer Policy: no-referrer-when-downgrade					
304	GET	local...	appAuthHelperBundle.js	script	js	cached	7...	1 ms						
404	GET	local...	favicon.ico	img	x-icon	cached	0 B							
200	GET	local...	appAuthHelperRedirect.html	subdocu...	html	cached	1...							
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B		Filter headers					
302	GET	login...	authorize?redirect_uri=http...	subdocu...		621 B	0 B	27 ms	Response headers (681 B)					
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms	Request headers (377 B) Accept: */* Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.5 Authorization: Bearer e1ue6sWk82QQNHid7ZOCcTedT_w Connection: keep-alive Host: rs.sample.forgeops.com Origin: http://localhost:8888 Referer: http://localhost:8888/ User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/67.0					
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B							
200	POST	login...	access_token	fetch	json	1.46 KB	1...	38 ms						
302	GET	login...	authorize?redirect_uri=http...	subdocu...		621 B	0 B	12 ms						
200	GET	local...	appAuthHelperRedirect.ht...	subdocu...	html	1.58 KB	1...	1 ms						
200	GET	local...	appAuthHelperFetchToken...	script	js	cached	0 B							
200	POST	login...	access_token	fetch	json	1.40 KB	1...	27 ms						
200	GET	rs.sa...	login	fetch	json	903 B	2...	135 ms						
200	GET	rs.sa...	login	fetch	json	service ...	2...							



Inspector Console Debugger Style Editor Performance Memory Network Storage Accessibility

Cache Storage Cookies Indexed DB Local Storage Session Storage

http://localhost:8888

appAuth (default)

appAuthClient

Key	Value
tokens	{"idToken":"eyJ0eXAiOiJKV1QiLCJraWQiOiJ3VTNpZk1pLCJ1b2N0b3R5IjoiYXNjaWkiLCJhdWQiOiJ1b2N0b3R5IiwiaXNjaWkiOiJ1b2N0b3R5In0="}

Filter items

Filter values

Data

tokens: {"idToken":"eyJ0eXAiOiJKV1QiLCJraWQiOiJ3VTNpZk1pLCJ1b2N0b3R5IjoiYXNjaWkiLCJhdWQiOiJ1b2N0b3R5IiwiaXNjaWkiOiJ1b2N0b3R5In0="}

Parsed Value

tokens: Object

idToken: "eyJ0eXAiOiJKV1QiLCJraWQiOiJ3VTNpZk1pLCJ1b2N0b3R5IjoiYXNjaWkiLCJhdWQiOiJ1b2N0b3R5IiwiaXNjaWkiOiJ1b2N0b3R5In0="

accessToken: "bhBwdlzVRfNkgfFXqCjho8EQn1k"

https://rs.sample.forgeops.com/openidm: "ekR2A5bi7VSubc9fEzIdQId56l"

__proto__: Object



Request URL: https://rs.sample.forgeops.com/openidm/info/login

Request method: GET

Remote address: 192.168.99.100:443

Status code: 401 Unauthorized ⓘ

Version: HTTP/2.0

Referrer Policy: no-referrer-when-downgrade

Filter headers

▼ Response headers (697 B)

HTTP/2.0 401 Unauthorized

server: nginx/1.15.9

date: Thu, 20 Jun 2019 21:00:23 GMT

content-length: 0

set-cookie: INGRESSCOOKIE=f9714211a5c6084e034bbcb6bcd3b981; Path=/; Secure; HttpOnly

www-authenticate: Bearer realm="OpenIG",error_description="The access token provided is expired, revoked, malformed, or invalid for other reasons.",error="invalid_token"



Status	Method	Domain	File	Headers	Cookies	Params	Response	Timings
304	GET	localhost:8888	/					
304	GET	localhost:8888	appAuthHelperBundle.js					
404	GET	localhost:8888	favicon.ico					
200	GET	localhost:8888	appAuthHelperRedirect.html					
401	GET	rs.sample.forgeops.com	login					
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js					
302	GET	login.sample.forgeops.com	authorize?redirect_uri=http://localhost:8888/a...					
200	GET	localhost:8888	appAuthHelperRedirect.html?code=tE8zYjIZ1x...					
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js					
200	POST	login.sample.forgeops.com	access_token					
200	GET	rs.sample.forgeops.com	login					
200	GET	rs.sample.forgeops.com	login					



Filter URLs

All

HT

Status	Method	Domain	File
304	GET	localhost:8888	/
304	GET	localhost:8888	appAuthHelperBundle.js
404	GET	localhost:8888	favicon.ico
200	GET	localhost:8888	appAuthHelperRedirect.html
401	GET	rs.sample.forgeops.com	login
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js
302	GET	login.sample.forgeops.com	authorize?redirect_uri=http://localhost:8888/a...
200	GET	localhost:8888	appAuthHelperRedirect.html?code=tE8zYjIZ1x...
200	GET	localhost:8888	appAuthHelperFetchTokensBundle.js
200	POST	login.sample.forgeops.com	access_token
200	GET	rs.sample.forgeops.com	login
200	GET	rs.sample.forgeops.com	login

Headers

Cookies

Params

Response

Timings

Security

Request URL: https://rs.sample.forgeops.com/openidm/info/login

Request method: GET

Remote address: 192.168.99.100:443

Status code: 200 OK ?

Version: HTTP/2.0

Referrer Policy: no-referrer-when-downgrade

Filter headers

Response headers (681 B)

Request headers (403 B)

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.5

Authorization: Bearer ekR2A5bi7VSubc9fEzldQlqd56I

Cache-Control: max-age=0

Connection: keep-alive

Host: rs.sample.forgeops.com

Origin: http://localhost:8888

Referer: http://localhost:8888/

TE: Trailers

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/67.0

A circular logo with a scalloped edge. Inside the circle, it says "CELEBRATING" at the top, "identiverse" in the middle, "10 YEARS" in a large font in the center, and "ANNIVERSARY" at the bottom.

The Identiverse logo, consisting of a stylized circular icon followed by the word "identiverse" in a sans-serif font.

- **AppAuthHelper** : <https://www.npmjs.com/package/appauthhelper>
- Wrapper for AppAuth for JS to assist with the full OAuth2 / OIDC token life-cycle.
- **OIDCSessionCheck**: <https://www.npmjs.com/package/oidcsessioncheck>
- JavaScript library to assist with binding sessions between an OIDC OP and RP
- Twitter: **@jakefeasel**
- <https://github.com/jakefeasel>
- <https://www.linkedin.com/in/jake-feasel/>



