

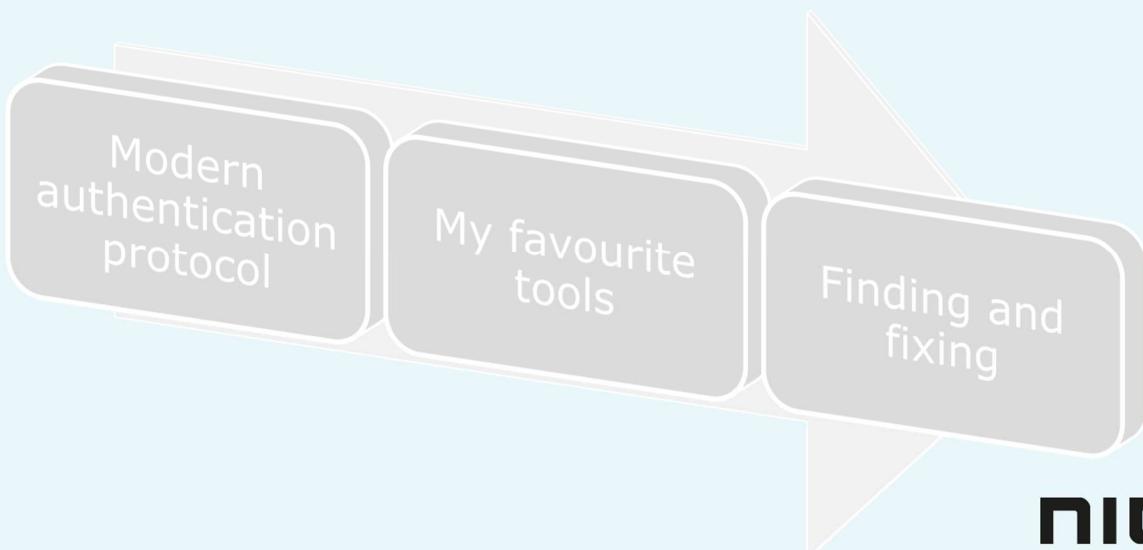


Troubleshooting Modern Authentication Protocols OAuth 2.0 & OpenID Connect

John Craddock
Identity and security architect, XTSeminars Ltd
johncra@xtseminars.co.uk @john_Craddock

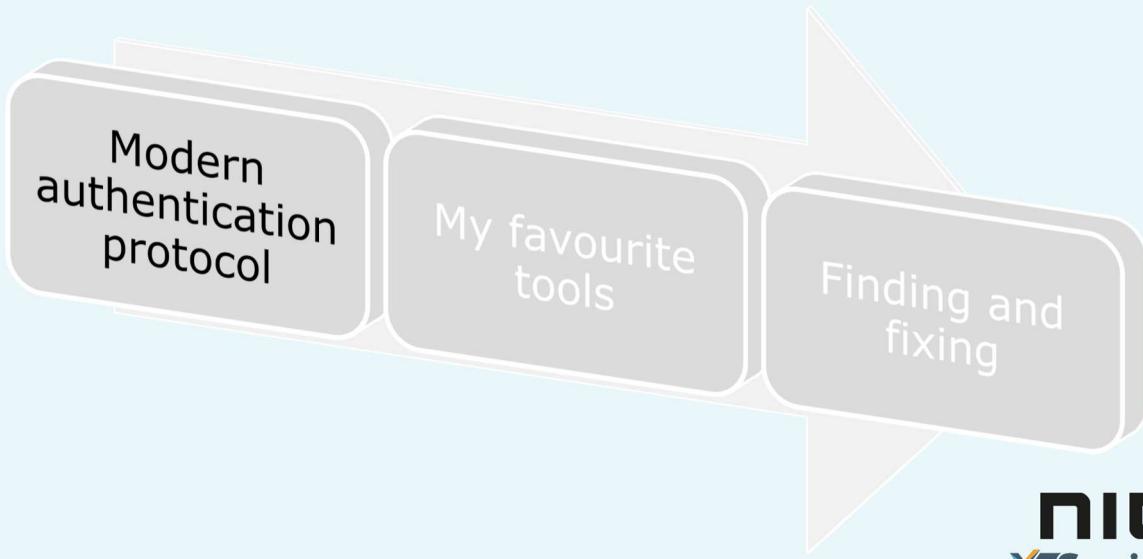
XTSeminars

What's in this session



nic
XTSeminars

What's in this session

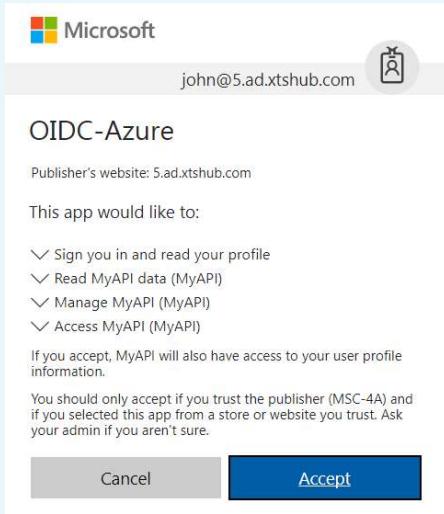


Modern authentication protocols

- OpenID Connect is an authentication protocol
 - Authenticates users to an application or service
 - The identity of the user is transported in an id_token
- Oauth 2.0 is an authorization protocol
 - Provides a mechanism to authorize one application to access protected resources either with its own identity or the identity of a user
 - If delegated access is configured, using the identity of a user, the user must "consent" to the access requested
 - Alternatively, consent can be given for all users by an administrator
 - The authorization data and identity are transported in an access_token
- OpenID Connect and OAuth2.0 supported by Azure AD and AD FS on Server 2016



Asking for consent



- Azure AD allows for user consent via the displaying the details of the request to the user
- A new Azure AD pattern is being developed for incremental consent
 - Look out for the V2 endpoints
- AD FS does not support a consent framework and administrator consent is assumed



JSON Web Token (JWT)

Header eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIiIng1dCI6Ik5H
VEZ2ZEStZnI0aEV1LTdgcHdBsk9NOW4QSj9...eyJhdW
QiOjodHRwczovL3h0c2VtaW5hcnMuY29tL0FQSS9NeX
NhbXBsZSImlzcyI6Imh0dBzOi8vc3RzLndpbmRvD3
MubmVOL2FmGE0NWM3LWmwODUUNGVyZl1hODY4LT
YyZlM5Mjc5MjZlZl8iLCjpxYXQjOjEzOTQ3MTE1MDAsIm5
IzIi6MTM5NDcxMTUwMCwiZXhwIjoxMzk0NzE1NDAwL
CJ2ZXlIiOixLjAilCj0aWQjOjhYjhNDVjY1jMDg1LTR
mM2YtYTg2OC02MmYzOTI3OTI2ZWVYiLCjvaWQjOj1M
GNIMDBmMC1IjFhLTQ5MWQtDhiNi0zNjQ3NDZjMzg
1NmQjLCj1cG4iOjqp2huqjH0c2VtaW5hcnMuY28udW
siLCj1bmIxWVfbmFtZS16ImpvaG5AeHRzZW1pbmFyc
y5jby51ayIsInN1YiIjF15Ep1OGtZEVFcXZVaGloak1I
QXNLrnV3OTINTVpDREtISmtJVjZYdEkILCjmyW1pbHif
bmFTZS16IkNyYWlk02Nrliwz2l2ZW5fbmFtZS16lkpv
G4iLCjchCBpZC16jhlnzjZmY4LWMLzjMtnDE3Ni05Zj
AOlTI0ZDBhNWIwNzE0YIsImFwlyWVnyIjoiMClsIn
NjcCI6InVzXJfaW1wZXJzb25hdGlvbIisImFjciI6IjEifQ.
ZG2Kaag2tnqYWBPnP0PggNgmVyh18zs1IXXW-
hGFMrQv0TosF2Em5QvaOBz2WUkeEWiw16XRo47nng
WgTtaD0vzPDxD0_AZhni5HbT6UmrmBEOd3tj5Si3z6
E5nbWB4KQZ4K7Lz_UhcMM3onD2uS0tyUKIzg-
zj4OjGgZPzYUfiDa72AH6esy-
adF7_HutB0zS6m35U97aUK6KOYs6F1-
qTn63gAZ_G5_MNpm9yICKBU1v2fktOwZMd7pQST8Y
Dz9QYm9p5BF-dHP1_nk2KCX-
1HWlbbtpSBFYInFyjb_q310iG7BXl2HAbouf_YXDA1J5
HDC1JcJca0xWVwkDQ

Body

```
{
  "aud": "https://graph.windows.net",
  "iss": "https://sts.windows.net/ab0a45c7-c085-4f3f-a868-62f3927926ef/",
  "iat": 1394710750,
  "nbf": 1394710750,
  "exp": 1394714650,
  "ver": "1.0",
  "tid": "ab0a45c7-c085-4f3f-a868-62f3927926ef",
  "oid": "50ce00f0-eb1a-491d-88b6-364746c3856d",
  "upn": "john@xtseminars.co.uk",
  "unique_name": "john@xtseminars.co.uk",
  "sub": "i9Q7DOmfN6x2R6RNQu1U1KV12jg9rKm9a9JNp1jQSpo",
  "puid": "10033FFF855525C2",
  "family_name": "Craddock",
  "given_name": "John",
  "appid": "92aaae6f-cbd0-4935-93a0-03fdbd540a7c",
  "appidacr": "1",
  "scp": "62e90394-69f5-4237-9190-012177145e10",
  "acr": "1"
}
```

- JWT mandated for the id_token, often used for the access_token

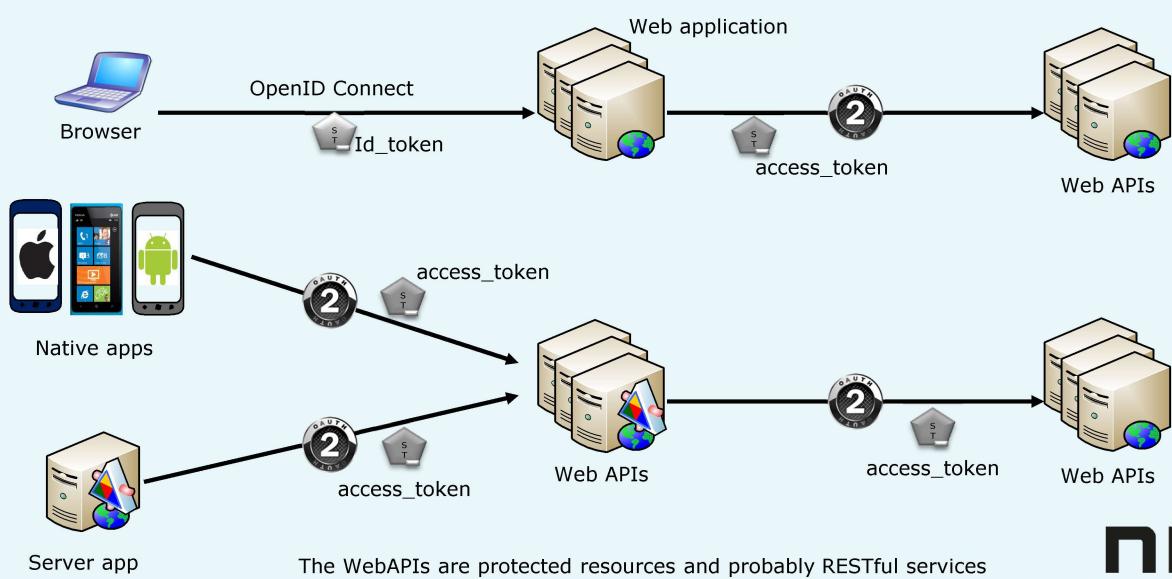


Validating the token

- The website/API **must** validate the token before authorizing access
 - Audience (aud) claim
 - Trusted issuer (iss)
 - Time validity: nbf, iat & exp
 - Trusted signature
 - Required authorization claims



Modern authentication scenarios



A word on terminology

- In the OAuth world the application (program) that requests the token(s) is called the client
- Microsoft refers to the “client” as “application” in Azure AD
 - AD FS uses “client”
- When tracing the protocol you will see client_id
- Different authentication flows can be configured to meet the needs of the different supported client types
 - In OAuth 2.0 terminology these are referred to as Grants

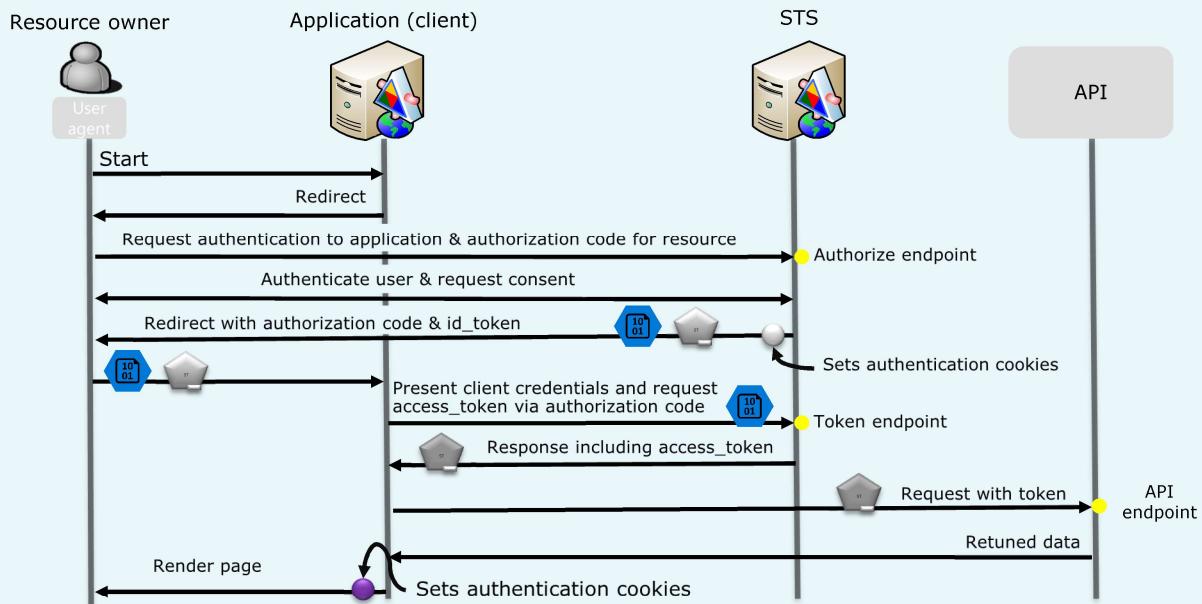


The OAuth 2.0 Grants (flows)

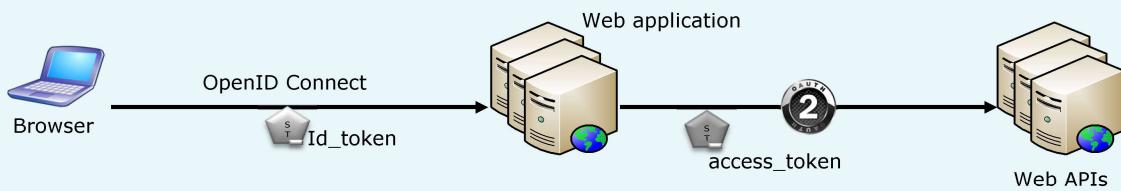
- **Web application client (Authorization Code Grant)**
 - Server side web application
- **Native / mobile client (Implicit Grant)**
 - Code runs locally
 - Can also use Authorization Code Grant
- **Trusted client (Resource Owner Password Credential Grant)**
 - Code runs locally on “trusted software”
- **Client to server communication authenticating with the client credentials (client credential Grant)**



Hybrid-flow - one of many flows



Demo environment



Security token service (STS)
AD FS or Azure AD

What's in this session



nic
XSeminars

Fiddler

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Go Stream Keep: All sessions Any Process Find Save Clear Cache Tearoff

#	Protocol	Host	URL	Body	Caching
1	200	HTTP	Tunnel to oidaeure.example.com:443	651	
2	200	HTTP	Tunnel to oidaeure.example.com:443	0	
3	200	HTTP	Tunnel to oidaeure.example.com:443	651	
4	200	HTTP	Tunnel to oidaeure.example.com:443	0	
5	200	HTTP	oidaeure.example.com	2,973	no-store
6	200	HTTP	Tunnel to login.microsoftonline.com.../2801e67da-4450-ad4-3dacecbfde17/login	19,938	no-cache
7	200	HTTP	POST /2801e67da-4450-ad4-3dacecbfde17/login HTTP/1.1		
8	200	HTTP	Cache-Control: max-age=0		
9	200	HTTP	Client		
10	401	HTTP	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8		
11	200	HTTP	Accept-Encoding: gzip, deflate		
12	200	HTTP	Accept-Language: en-US,en-US;q=0.9,en;q=0.8		
13	200	HTTPS	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/6		
14	401	HTTP	Cookies		
15	200	HTTP	AQDSSo=NAjNoExtension		
16	200	HTTP	bud=AGQAAEAAABHflmS_alkTSjzxRAtzuF931gRyG8ZBjQzJcJzLbZD0AnOnTwFsF5_MPxQz		
17	200	HTTP	esxtc=AQABAAAAAABHflmS_kTStjzxRAtzuF931gRyG8ZBjQzJcJzLbZD0AnOnTwFsF5_MPxQz		
18	200	HTTPS	login.microsoftonline.com.../common/instrumentation/	249	no-store
19	200	HTTP	login.microsoftonline.com.../common/instrumentation/	264	private
20	304	HTTP	login.microsoftonline.com.../common/instrumentation/	1,808	no-store
21	304	HTTP	login.microsoftonline.com.../common/instrumentation/	2,403	no-store
22	304	HTTPS	settings-win.data.microsoft.com.../settings/3.0/TELEMETRY...	0	
23	304	HTTPS	settings-win.data.microsoft.com.../settings/3.0/lu/app/ex...	0	

FiddlerOrchestrator Beta Log Timeline

Headers TextView SyntaxView WebForms HexView ODBC Federation Auth

Cookies Raw JSON XML

Request Headers [Raw] [Header Definitions]

Cache-Control: max-age=0

Client

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-US,en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/6

Cookies

Cookie

Transferring Headers TextView SyntaxView ImageView HexView WebView [CIBD]

Federation Auth Caching Cookies Raw JSON XML

Name Value

code AQQABAAIAABHflmS_gkTSjzxRAtzuF931gRyG8ZBjQzJcJzLbZD0AnOnTwFsF5_MPxQz

state 9999

session_state 0d3adbc-dce-4eb-5ebf-003dc-78a4f7

id_token.aud d7d3fb-dfb8-4de7-921b-2cabe3468

id_token.iss https://sts.windows.net/2801e67da-4450-ad4-3dacecbfde17/

id_token.iat 1516347656 (19/01/2018 07:40:56)

id_token.nbf 1516347656 (19/01/2018 07:40:56)

id_token.exp 1516351556 (19/01/2018 08:45:56)

id_token.aio Y2hjYLBLS7u4fD3xvpggdYlCneAtSZEvt+uLNy

id_token.amr pved,ria

Adding Inspectors

[http://identitymodel.codeplex.com
/releases/view/52187](http://identitymodel.codeplex.com/releases/view/52187)

[https://github.com/vibronet
/OInspector/tree/dev](https://github.com/vibronet/OInspector/tree/dev)

- www.telerik.com

NIC
XTSeminars

Postman

Many vendors supply Postman collections for testing their API

```

{
  "error": {
    "code": "MS_Authentication_ExpiredToken",
    "message": "Your access token has expired. Please renew it before submitting the request.",
    "lang": "en",
    "value": "Your access token has expired. Please renew it before submitting the request."
  },
  "date": "2018-01-19T08:16:17",
  "requestId": "00005d88-c38b-432c-ab09-a276aae89e70",
  "userId": null
}

```

- www.getpostman.com



Examining tokens jwt.io

<https://gallery.technet.microsoft.com/JWT-Token-Decode-637cf001>

```

{
  "headers": {
    "typ": "JWT",
    "alg": "RS256",
    "x5t": "z44wMdHu8WkKsumrbfaK98qxs5YI",
    "kid": "z44wMdHu8WkKsumrbfaK98qxs5YI"
  },
  "claims": {
    "aud": "https://graph.windows.net",
    "v": "https://sts.windows.net/28019ede-7bda-4450-adf4-3daecbfdfef1/",
    "iat": 1515934049,
    "nbf": 1515934049,
    "exp": 1515934300,
    "acr": "A",
    "aio": "AT0Ay/8GAAAu3U2lSkkuPp2zhw4M1ZPkZZL+SQ8VdxI1QyemXaJ8kyFYjZzcud6HVQwicGL",
    "aitecid": "5:10030000F69A3AC",
    "amr": [
      "pwd"
    ],
    "appid": "a8630b71-e5d4-4dab-81be-dca2bb244846",
    "appidcr": "",
    "email": "tom@partners.xtshub.com",
    "ipd": "https://sts.windows.net/3e224725-c942-45dc-8e96-d6a8b41c4691/",
    "ipaddr": "86.9.25.26",
    "name": "tom",
    "oid": "65f6ba31-5192-417c-bde3-68b5845496e1",
    "pid": "1003FFEA79334D5",
    "scp": "Directory.ReadWrite.All User.Read",
    "sub": "fju0e02_zwc4uomDzUfMKxDmDmMe11X5jmDnt2s",
    "tid": "28019ede-7bda-4450-adf4-3daecbfdfef1",
    "token_type": "jwt",
    "ut": "BMrfvdv4oEmpRajNEmgVAA",
    "utid": "BMrfvdv4oEmpRajNEmgVAA",
    "ver": "1.0"
  }
}

```

- Security sensitive tokens should not be decoded online

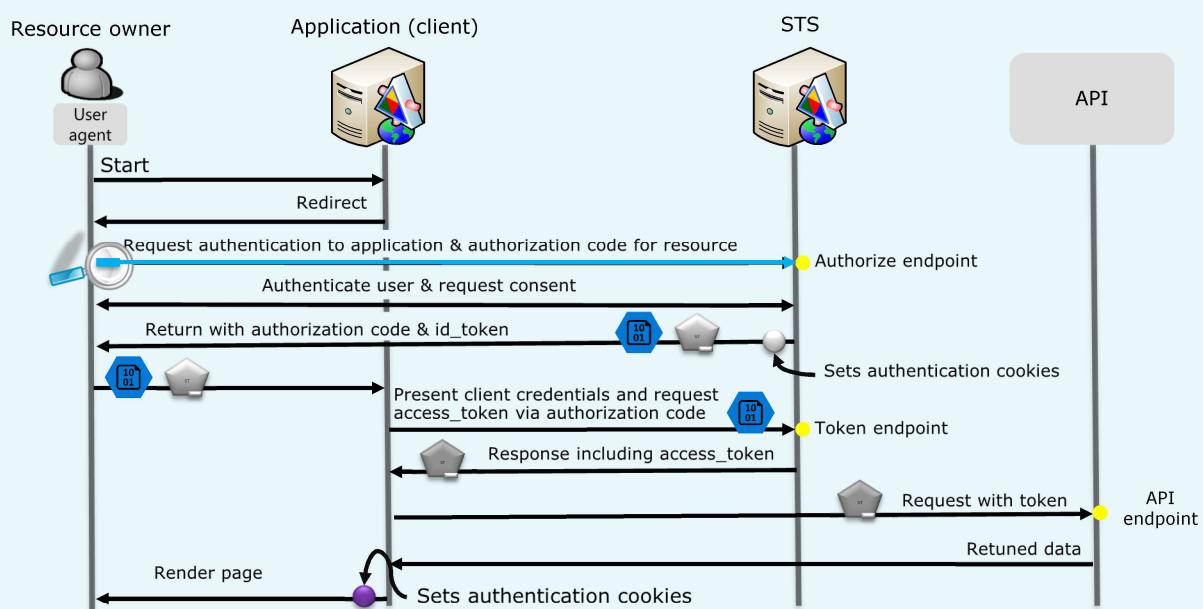


What's in this session

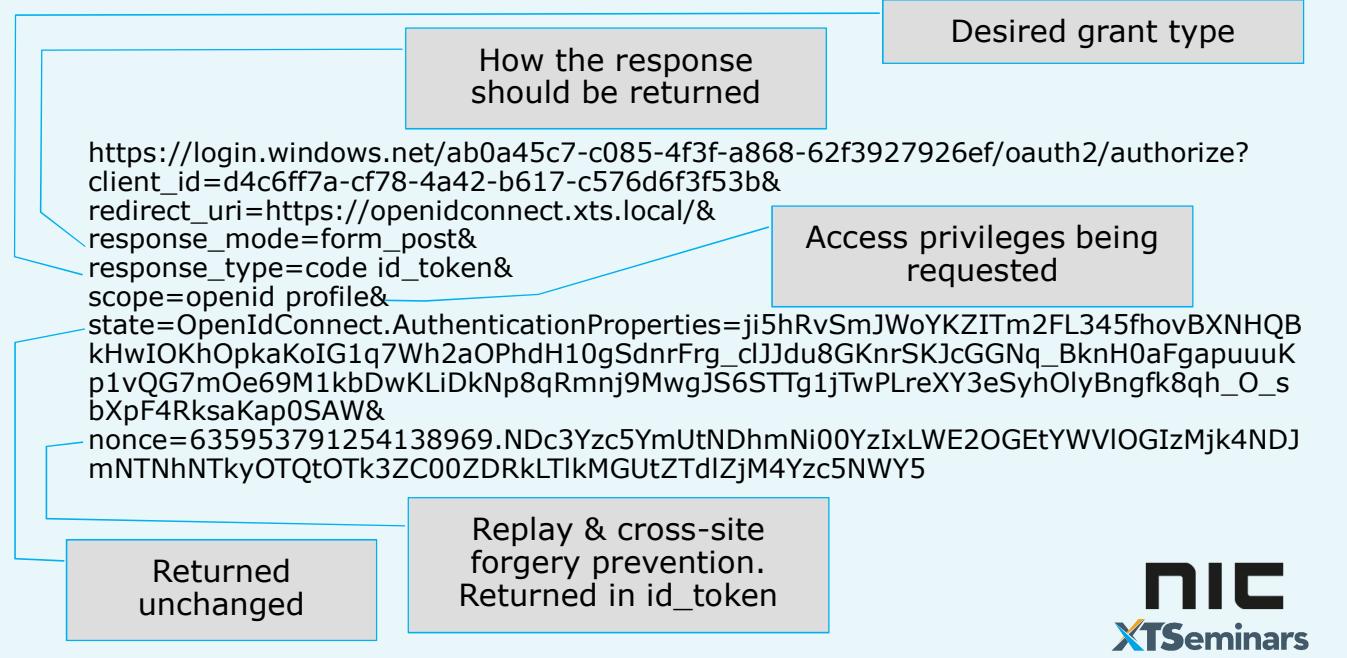


NIC
XTSeminars

1st Request to the STS



First redirect



Endpoints and more...

```
{
  "authorization_endpoint": "https://login.microsoftonline.com/2801cede-7bda-4450-adfa-3daecbfdf17/oauth2/v2.0/authorize",
  "token_endpoint": "https://login.microsoftonline.com/2801cede-7bda-4450-adfa-3daecbfdf17/oauth2/v2.0/token",
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post",
    "private_key_jwt"
  ],
  "jwks_uri": "https://login.microsoftonline.com/2801cede-7bda-4450-adfa-3daecbfdf17/discovery/v2.0/keys",
  "response_modes_supported": [
    "query",
    "form_post"
  ],
  "subject_types_supported": [
    "pairwise"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "http_logout_supported": true,
  "post_logout_redirect_uris_supported": true,
  "end_session_endpoint": "https://login.microsoftonline.com/2801cede-7bda-4450-adfa-3daecbfdf17/oauth2/v2.0/logout",
  "response_types_supported": [
    "code",
    "code_id_token",
    "code_token",
    "id_token"
  ],
  "scopes_supported": [
    "openid",
    "profile",
    "email",
    "offline_access"
  ],
  "issuer": "https://login.microsoftonline.com/2801cede-7bda-4450-adfa-3daecbfdf17/v2.0",
  "claims_supported": [
    "sub",
    "tid",
    "cloud_instance_name",
    "cloud_instance_host_name",
    "cloud_graph_host_name",
    "magraph_host",
    "graph_host",
    "ext",
    "ext",
    "iat",
    "auth_time",
    "exp",
    "nonce",
    "preferred_username",
    "aud",
    "tid",
    "ver",
    "at_hash",
    "email",
    "email"
  ],
  "request_url_parameter_supported": false,
  "tenant_region_scope": "EU",
  "cloud_instance_name": "MicrosoftOnline.com",
  "cloud_graph_host_name": "graph.windows.net",
  "magraph_host": "graph.microsoft.com"
}
```

Location of public key(s) for token signature validation

Definitive source

Azure:

<https://login.microsoftonline.com/<tenant name>/v2.0/.well-known/openid-configuration>

AD FS

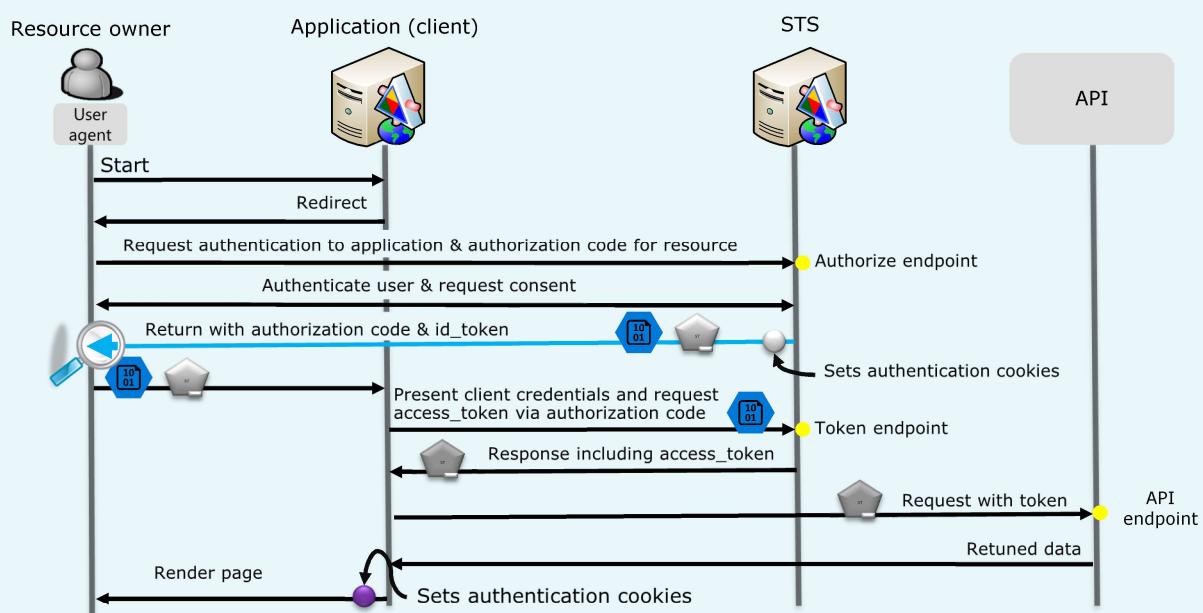
<https://<adfs service name>/adfs/.well-known/openid-configuration>



Demo...

1st Redirect

1st response after authentication



200 OK

```
<html><head><title>Working...</title></head><body>
<form method="POST" name="hiddenform" action="https://oidcazure.example.com/post.php">
<input type="hidden" name="code" value="AQAB..." />
<input type="hidden" name="id_token" value="eyJ0eX..." />
<input type="hidden" name="state" value="9999" />
<input type="hidden" name="session_state"
      value="5151341e-f9bb-4f70-b561-278794a0c761"/>
<noscript><p>Script is disabled. Click Submit to continue.</p>
<input type="submit" value="Submit" /></noscript></form>
<script language="javascript">document.forms[0].submit();</script></body></html>
```

- The 1st request to the STS defines the response_mode
 - In this example it was set to form_post
 - Alternatives query and fragment



Subsequent POST

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Replay Go Stream Decode | Keep: All sessions • Any Process Find Save Browse Clear Cache TextWizard Tearoff

F0 Fiddler Orchestra Beta F1 FiddlerScript Log Filters Timeline

Statistics Inspectors AutoResponder Composer

Headers TextView SyntaxView WebForms HexView OIDC Federation Auth

Cookies Raw JSON XML

QueryString

Name	Value
code	AQABAAIAABlh4kmE_aKTSVjz2RAHdM8-AWAKQhxYG
id_token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNTIzLndIdC16Ino0NH
state	9999
session_state	29aa2cf5-4e79-4c7e-9c12-4176ddc2270

Body

Name	Value
code	AQABAAIAABlh4kmE_aKTSVjz2RAHdM8-AWAKQhxYG
id_token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNTIzLndIdC16Ino0NH
state	9999
session_state	29aa2cf5-4e79-4c7e-9c12-4176ddc2270

Tunnel to translate.googleapis.com:443

Tunnel to clientservices.googleapis.com:443

Tunnel to translate.a/?client=trv... (2,973 no-ca)

Tunnel to oidcazure.example.com:443 (1,245)

Tunnel to login.microsoftonline.com:443 (20,367 no-ca)

Tunnel to feigfsaq (512 no-ca)

Tunnel to paapsmtbfwdmfl (512 no-ca)

Tunnel to dmrxz (512 no-ca)

Tunnel to login.microsoftonline.com:443 (1,119 privat)

Tunnel to autologon.microsoftonline.com:443 (0)

Tunnel to 5.ad.xthub.com/vinauth (12 no-ca)

Tunnel to login.microsoftonline.com:443 (264 privat)

Tunnel to ssl.gstatic.com:443 (0)

Tunnel to ssl.gstatic.com:443 (0)

ssl.gstatic.com /safebrowsing/csd/client_... (69,547 public)

ssl.gstatic.com /safebrowsing/csd/client_... (69,547 public)

ssl.gstatic.com /28019ede7bda4450-ad... (6,400 no-ca)

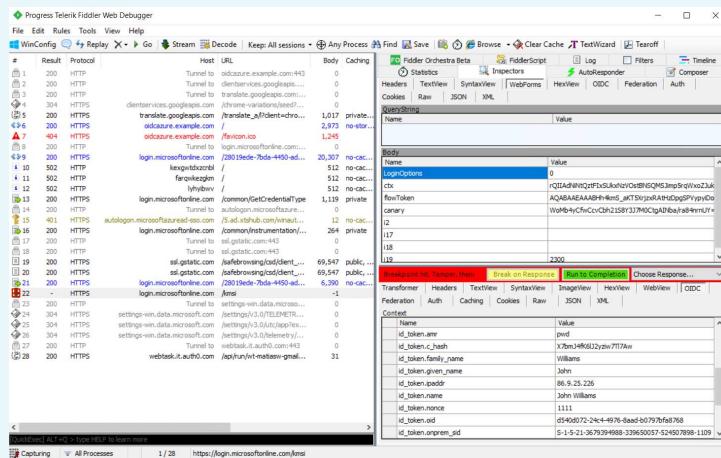
ssl.gstatic.com /amsi (1,808 privat)

ssl.gstatic.com /post.php (2,398 no-ca)

- If you are not getting back what you expect, check the response_type and scope values in the 1st redirect to the STS



200 OK



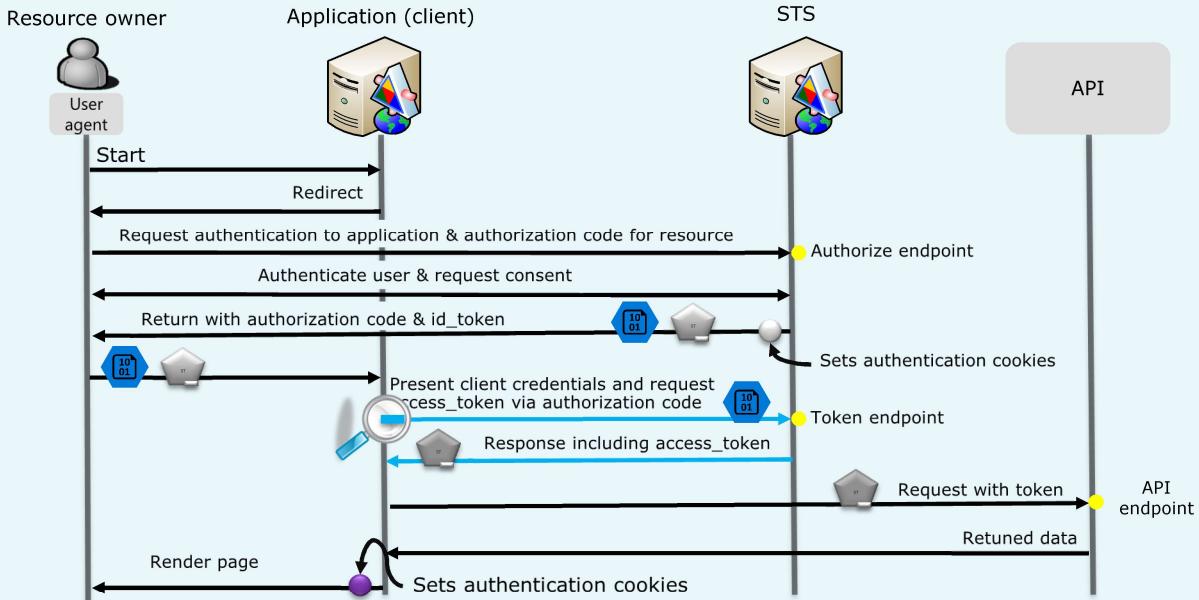
- Using Fiddler you can set a breakpoint so that you can fiddle with the response before sending it back to the application
 - Allows testing that token is being properly validated by the app
- Fiddler can be used to replay tokens and evaluate if the app is correctly handling replay detection

NIC
XTSeminars

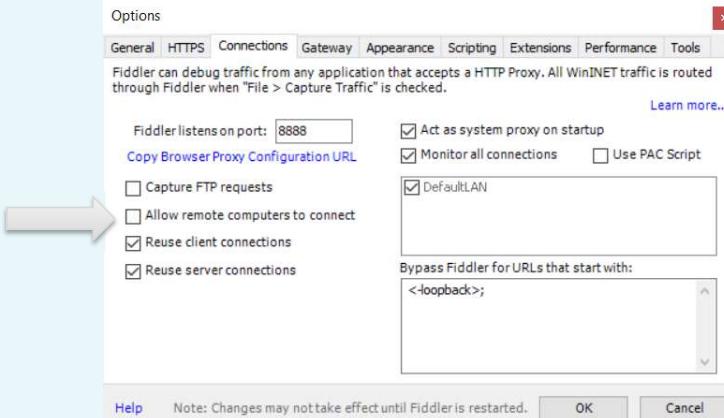
Demo...

Breakpoints

Code to token exchange

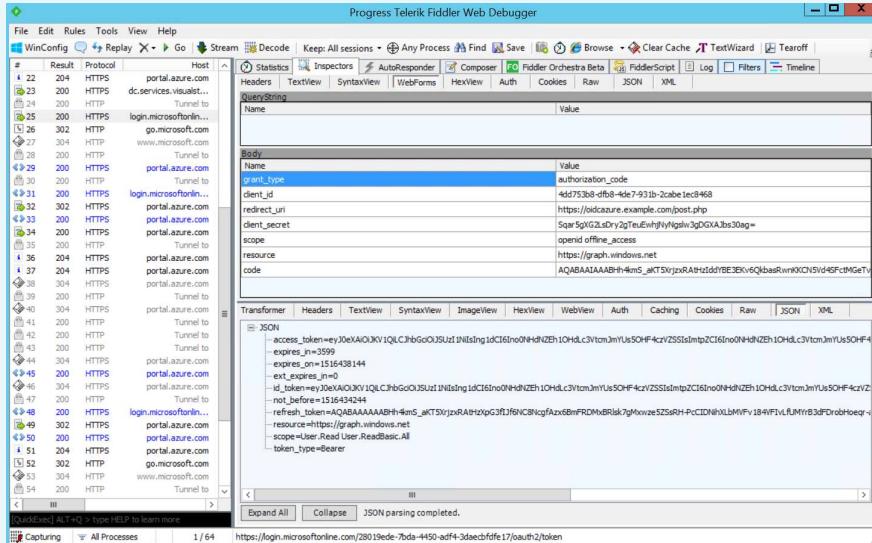


Top tip!



- Set up the application to use Fiddler as a proxy and capture the code to token exchange
- If you can't run Fiddler on the app server, enable Fiddler to support the connection of remote computers
 - Also allows tracing a browser interaction from a mobile device

Code to token exchange



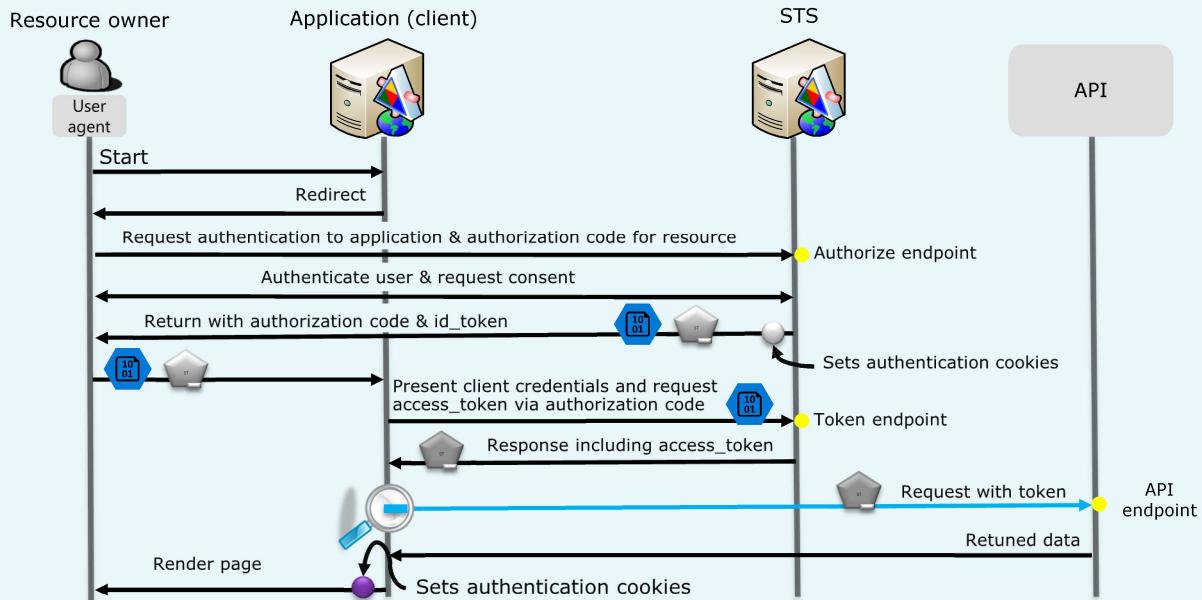
- Capture from web application

NIC
XT Seminars

Demo...

Code to token exchange

Accessing the API



Use Postman to test interaction with the API

The screenshot shows the Postman application interface with the following details:

- Request Method**: GET
- URL**: `https://graph.windows.net/myorganization/me?api-version=1.6`
- Authorization**: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIn... (access_token)
- Headers (1)** tab is selected
- Body** tab is selected
- Test Results** tab shows the response status: `Status: 200 OK`, `Time: 427 ms`, `Size: 3.61 KB`
- Body** tab displays the JSON response content:

```

    {
      "id": "12345678901234567890123456789012",
      "jobTitle": "Manager",
      "isCompliant": true,
      "employeeId": "12345678901234567890123456789012",
      "displayName": "John Williams",
      "givenName": "John",
      "middleName": "Williams",
      "surName": "Williams",
      "department": "Sales",
      "creationType": "Employee",
      "country": null,
      "city": null,
      "companyName": null,
      "facsimileTelephoneNumber": null,
      "mobile": null,
      "officePhone": null,
      "postOfficeBox": null,
      "streetAddress": null,
      "userPrincipalName": "jwilliams@contoso.com",
      "extensionAttribute1": null,
      "extensionAttribute2": null,
      "extensionAttribute3": null,
      "extensionAttribute4": null,
      "extensionAttribute5": null
    }
  
```

- Use the access_token returned to interact with the API

Demo...

Postman

The documentation nightmare!

- OAuth 2.0 is defined as a framework and there are many different interpretations as to exactly how it should be implemented
- Always look to the documentation from the appropriate IDaaS vendor when working with OAuth 2.0
- Always check that you are reading OAuth 2.0 documentation
 - OAuth is completely different
- It's easy for developers to leave security holes through inappropriate implementation
 - Always check token validation, replay detection and cross-site forgery detection



So where next?

5-Day Hands-On Masterclass with John Craddock **Microsoft Identity solutions with Azure Active Directory, on-premises AD FS and AD**

38 hands-on labs

**10% Discount if you book by this Friday for:
 Oslo : April 23 – 27 or
 Oslo : August 27 - 31**

Talk to the NIC/Crayon team or email info@niccomf.com

<http://www.xtseminars.co.uk/masterclass>



Consulting services on request



**John
Craddock**
Infrastructure and
security Architect
XTSeminars Ltd

Johncra@xtseminars.co.uk
 @john_craddock



John has designed and implemented computing systems ranging from high-speed industrial controllers through to distributed IT systems with a focus on security and high-availability. A key player in many IT projects for industry leaders including Microsoft, the UK Government and multi-nationals that require optimized IT systems. Developed technical training courses that have been published worldwide, co-authored a highly successful book on Microsoft Active Directory Internals, presents regularly at major international conferences including TechEd, IT Forum and European summits. John can be engaged as a consultant or booked for speaking engagements through XTSeminars. www.xtseminars.co.uk



Resources

Slides and demos from the conference will be available at
github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)

