Extending OAuth

Scott Brady
IDENTITY & ACCESS CONTROL LEAD

@scottbrady91 www.scottbrady91.com

Overview

Adding identity with OpenID Connect

Programmatic client configuration with OAuth metadata

OAuth device flow for browserless devices

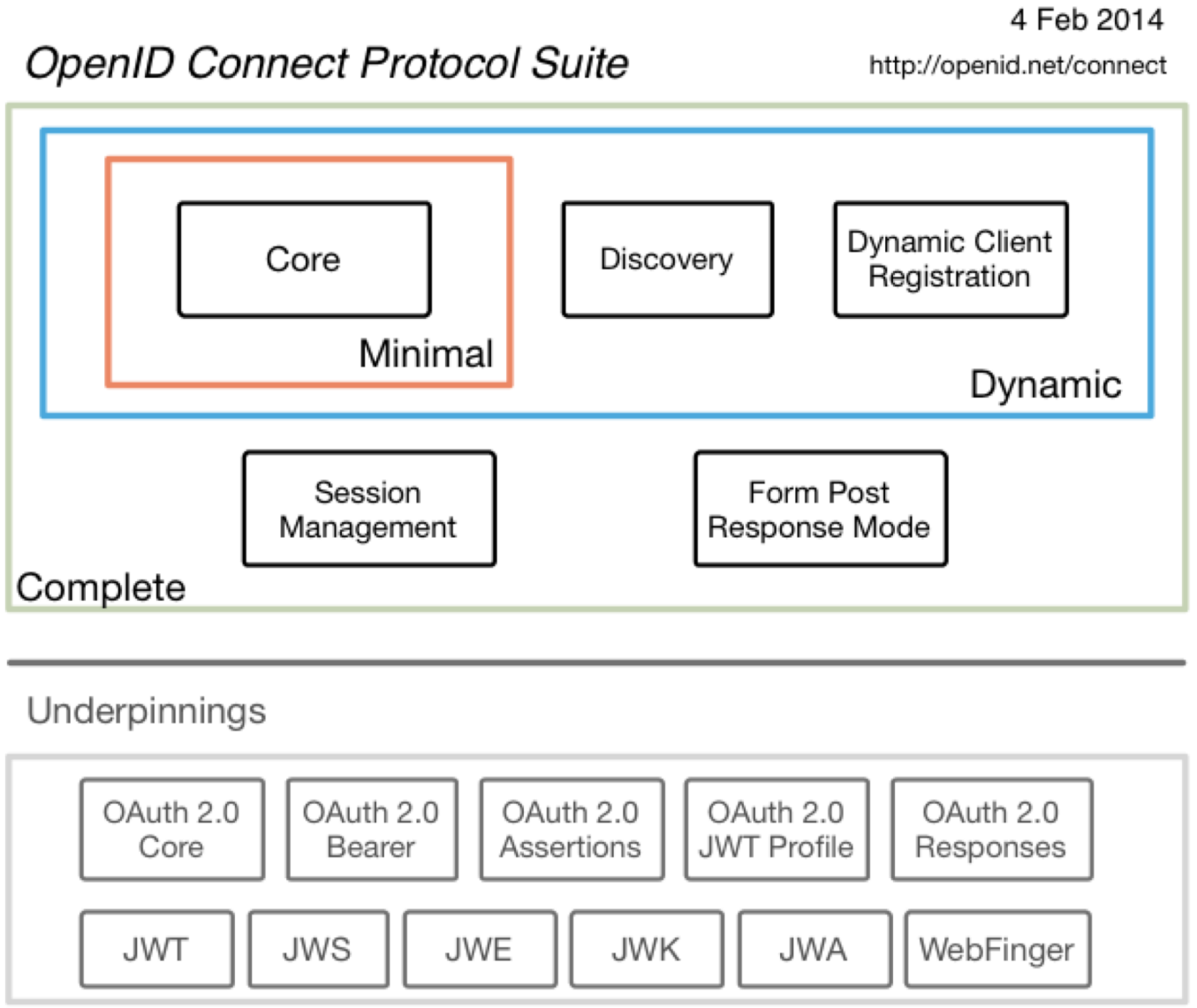
Combining SAML 2.0 and OAuth 2.0

OpenID Connect 1.0

Identity Layer on top of OAuth 2.0

Formalizes some OAuth ambiguity

Authorization Server becomes an Identity Provider



Identity Access

UserInfo endpoint

Identity scopes

Identity Token

Describes the authentication event

Intended for the client application

Verifiable signature

Identity Token - JWT


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjU1NmZkMzk2YWM3NDdkNDQwYjY0ZjEzNzQzNmJjYT
gzIiwidHlwIjoiSldUIn0.eyJuYmYiOjE1MzUyMTU3NjEsImV4cCI6MTUzNTIxNjA2MSwi
aXNzIjoiaHR0cDovL2xvY2FsaG9zdDo1MDAwIiwiYXVkIjoib2lkY19jbGllbnQiLCJub2
5jZSI6IjYzNjcwODEyNTM4MzI0MzMzNy5ZelprWVdJNU1URXRZalkzWkMwMFlUY3pMVGht
WkdRdFltVTVOR0l5TVRRNFpEUmxaV1V3WkRsbE9EY3RPRGMxWmkwME1UZzVMVGxsT0dRdF
lXRmtObVZsTnpBeFpqbG0iLCJpYXQiOjE1MzUyMTU3NjEsImF0X2hhc2giOiJvaVQyUEQt
MzBLVVRpbjI5LUhKTndRIiwic3ViIjoiNzc0YTAwNjhlOWMwNGU5N2JhNmE5NmY4NWY2MW
MwNWMiLCJhdXRoX3RpbWUiOjE1MzUyMTU3NTMsImlkcCI6ImxvY2FsIiwiYW1yIjpbInB3
ZCJdfQ.l55cmox4VqoCzovztlEVcd6egabdbUqBwfQaRJOT9lLI8L2vMFNyA02j_NKbgn7
LIVWSiozMDFJ5gmNul11LEao5M9p82j5ZJE1EO2-K4gDO8w5N8J72-
6yrCATbVzisoG2PP9oWOcbBNBZc0cnchRAPrRrYiOi5v1hcRv6VUP4nUDtc9gcKwbeImVh
NvCE9D_XjJxarIoz5m6NUziO2F0OCsmyng-
qk6ShzePd4HEurHIVfz5QS1Qdo20BIbl86gF8bGh7QNS5dCZYwNvxocFy5dA39xhqlzOmy
tsMLGVwFjO5uPdbxIX7PvqbnJEo709mHFGE6QypceKLToYSj5Q
```

Identity Token - Header


```
{
  "alg": "RS256",
  "kid": "556fd396ac747d440b64f137436bca83",
  "typ": "JWT"
}
```

Identity Token - Payload


```
{
  "nbf": 1535215761,
  "exp": 1535216061,
  "iat": 1535215761,
  "auth_time": 1535215753,
  "iss": "http://localhost:5000",
  "aud": "oidc_client",
  "nonce": "636708...[omitted for brevity]...QtYWFkNmVlNzAxZjlm",
  "at_hash": "oiT2PD-30KUTin29-HJNwQ",
  "sub": "774a0068e9c04e97ba6a96f85f61c05c",
  "idp": "local",
  "amr": [ "pwd" ]
}
```


Hybrid Flow

`code id_token`

`code token`

`code id_token token`

All other combinations of `response_type`

Gives us something to validate before revealing secrets

Demo

OpenID Connect in action

OAuth 2.0 Authorization Server Metadata

RFC 8414

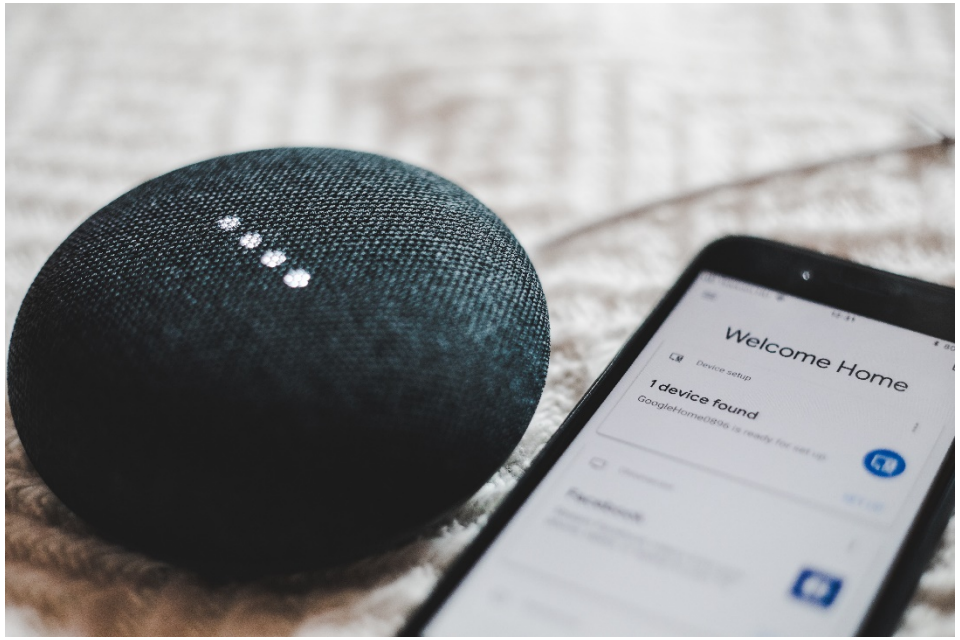
/.well-known/oauth-authorization-server

Metadata Document


```
{
 "issuer": "https://server.example.com",
 "authorization_endpoint": "https://server.example.com/authorize",
 "token_endpoint": "https://server.example.com/token",
 "token_endpoint_auth_methods_supported": ["client_secret_basic"],
 "scopes_supported": ["api1.read", "api1.write", "offline_access"],
 "response_types_supported": ["code", "code token"]
}
```

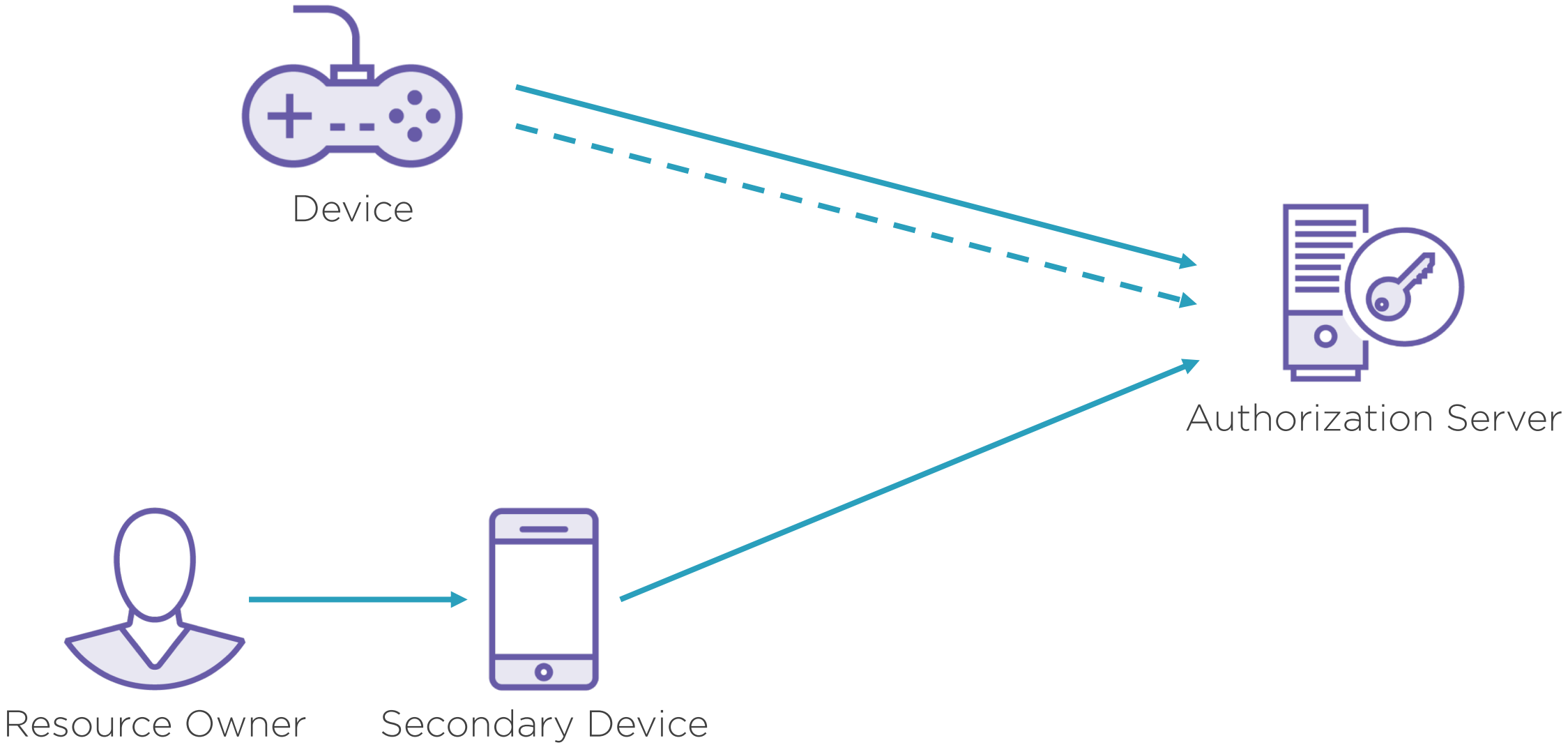

OAuth Device Flow

Browserless Devices



Input Constrained Devices

OAuth Device Flow



Device Authorization - Request

```
POST /device_authorization HTTP/1.1
  Host: server.example.com
  Content-Type: application/x-www-form-urlencoded

 client_id=459691054427
```

Device Authorization - Response


```
{
  "device_code": "GMMhmHCXhWEzkobqIHGG_EnNYYsAkukHspeYUk9E8",
  "user_code": "WDJB-MJHT",
  "verification_uri": "https://www.example.com/device",
  "verification_uri_complete":
     "https://www.example.com/device?user_code=WDJB-MJHT",
  "expires_in": 1800,
  "interval": 5
}
```


User Interaction

```
+-----------------------------------------+
|                                         |
|  Using a browser on another device, visit:  |
|  https://example.com/device             |
|                                         |
|  And enter the code:                    |
|  WDJB-MJHT                              |
|                                         |
+-----------------------------------------+
```

User (Friendly) Interaction

QR code

NFC

Bluetooth Low Energy

Token Request - Request

```
POST /token HTTP/1.1
  Host: server.example.com
  Content-Type: application/x-www-form-urlencoded


 grant_type=urn:ietf:params:oauth:grant-type:device_code
 &device_code=GMMhmHCXhWEzkobqIHGG_EnNYYsAkukHspeYUk9E8
 &client_id=459691054427
```

Token Request - Response

```
{
  "error": "authorization_pending"
}
```

Token Request - Response

```
{
  "access_token": "2YotnFZFEjr1zCsicMWpAA",
  "token_type": "example",
  "expires_in": 3600,
}
```

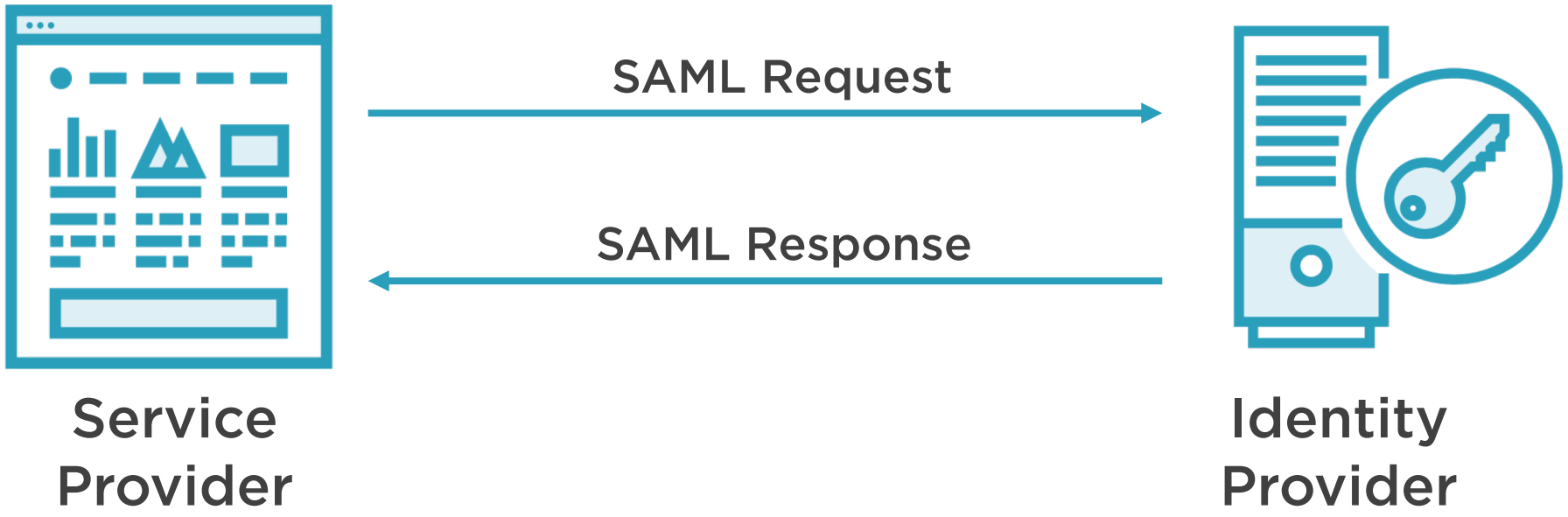
Demo

Device flow in action

SAML & OAuth

RFC 8414

SAML at a Glance



SAML Assertion

```
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="65safd321asdf54w98456546bn3m2sdf" Version="2.0"
IssueInstant="20148-08-24T18:01:24Z">
  <saml:Issuer>http://idp.example.com</saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="65safd321asdf54w98456546bn3m2sdf">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
        <ds:DigestValue>DSF68H2V33D59sdfg87/Z48=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>x+91uRPRDVJ9IKk76dp0kP6sznQqD7tD2FrmoJDnAqzGcP7r7WVkr2v9Luh+ ...[omitted for brevity]... XAbKkv8Qv2xktA5jNcu+epfVvGfLX4Ih1wLcNN+Pgb4C3d4=</ds:SignatureValue>
    <ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICajCCAdOgAw...[omitted for brevity]...Cnf5ek0nK00m0YZGyc4LzgD0CROMASTWNg==</ds:X509Certificate></ds:X509Data></ds:KeyInfo>
  </ds:Signature>
  <saml:Subject>
    <saml:NameID SPNameQualifier="http://sp.example.com" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
      _p4987l5665vcbn987f56s54gh9as8sdf96
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData NotOnOrAfter="2018-08-24T19:21:35" Recipient="http://sp.example.com/acs" InResponseTo="#_454asdf3b046395c654sdf661e97f8900b52as9d87f2"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="20148-08-24T18:01:24Z" NotOnOrAfter="2018-08-24T19:21:35">
    <saml:AudienceRestriction>
      <saml:Audience>https://sp.example.com</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="20148-08-24T18:01:24Z" SessionNotOnOrAfter="2018-08-24T19:21:35" SessionIndex="_395c654sdf661e977f56s54gh9as8sdf96">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
      <saml:AttributeValue xsi:type="xs:string">Scott</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Token Request - Request

```
POST /token HTTP/1.1
  Host: server.example.com
  Content-Type: application/x-www-form-urlencoded

 grant_type=urn:ietf:params:oauth:grant-type:saml2-bearer
 &assertion=PHNhbWxwOl...[omitted for brevity]...ZT4
```

Summary

Adding identity with OpenID Connect

Programmatic client configuration with OAuth metadata

OAuth device flow for browserless devices

Combining SAML and OAuth 2.0

Honourable mention:

- UMA 2
- JWT Client Authentication (RFC 7523)