OpenID Connect & IdentityServer

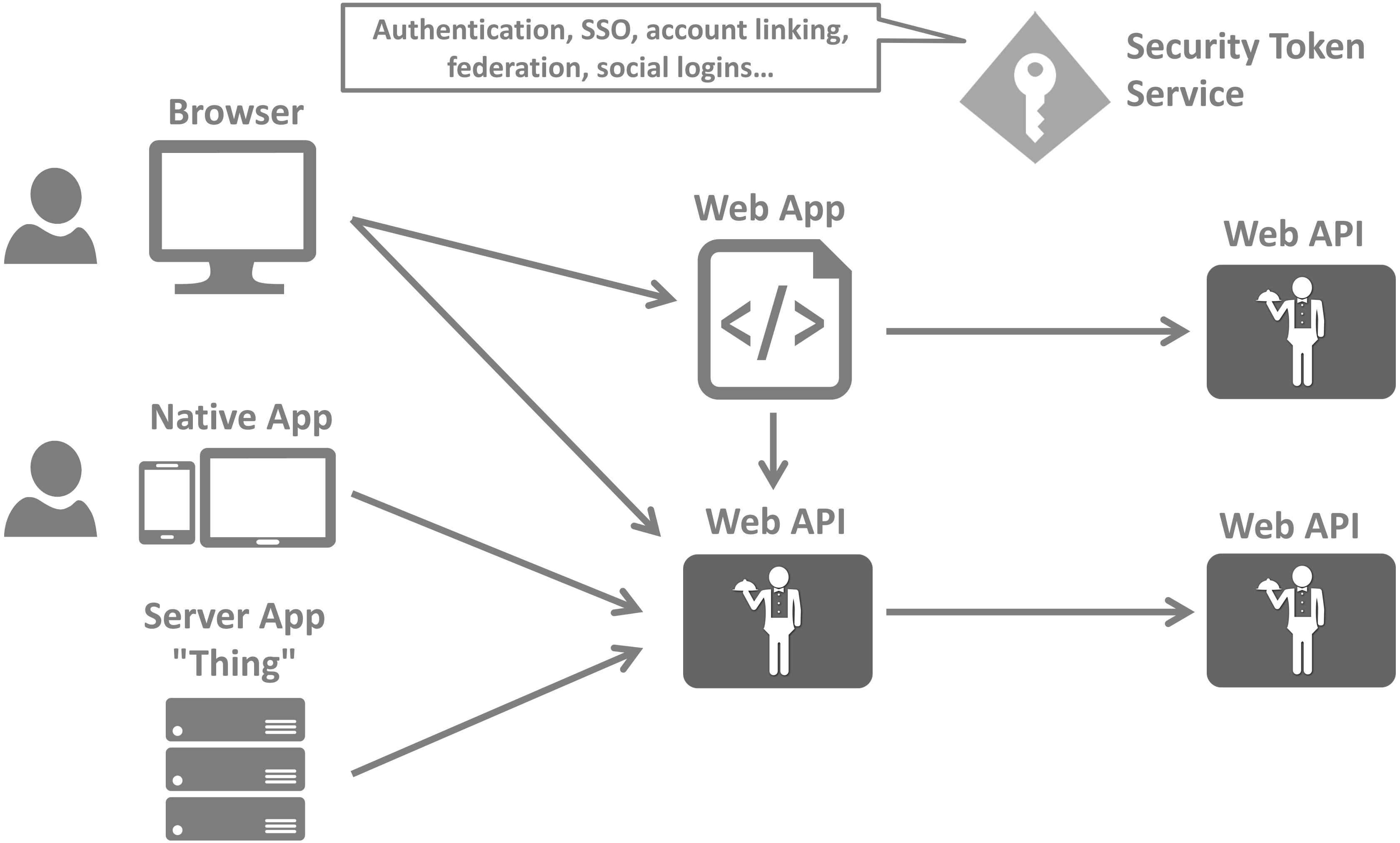
Dominick Baier
http://leastprivilege.com
@leastprivilege

Brock Allen
http://brockallen.com
@brocklallen

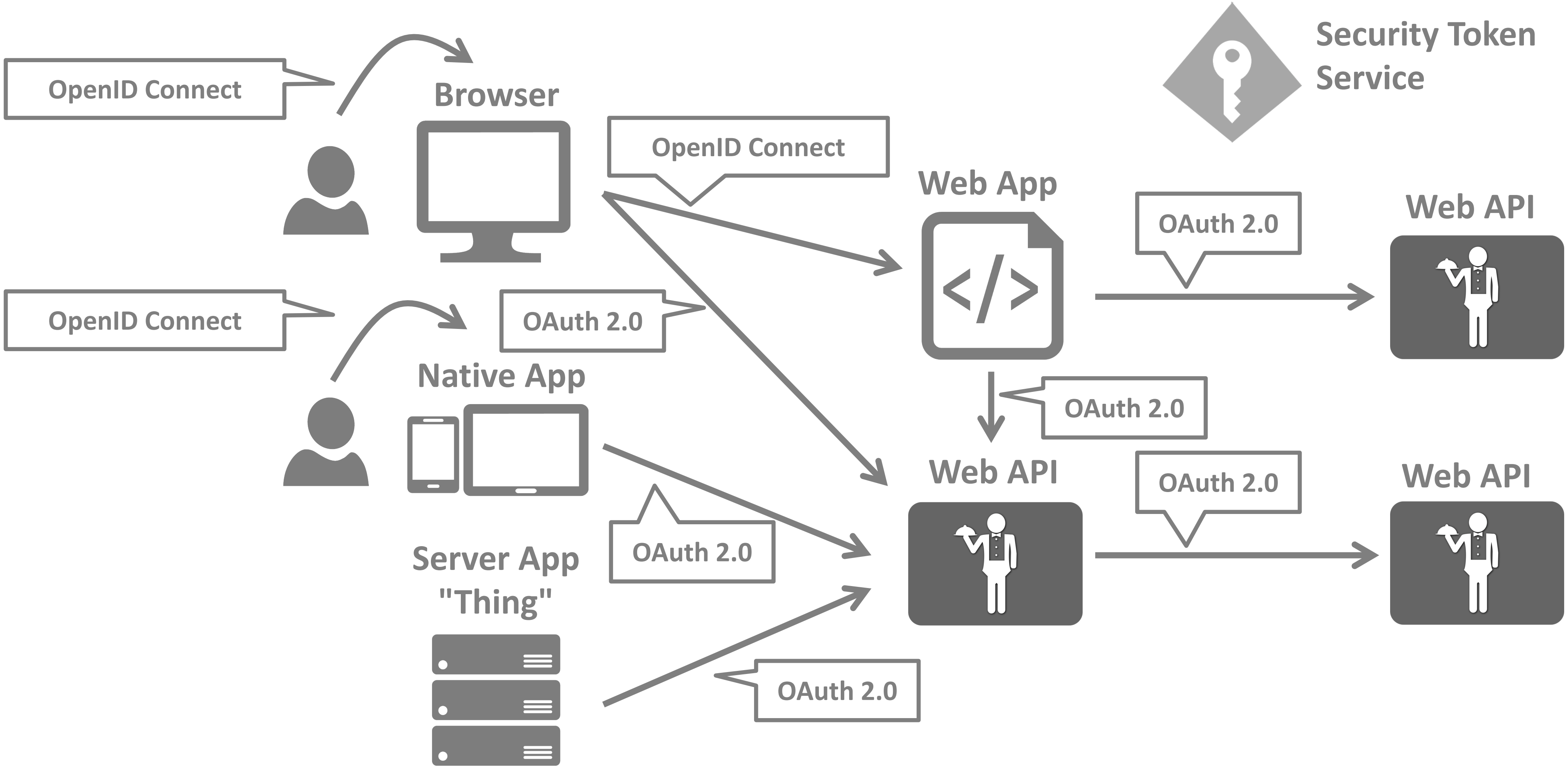
identity
SERVER

identity
MODEL

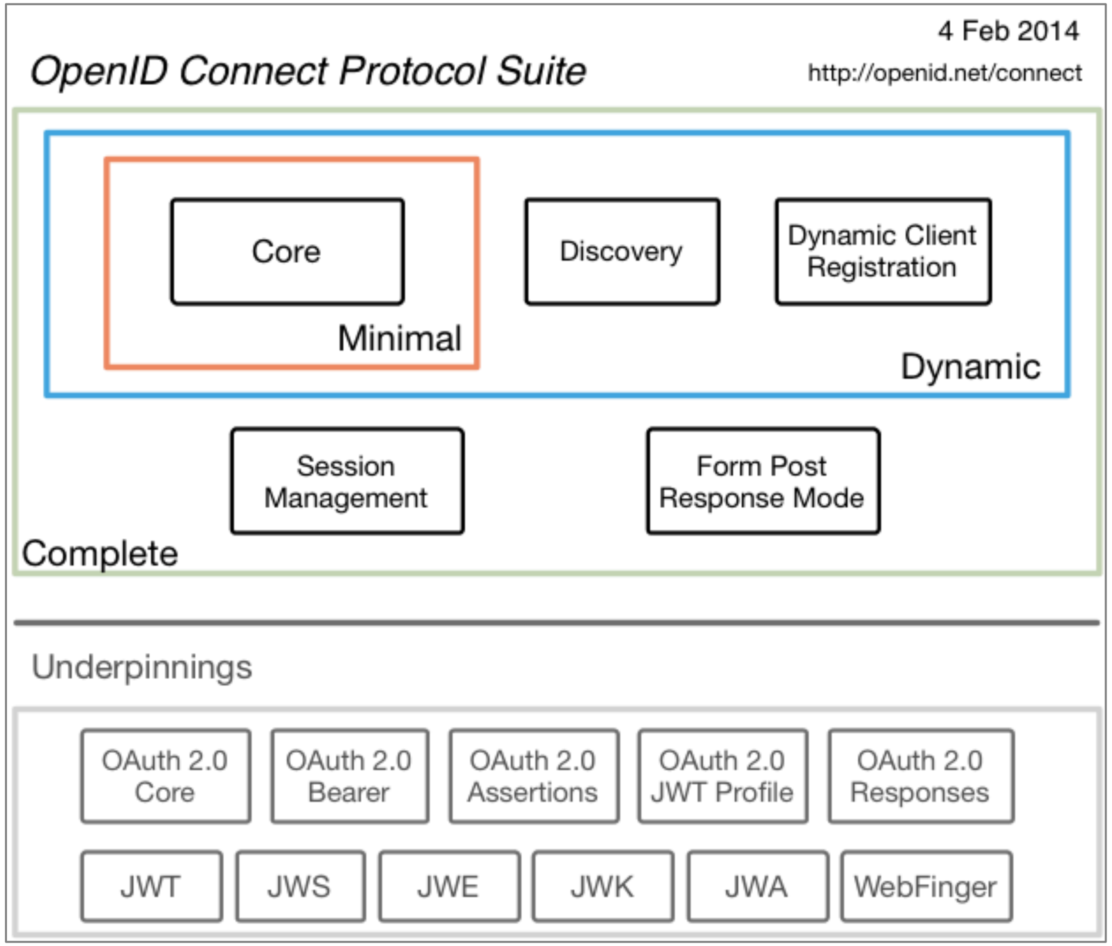
The way forward…



Security Protocols

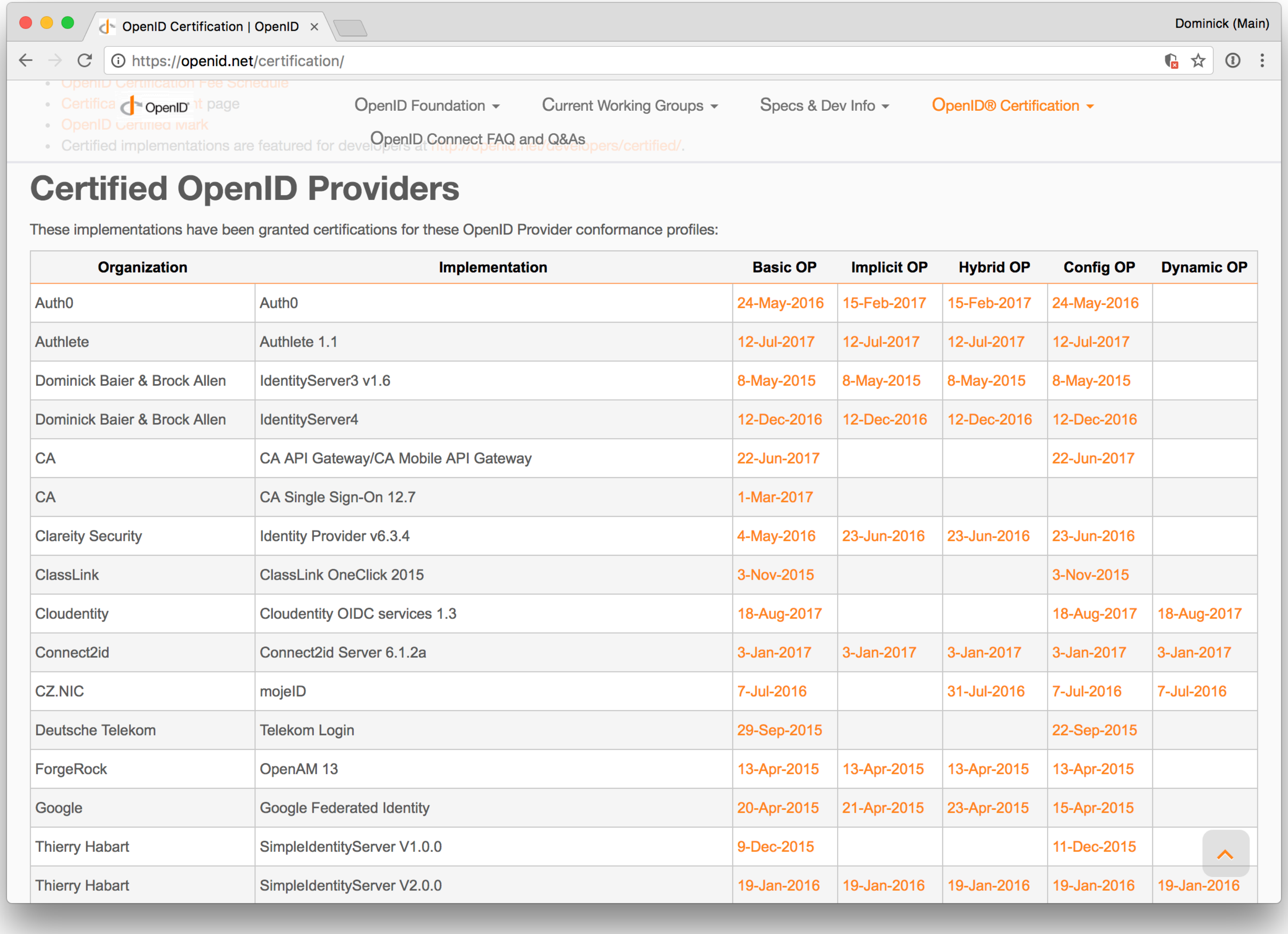


http://openid.net/connect/



OpenID Connect Certification

for providers and
client libraries

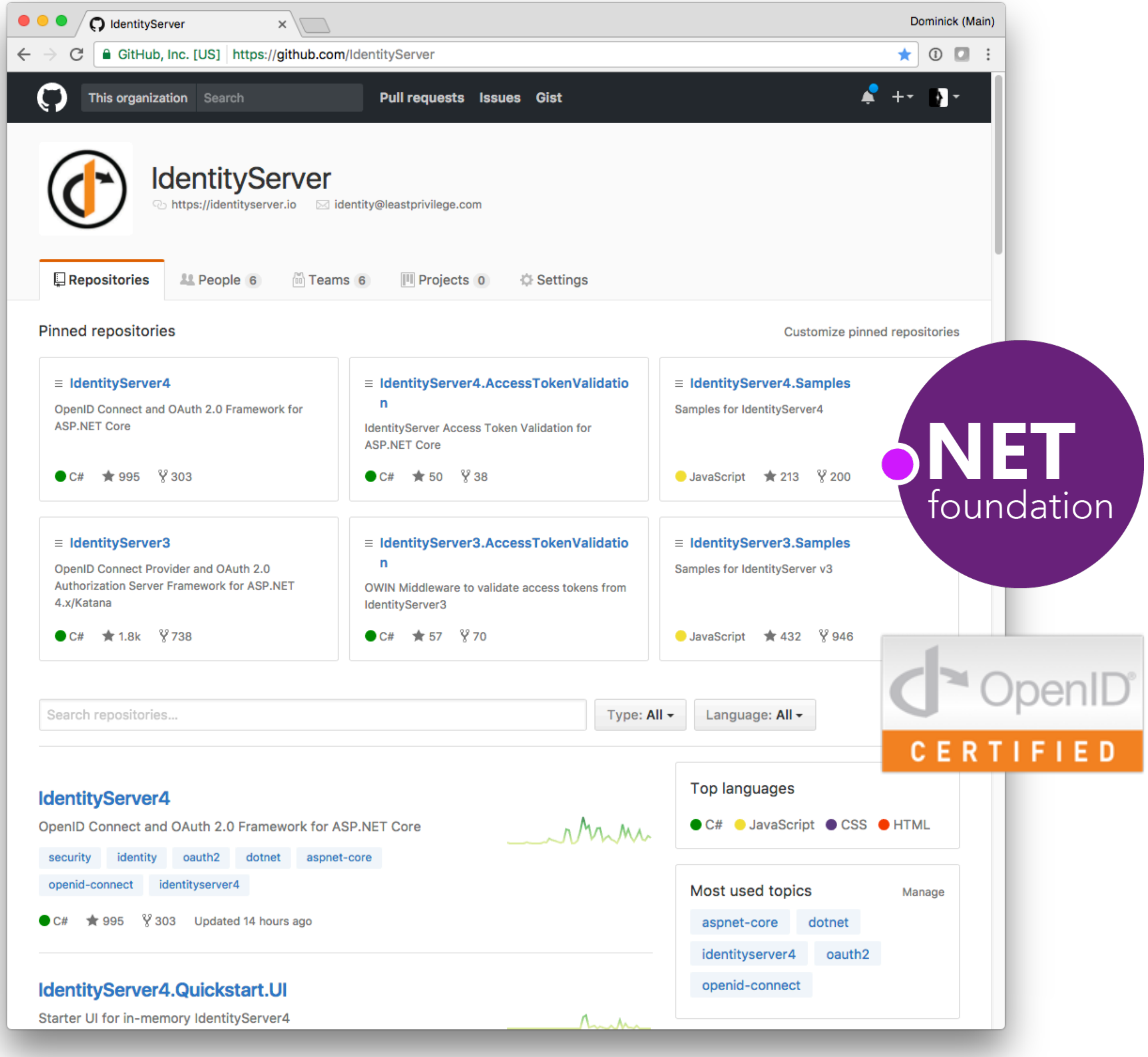


- OpenID Certification Fee Schedule
- Certifica t page
- OpenID Certified Mark
- Certified implementations are featured for developers at http://openid.net/developers/certified/.

Certified OpenID Providers

These implementations have been granted certifications for these OpenID Provider conformance profiles:

Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP
Auth0	Auth0	24-May-2016	15-Feb-2017	15-Feb-2017	24-May-2016	
Authlete	Authlete 1.1	12-Jul-2017	12-Jul-2017	12-Jul-2017	12-Jul-2017	
Dominick Baier & Brock Allen	IdentityServer3 v1.6	8-May-2015	8-May-2015	8-May-2015	8-May-2015	
Dominick Baier & Brock Allen	IdentityServer4	12-Dec-2016	12-Dec-2016	12-Dec-2016	12-Dec-2016	
CA	CA API Gateway/CA Mobile API Gateway	22-Jun-2017			22-Jun-2017	
CA	CA Single Sign-On 12.7	1-Mar-2017				
Clareity Security	Identity Provider v6.3.4	4-May-2016	23-Jun-2016	23-Jun-2016	23-Jun-2016	
ClassLink	ClassLink OneClick 2015	3-Nov-2015			3-Nov-2015	
Cloudentity	Cloudentity OIDC services 1.3	18-Aug-2017			18-Aug-2017	18-Aug-2017
Connect2id	Connect2id Server 6.1.2a	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017	3-Jan-2017
CZ.NIC	mojeID	7-Jul-2016		31-Jul-2016	7-Jul-2016	7-Jul-2016
Deutsche Telekom	Telekom Login	29-Sep-2015			22-Sep-2015	
ForgeRock	OpenAM 13	13-Apr-2015	13-Apr-2015	13-Apr-2015	13-Apr-2015	
Google	Google Federated Identity	20-Apr-2015	21-Apr-2015	23-Apr-2015	15-Apr-2015	
Thierry Habart	SimpleIdentityServer V1.0.0	9-Dec-2015			11-Dec-2015	
Thierry Habart	SimpleIdentityServer V2.0.0	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016	19-Jan-2016



IdentityServer

Dominick (Main)

GitHub, Inc. [US] https://github.com/IdentityServer

This organization Search Pull requests Issues Gist

IdentityServer

https://identityserver.io identity@leastprivilege.com

Repositories People 6 Teams 6 Projects 0 Settings

Pinned repositories

Customize pinned repositories

IdentityServer4
OpenID Connect and OAuth 2.0 Framework for ASP.NET Core
● C# ★ 995 303

IdentityServer4.AccessTokenValidation
IdentityServer Access Token Validation for ASP.NET Core
● C# ★ 50 38

IdentityServer4.Samples
Samples for IdentityServer4
● JavaScript ★ 213 200

IdentityServer3
OpenID Connect Provider and OAuth 2.0 Authorization Server Framework for ASP.NET 4.x/Katana
● C# ★ 1.8k 738

IdentityServer3.AccessTokenValidation
OWIN Middleware to validate access tokens from IdentityServer3
● C# ★ 57 70

IdentityServer3.Samples
Samples for IdentityServer v3
● JavaScript ★ 432 946

Search repositories... Type: All Language: All

IdentityServer4
OpenID Connect and OAuth 2.0 Framework for ASP.NET Core
security identity oauth2 dotnet aspnet-core openid-connect identityserver4
● C# ★ 995 303 Updated 14 hours ago

IdentityServer4.Quickstart.UI
Starter UI for in-memory IdentityServer4

Top languages
● C# ● JavaScript ● CSS ● HTML

Most used topics Manage
aspnet-core dotnet identityserver4 oauth2 openid-connect

.NET foundation

OpenID CERTIFIED

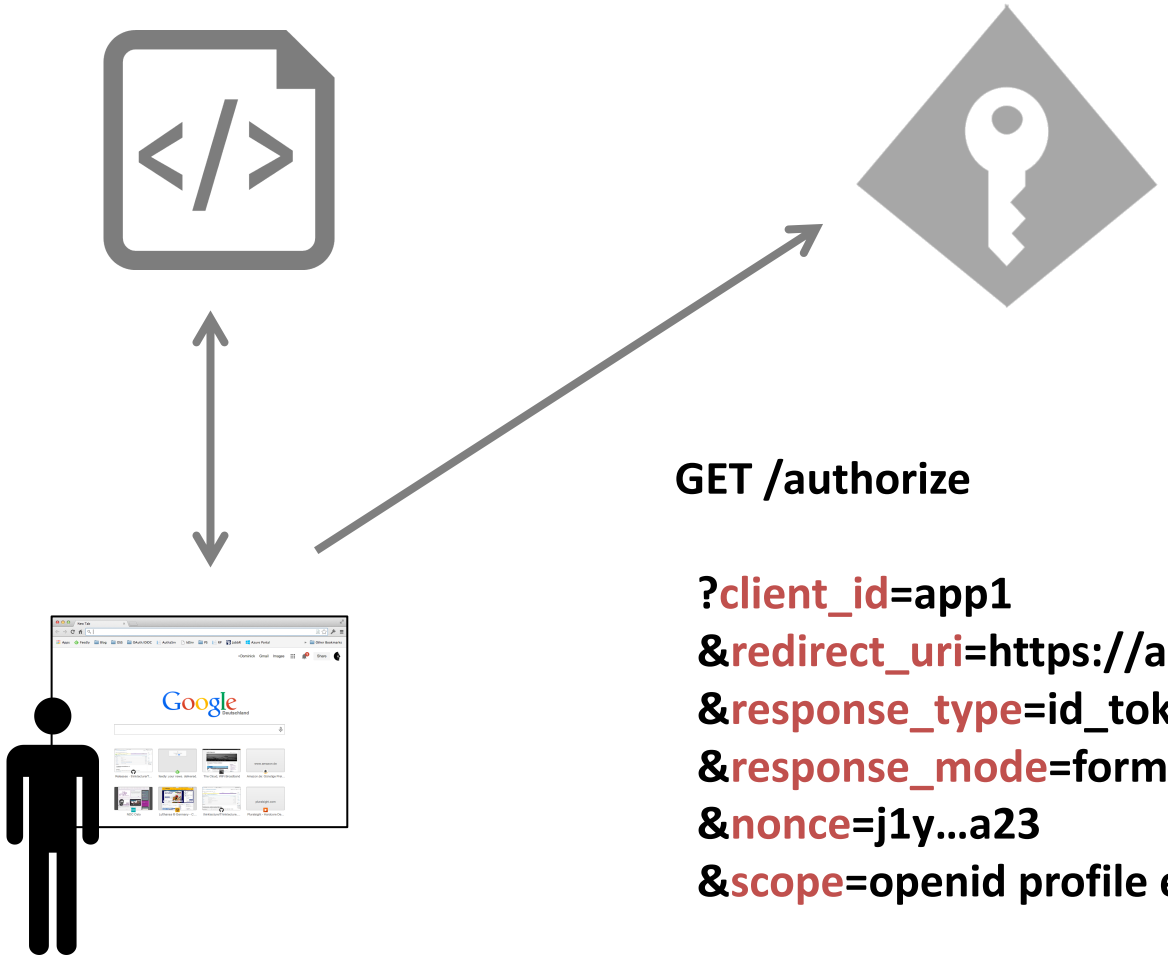
Endpoints

Discovery Endpoint

Authorize Endpoint

Token Endpoint

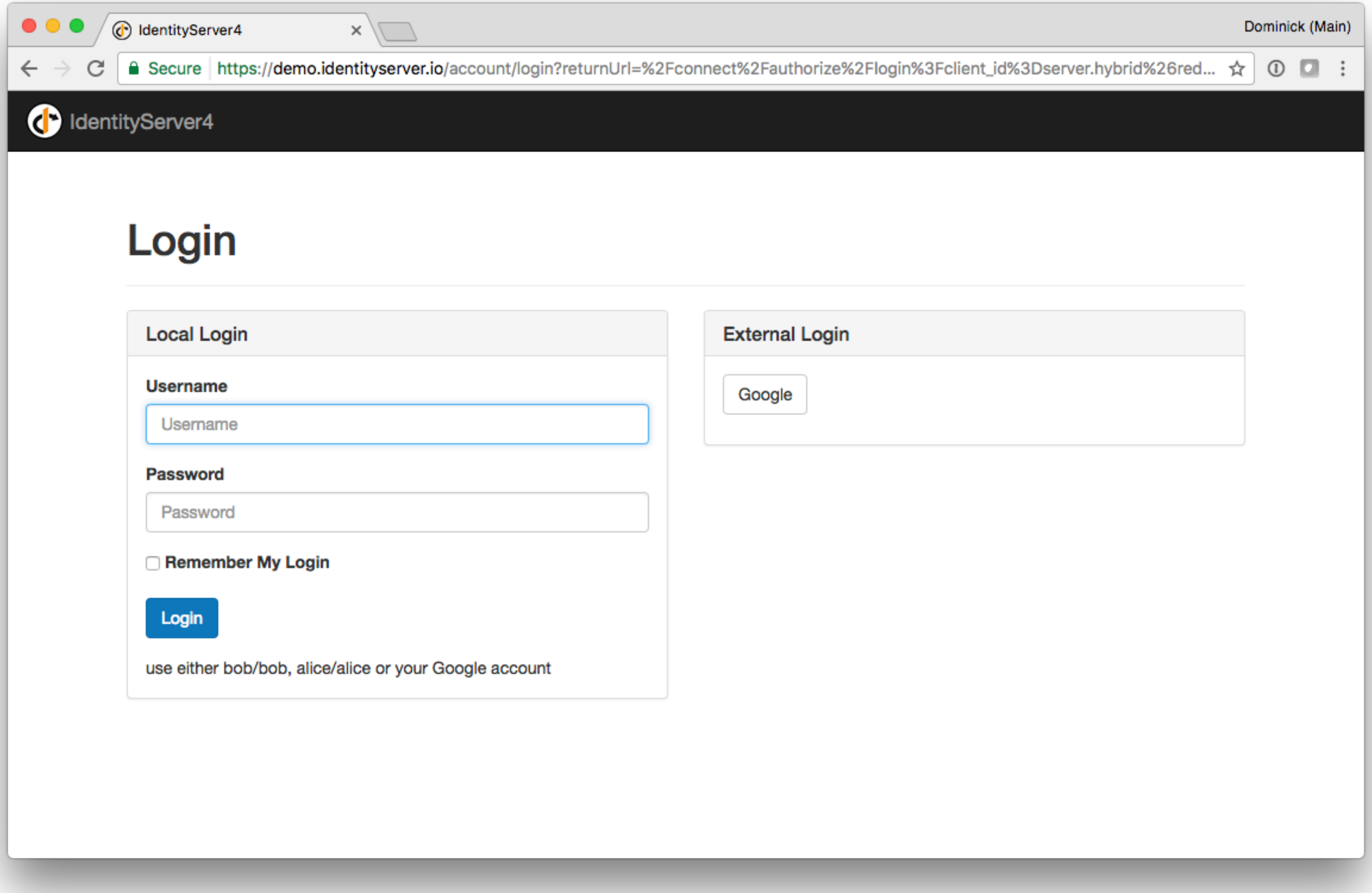
Authentication for Web Applications



```
GET /authorize

  ?client_id=app1
  &redirect_uri=https://app.com/cb
  &response_type=id_token
  &response_mode=form_post
  &nonce=j1y…a23
  &scope=openid profile email
```

Authentication



IdentityServer4
Dominick (Main)
Secure
https://demo.identityserver.io/account/login?returnUrl=%2Fconnect%2Fauthorize%2Flogin%3Fclient_id%3Dserver.hybrid%26red...
IdentityServer4

Login

Local Login

Username

Username

Password

Password

□ Remember My Login

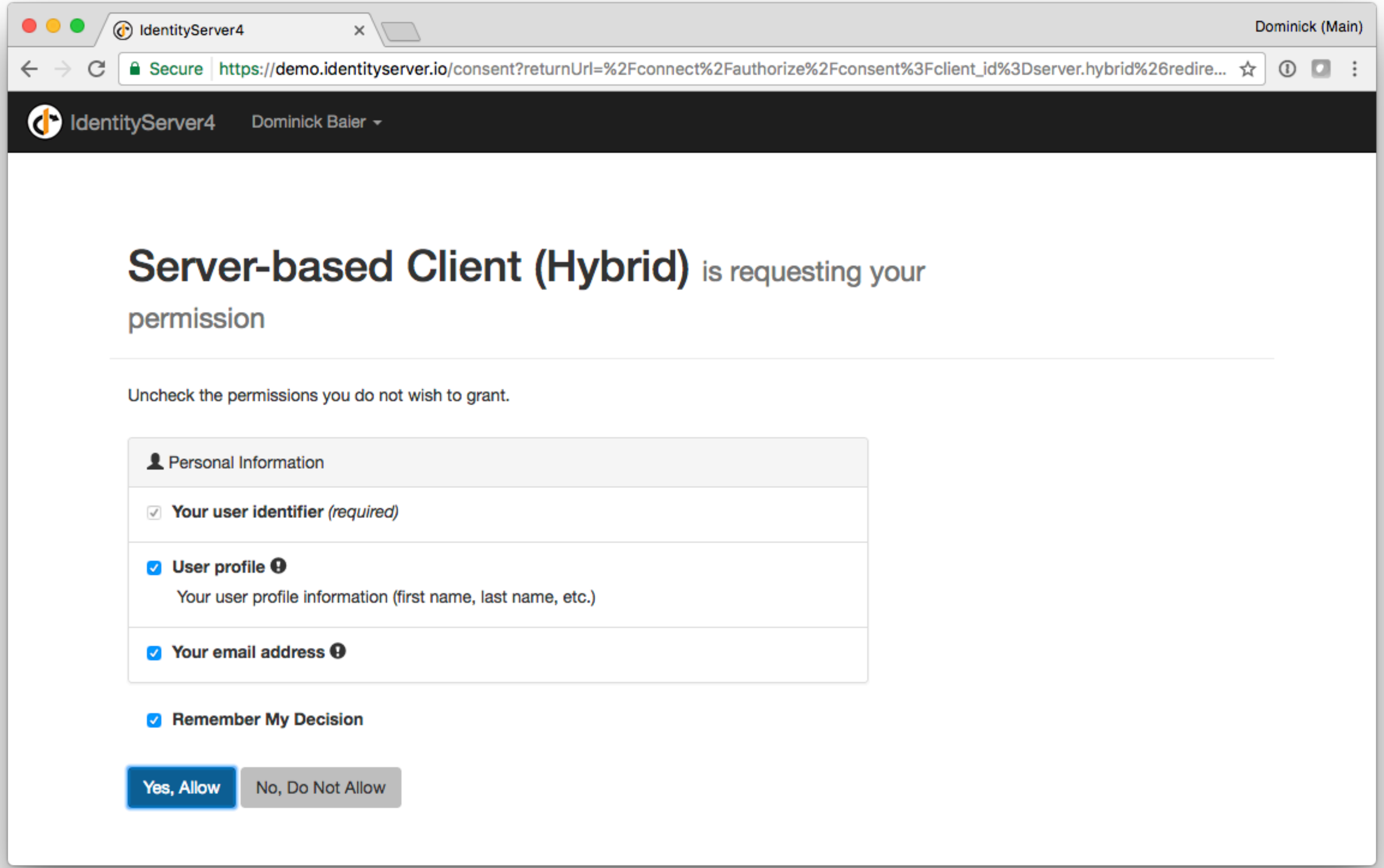
Login

use either bob/bob, alice/alice or your Google account

External Login

Google

Consent



IdentityServer4
Dominick (Main)
Secure
https://demo.identityserver.io/consent?returnUrl=%2Fconnect%2Fauthorize%2Fconsent%3Fclient_id%3Dserver.hybrid%26redire...
IdentityServer4
Dominick Baier

Server-based Client (Hybrid) is requesting your permission

Uncheck the permissions you do not wish to grant.

Personal Information

☑ **Your user identifier** *(required)*

☑ **User profile**

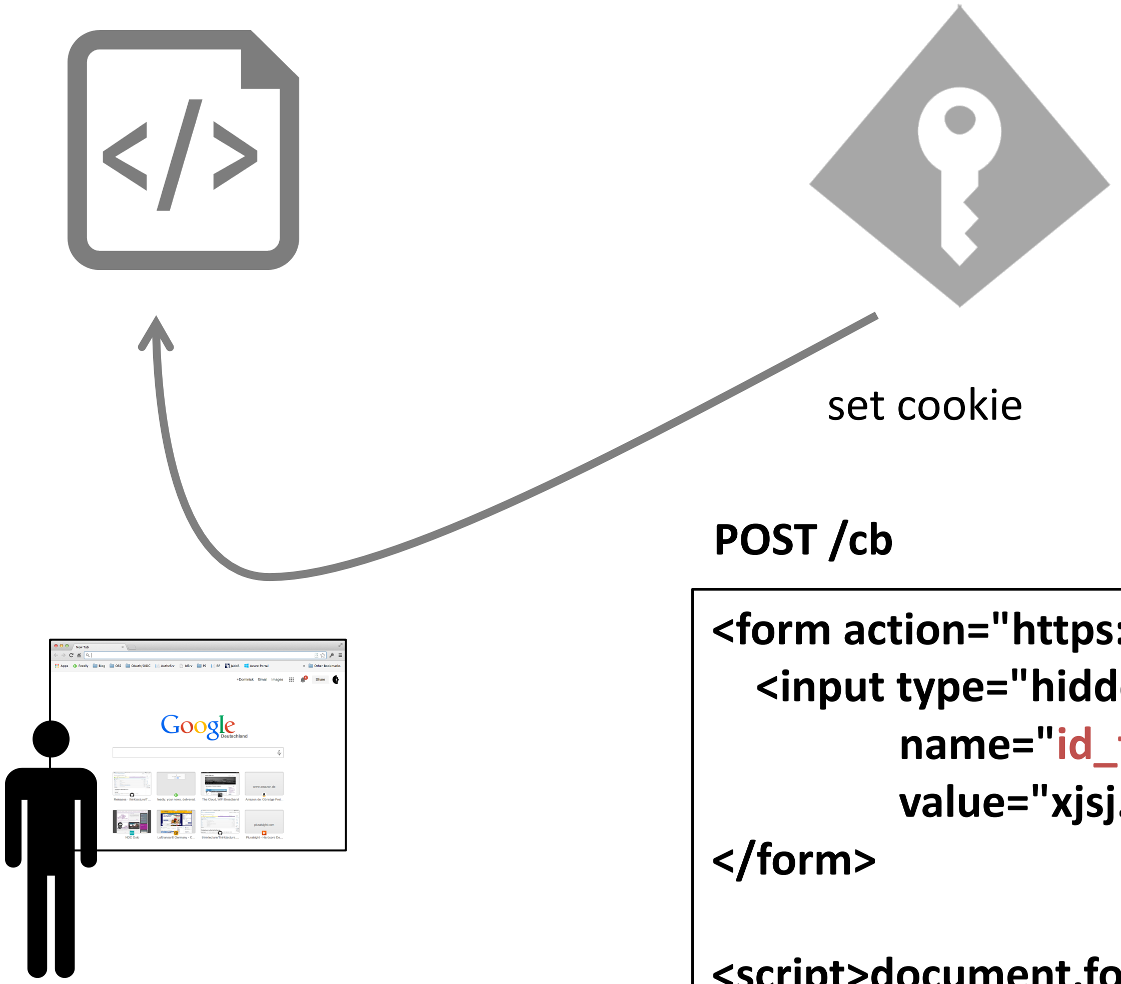
Your user profile information (first name, last name, etc.)

☑ **Your email address**

☑ **Remember My Decision**

Yes, Allow | No, Do Not Allow

Response



POST /cb

```
<form action="https://app.com/cb">
   <input type="hidden"
             name="id_token"
             value="xjsj…aas" />
</form>

<script>document.forms[0].submit()</script>
```

Identity Token

Header

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "mj399j…"
}
```

Payload

```
{
  "iss": "https://idsrv3",
  "exp": 1340819380,
  "iat": 1340818761,
  "aud": "app1",
  "nonce": "j1y…a23",
  "amr": [ "pwd" ],
  "auth_time": 12340819300

  "sub": "182jmm199",
  "name": "Alice",
}
```

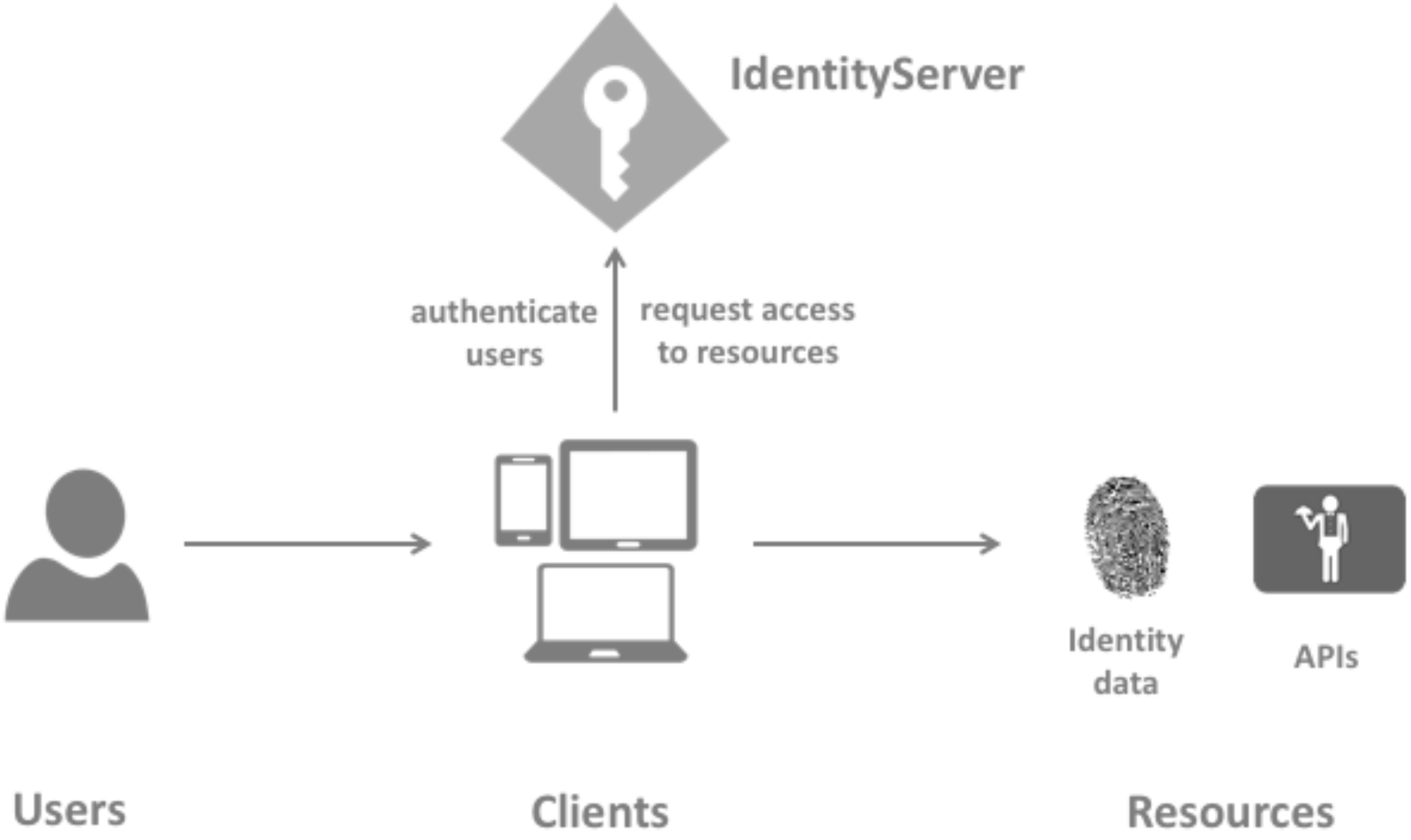
```
eyJhbGciOiJub25lIn0.eyJpc3MiOiJqb2UiLA0KICJleHAiOjEzMD.4MTkzODAsDQogImh0dHA6Ly9leGFt
```

Header **Payload** **Signature**

Identity Token Validation

- **According to 3.1.3.7 of the OpenID Connect specification**
  - The issuer name in the discovery document MUST exactly match the value of the **iss** claim.
  - The client MUST validate that the **aud** (audience) claim contains its **client_id** value registered at the issuer.
  - The **alg** value SHOULD be the default of RS256 or some other expected value.
  - The current time MUST be before the time represented by the **exp** Claim.
  - The **iat** claim can be used to reject tokens that were issued too far away from the current time.
  - The **nonce** value must match the nonce that was sent in the authentication request. A nonce claim MUST be present.
  - (some more checks for specific scenarios)

IdentityServer – the big Picture



IdentityServer

authenticate users

request access to resources

Identity data

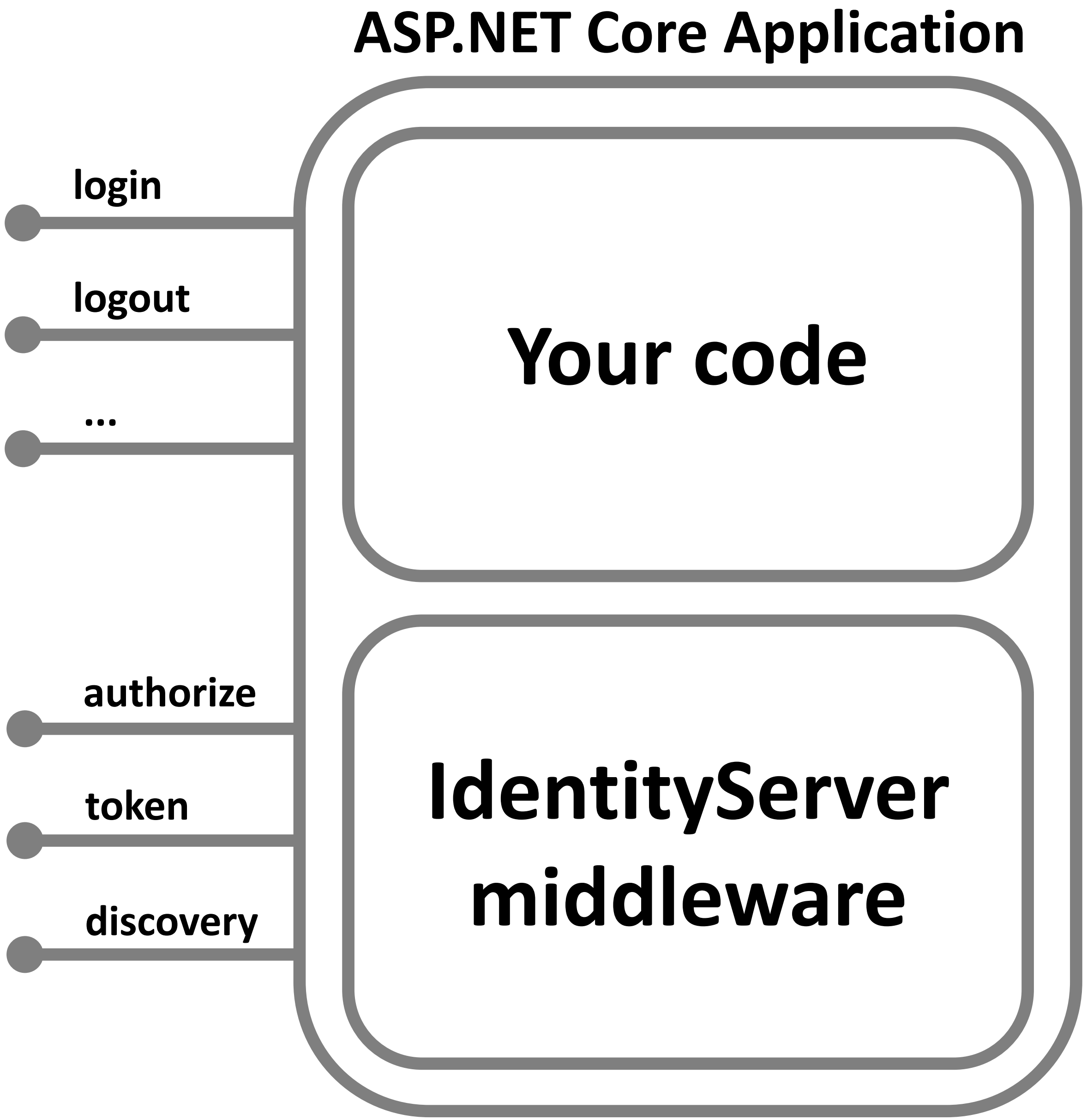
APIs

Users

Clients

Resources

Setting up


ASP.NET Core Application
login
logout
...
authorize
token
discovery
Your code
IdentityServer middleware

Connecting an MVC Client

```
services.AddAuthentication("Cookies")
    .AddCookie("Cookies", options =>
    {
        options.LoginPath = "/account/login";
        options.AccessDeniedPath = "/account/denied";
    })
    .AddOpenIdConnect("oidc", options =>
    {
        options.Authority = "https://demo.identityserver.io";
        options.ClientId = "mvc";

        options.TokenValidationParameters = new TokenValidationParameters
        {
            NameClaimType = "name",
            RoleClaimType = "role"
        };
    });
```

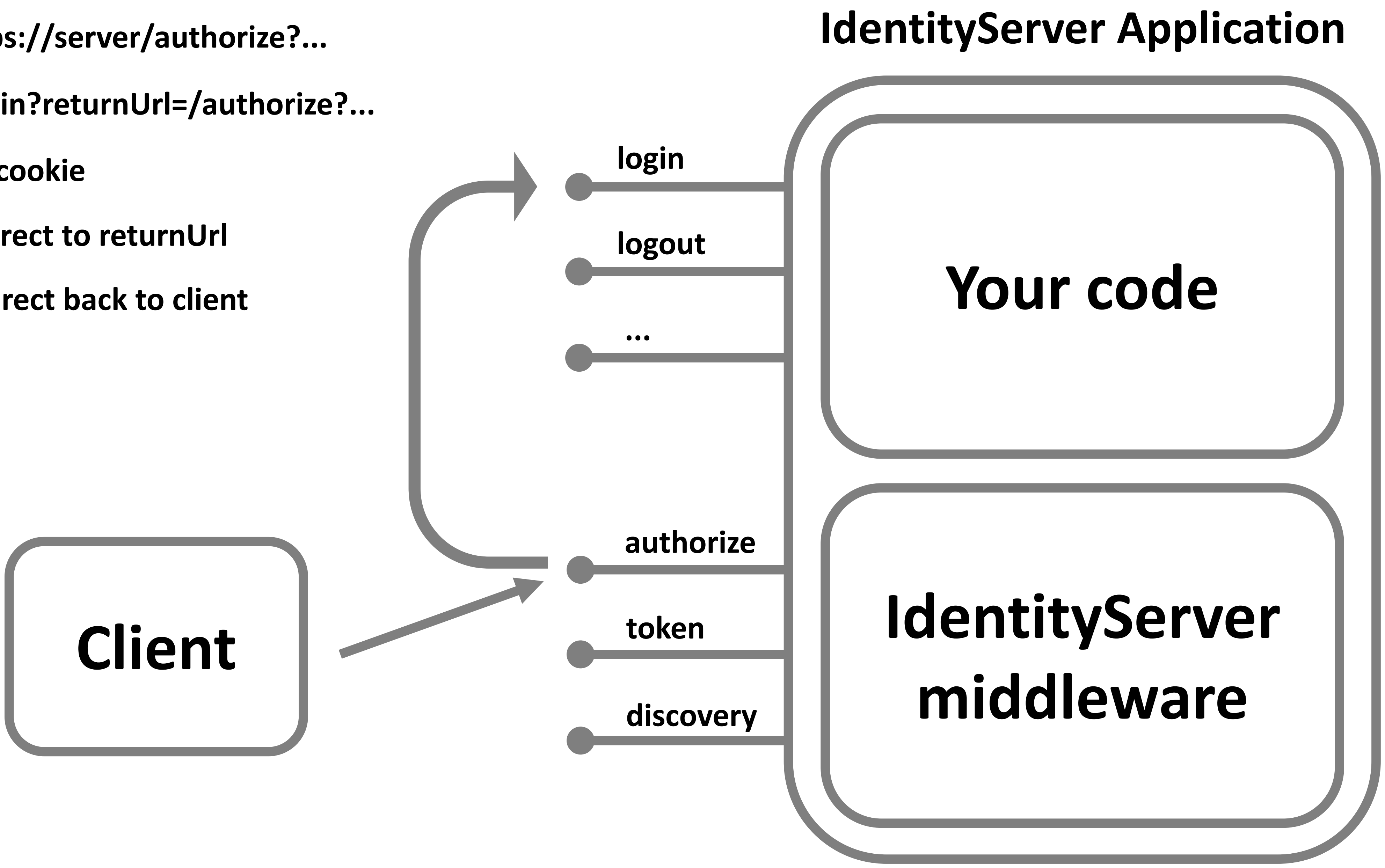
1) https://server/authorize?...

2) /login?returnUrl=/authorize?...

3) set cookie

4) redirect to returnUrl

5) redirect back to client



Summary

- **OpenID Connect is an authentication protocol for modern applications**
  - web, mobile, native…
  - simplified configuration management via discovery
  - designed around browser based user interactions

- **Certification makes sure implementations are spec compliant**
- **Close relationship to OAuth 2.0 makes adding APIs very easy (stay tuned!)**