

Microsoft FHIR Server implementation to support SMART on FHIR and U.S. g(10) requirements

Jared Erwin, Microsoft Corp.



HL7 FHIR DevDays 2023 | Hybrid Edition, Amsterdam | June 6–9, 2023 | @HL7 | @FirelyTeam | #fhirdevdays | www.devdays.com

ORGANIZED BY



Who am I?

- Jared Erwin
- Senior Software Engineer at Microsoft
 - Azure Health Data Services – FHIR Server

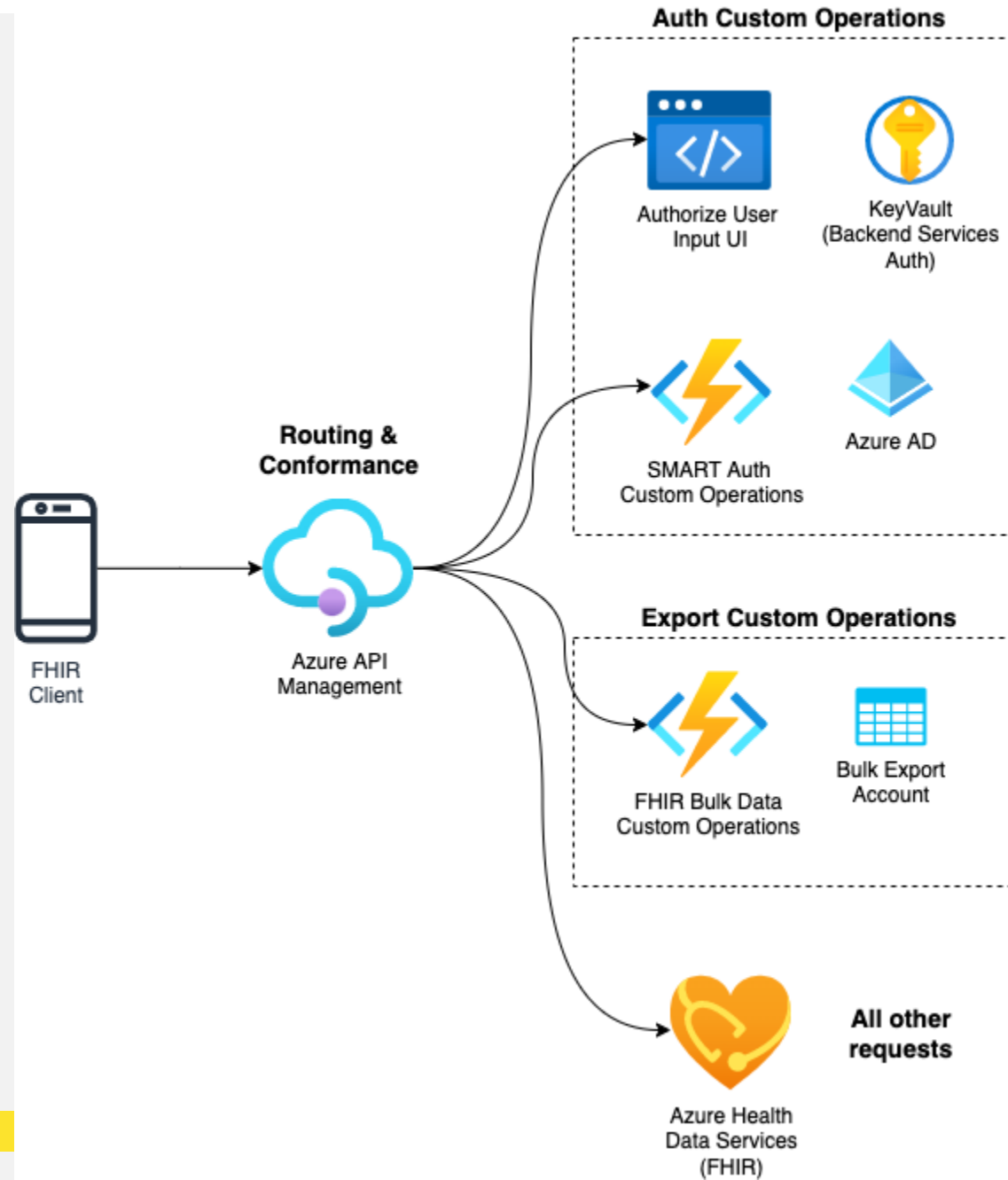


Overview of g(10)

- What is g(10)?
 - Set of certification requirements for Health IT certification in the USA
 - <https://www.healthit.gov/test-method/standardized-api-patient-and-population-services>
 - Designed to improve access to health care data
 - Driven by the 2015 21st Century Cures Act and ONC Final Rule
 - Relies on FHIR, US Core and SMART on FHIR
 - Went into effect Dec 2022
- Inferno test suite

Challenges integrating with existing IDP

- SMART on FHIR
 - Scope syntax
 - How to get fhirUser identity to the FHIR API
 - Performant queries when restricting data access
- Bulk data/export requirements, 384 encryption
- Missing data requirement in US Core



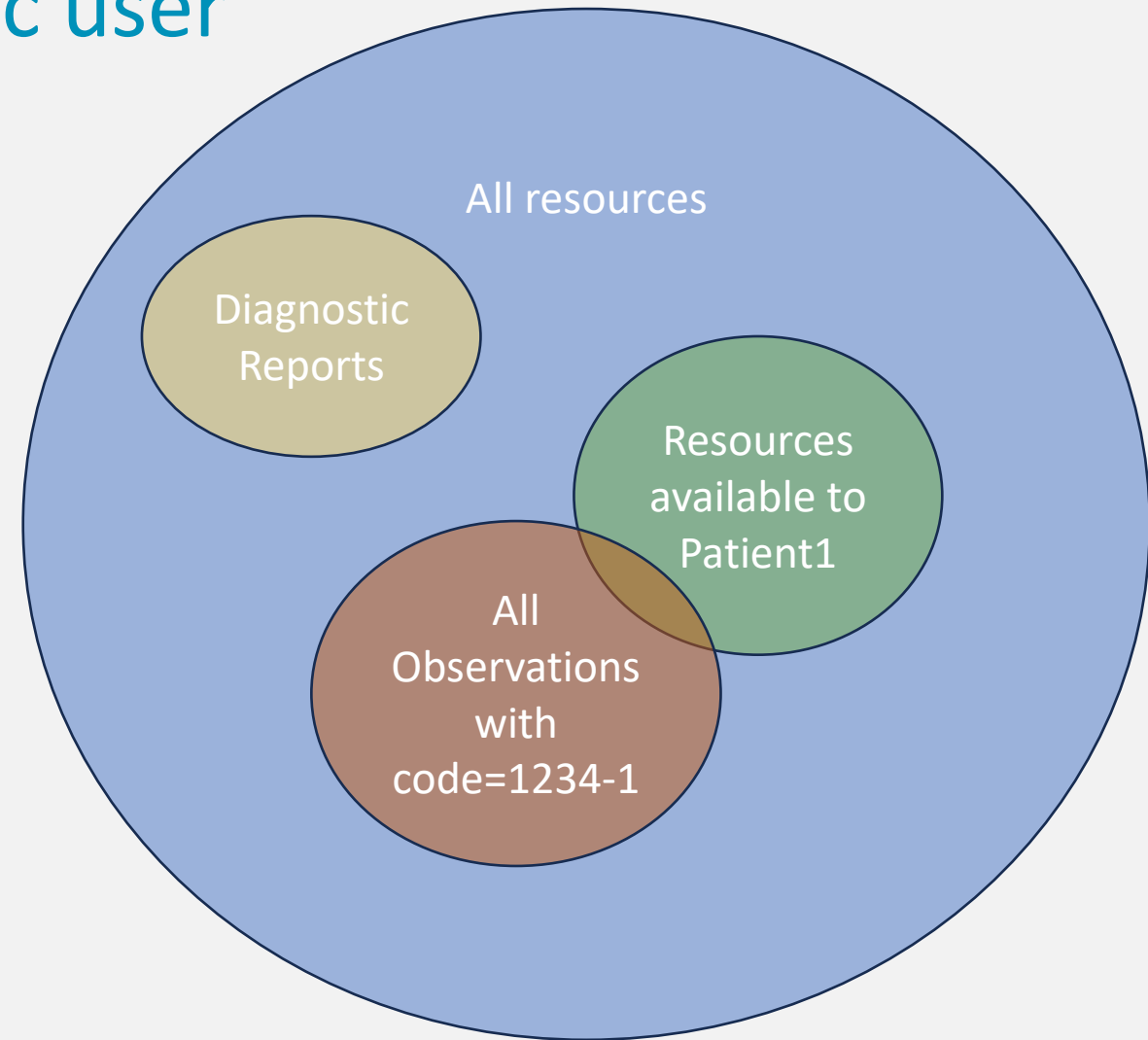
fhirUser information

- SMART indicated fhirUser shall be available in the id_token
- We included the same claim in the access token

Limit access to data by specific user and scope

- `/Observation?code=loinc|1234-1`
- `fhirUser=Patient1`
- `Scope=patient/Observation.read`

- `Scope=patient/DiagnosticReport.read`



Performant queries with restricted access

- Ensure the restrictions are processed by the data layer
- Data layer agnostic expression tree



Azure Active Directory limitations

- Scope syntax
 - / and *
 - patient/*.read = patient.all.read
- ~~384 Encryption for bulk data~~

Registering a new client app

[Refresh](#) | [Got feedback?](#)

i The "Admin consent required" column shows the default value for an organization. How where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins. All the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [✓ Grant admin consent for Health Architectures](#)

API / Permissions name	Type	Description
v Azure Healthcare APIs (1)		
patient.Observation.read	Delegated	patient.Observation.read
v Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile

To view and manage consented permissions for individual apps, as well as your tenant's

Request API permissions

<input type="checkbox"/>	launch	...
<input type="checkbox"/>	online_access ⓘ online_access	No
<input type="checkbox"/>	user_impersonation ⓘ Access Azure Healthcare APIs	No
> launch		
v patient (1)		
<input type="checkbox"/>	patient.all.read ⓘ patient.all.read	No
<input type="checkbox"/>	patient.AllergyIntolerance.read ⓘ patient.AllergyIntolerance.read	No
<input type="checkbox"/>	patient.CarePlan.read ⓘ patient.CarePlan.read	No
<input type="checkbox"/>	patient.CareTeam.read ⓘ patient.CareTeam.read	No
<input type="checkbox"/>	patient.Condition.read ⓘ patient.Condition.read	No
<input type="checkbox"/>	patient.Device.read ⓘ patient.Device.read	No
<input type="checkbox"/>	patient.DiagnosticReport.read ⓘ patient.DiagnosticReport.read	No
<input type="checkbox"/>	patient.DocumentReference.read ⓘ patient.DocumentReference.read	No
<input type="checkbox"/>	patient.Encounter.read ⓘ patient.Encounter.read	No
<input type="checkbox"/>	patient.Goal.read ⓘ patient.Goal.read	No
<input type="checkbox"/>	patient.Immunization.read ⓘ patient.Immunization.read	No
<input type="checkbox"/>	patient.Location.read ⓘ patient.Location.read	No

[Add permissions](#) [Discard](#)

Missing data requirement

```
"participant" : [  
  {  
    "role" : [  
      { "coding" : [  
        {  
          "system" : "http://terminology.hl7.org/CodeSystem/data-absent-reason",  
          "code" : "unknown",  
          "display" : "unknown"  
        }  
      ]  
    }  
  ]  
},  
  "member" :  
  .  
  .  
  .
```

[HL7.FHIR.US.CORE\Missing Coded Data Example - JSON Representation - FHIR v4.0.1](#)

- Typically we would return data as we received it
- This requires a modification to the FHIR resource and a performance hit

Overview of Azure g(10) solution

- Azure Health Data Services Samples
 - [azure-health-data-services-samples/samples/patientandpopulationservices-smartonfhir-oncg10 at main · Azure-Samples/azure-health-data-services-samples · GitHub](#)

Summary

- FHIR resource server is wrapped with other components
- The Identity provider is important!
 - We can't always choose the IDP
 - It may be pre-existing
 - There may be other organizational priorities dictating the identity provider
 - Some communication between IDP and FHIR is outside the spec
 - In our case fhirUser in the access token

Q&A

Contact

- During DevDays, you can find / reach me here:
 - Via Whova App – Speaker’s Gallery
 - jaerwin@microsoft.com
 - <https://www.linkedin.com/in/jarederwin/>
 - ..

ORGANIZED BY

