A whistlestop tour of FHIR API authentication and authorization

Dunmail Hodkinson

HL7 UK

Authentication

The process of identifying an individual

Authorization

Giving an individual access to operations and resources

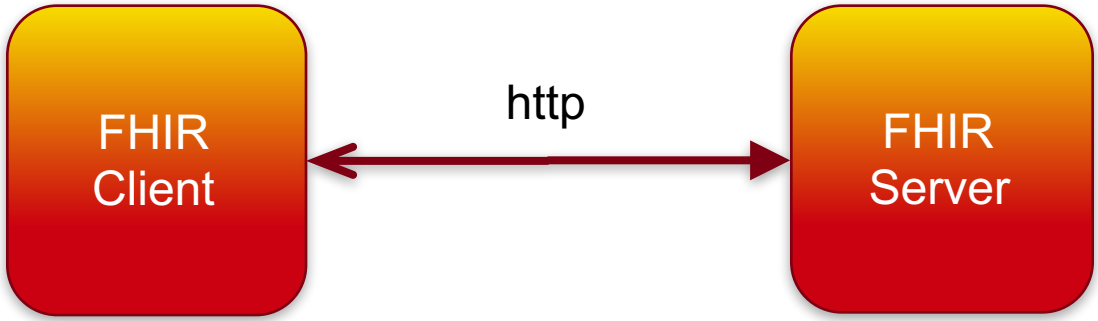
FHIR standard

- Does not include security
- Provides guidance and suggestions
- Includes supporting functionality

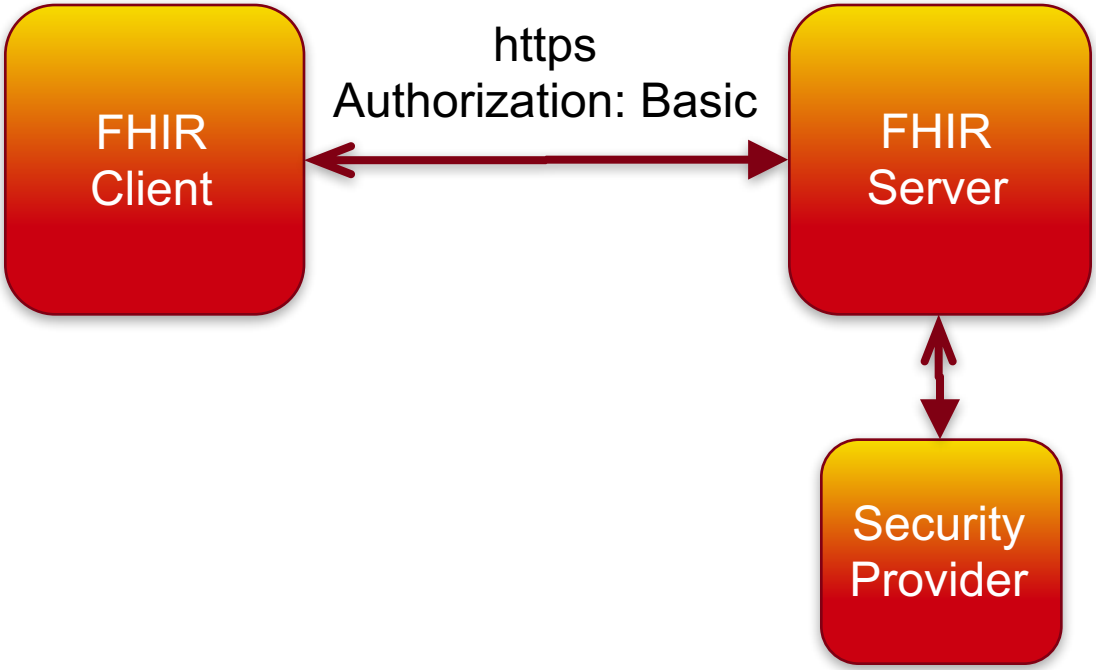
https://www.hl7.org/fhir/security.html#authentication
https://www.hl7.org/fhir/security.html#binding

PATTERNS

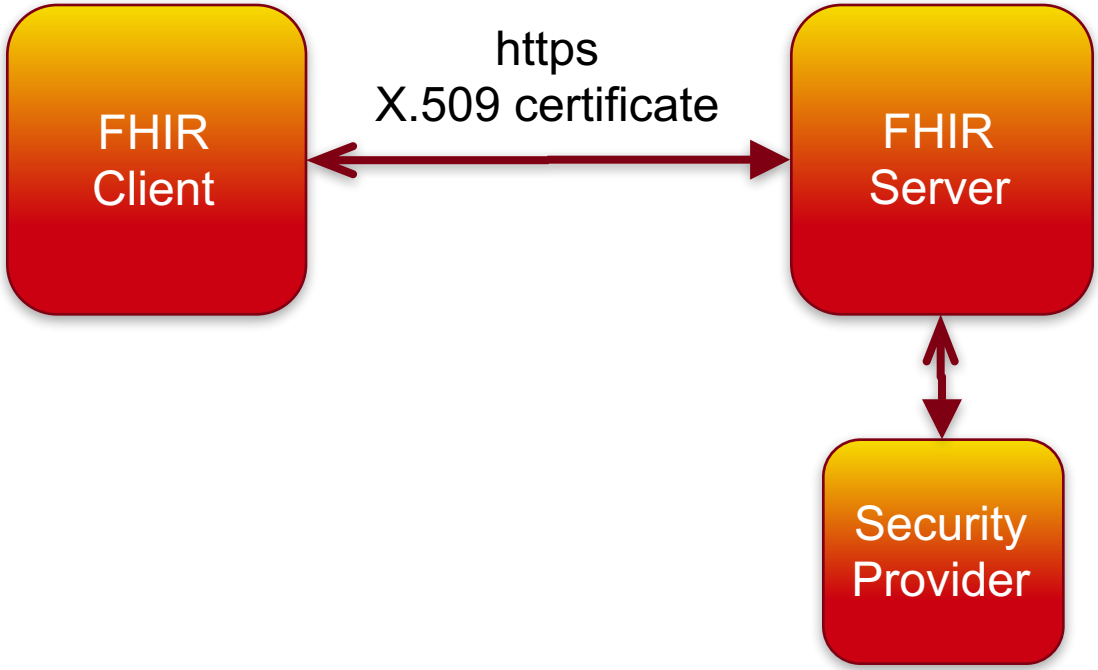
None



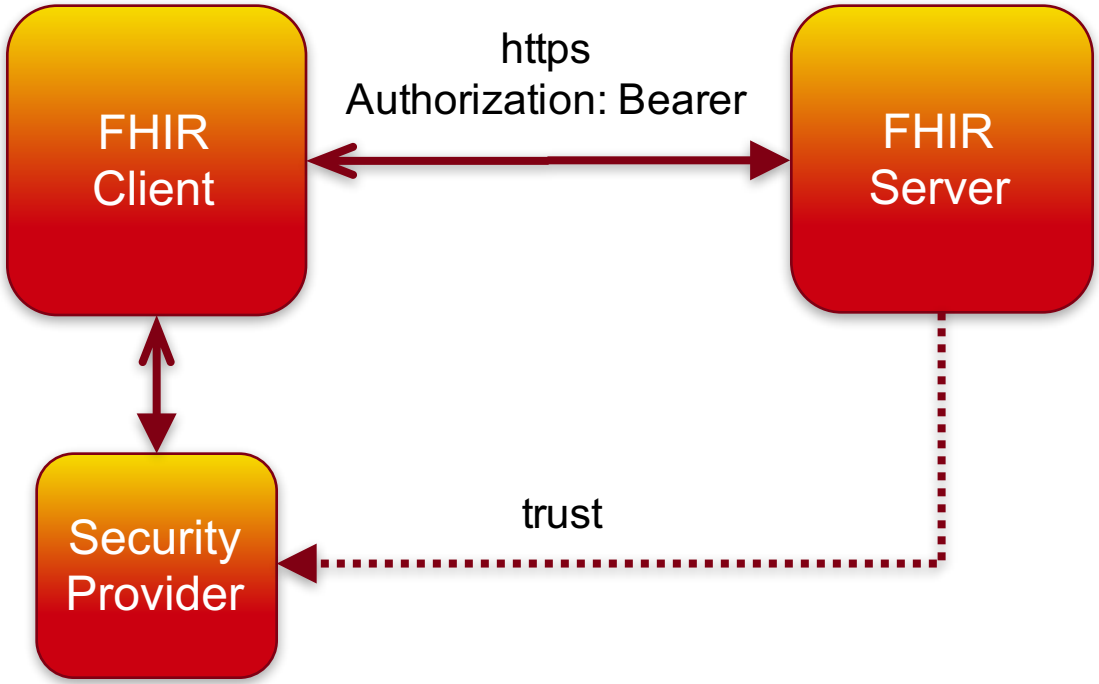
Basic


FHIR
Client
https
Authorization: Basic
FHIR
Server
Security
Provider

TLS-MA


FHIR
Client
https
X.509 certificate
FHIR
Server
Security
Provider

Bearer


FHIR Client
https
Authorization: Bearer
FHIR Server
Security Provider
trust

OAuth

‘An open protocol to allow secure authorization in a simple and standard way from web, mobile and desktop applications’

http://oauth.net/

SMART on FHIR

‘Medical apps that integrate into diverse EHRs at the point of care’

```
patient/*.read
user/*.*
patient/Observation.write
```

http://docs.smarthealthit.org/authorization/scopes-and-launch-context/

Health Level Seven UK

JSON Web Token (JWT)

‘an open, industry standard RFC 7519 method for representing claims securely between two parties’

```
{
    iss: 'https://auth.example.net',
    sub: 'user@example.net',
    nbf: 1463059456166,
    exp: 1463064578213,
    iat: 1463059366160,
    aud: ['https://fhir.example.net'],
    jti: '5794b4f6-90bb-41a2-8e11-27ff4adb8880',
}
```

https://jwt.io/

Health Level Seven UK

JWT claims for FHIR

```
{
    …
    fhir_scp: [
        '*'
    ],
    fhir_act: [
        'read:Patient,Observation',
        '$getRecord:Patient'
    ]
}
```

https://github.com/BlackPearSw/jwt-claims-fhir/blob/master/jwt-claims-fhir.md

SUPPORTING FUNCTIONALITY

Compartments

‘Each resource may belong to one or more logical compartments. A compartment is a logical grouping of resources which share a common property. … [They can] provide a definitional basis for applying access control to resources quickly.’

```
[base]/fhir/Patient/123/Condition
```

https://www.hl7.org/fhir/compartments.html

Contract resource

‘A formal agreement between parties regarding the conduct of business, exchange of information or other matters’

https://www.hl7.org/fhir/contract.html

Consent resource

‘A record of a healthcare consumer’s privacy policy, which is in accordance with governing jurisdictional and organization privacy policies that grant or withhold consent.’

http://hl7-fhir.github.io/consent.html

Dunmail Hodkinson

dunmail@blackpear.com

@dunmailh