API Security

Demystifying REST/GraphQL Security

Shiu Fun Poon (shiufun@us.ibm.com)

Senior Technical Staff Member

Swetha Sridharan (Swetha.Sridharan@ibm.com)

Senior Offering Manager

API Connect and Gateway Cloud and Cognitive Software

Security

- Protect data at REST
- Protect data at TRANSIT
  - Point to point
- Message Protection
  - Confidential
  - Integrity

- Authentication
  - Is the user who he/she assert to be
  - Is the application valid
- Authorization
  - Is user allowed to access the data, perform the operation
  - Is the application allowed to access the data, perform the operation
- Protect against resource exhaustion/Information Leakage/API abuse
- Auditing
  - Who has performed What, at When (WWW)

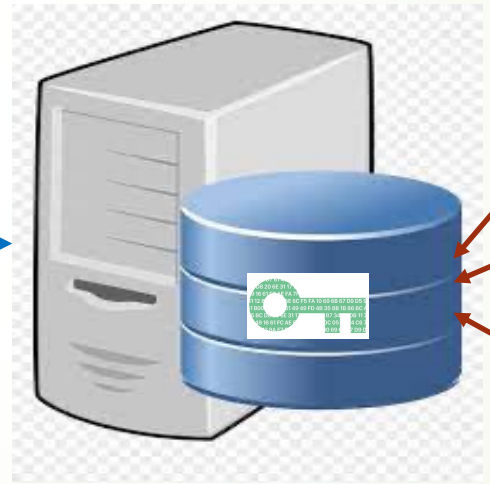
REST

- Representational State Transfer
- Doctoral dissertation by Roy Fielding, in 2000
- Standard HTTP verb/protocol
  - GET, POST, PUT, PATCH, DELETE
- Uniform interface/multiple endpoints
- Stateless (*) / Cacheable
- Client/Server

- API Developer defines the interface

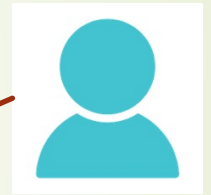
Protect Data At REST

Signature/
Encryption



Configuration/
Setting/
API/Application definition/
Application Data

Administrator



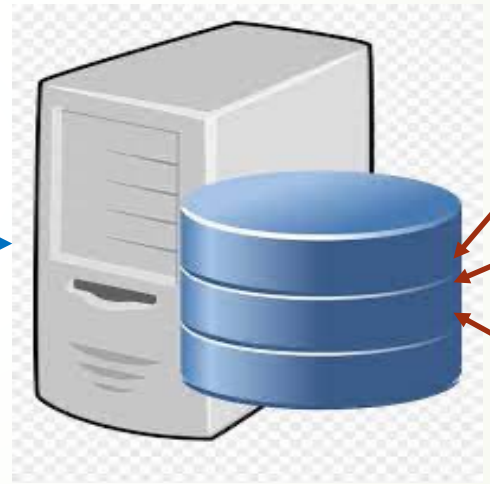
Application developers

API developers

Protect Data At Transit

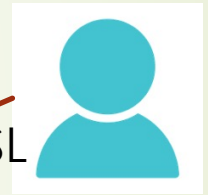
(m)TLS/SSL

Encryption(msg)



Administrator

(m) TLS/SSL



(m) TLS/SSL

Application developers

(m) TLS/SSL

API developers

Point to Point protection (pipe) : TLS/SSL, SSH, VPN
Message Level (target protection) : encryption (for a target audience)

Message Level Protection

Sign(msg)

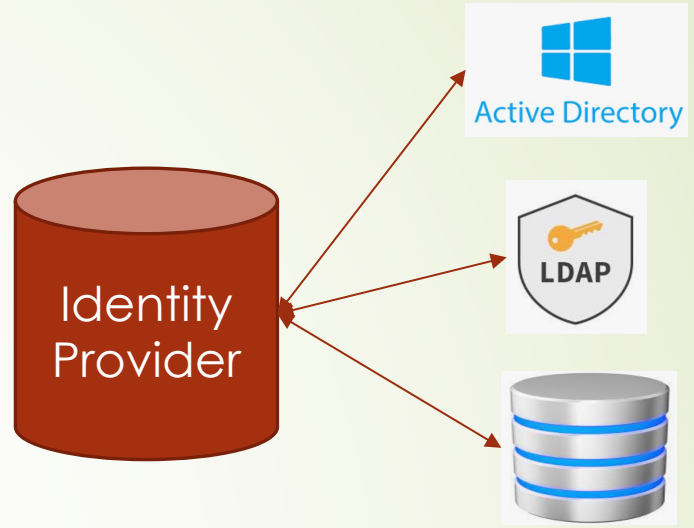
Encryption(msg)

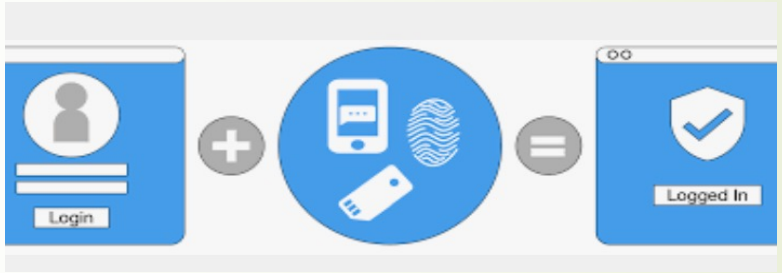
Message Level (target protection)
- encryption (confidential)
- signature (non-repudiation, integrity protection)

Public/Private Key vs Shared Secret

Authentication

- The right user ?
  - Username/password/(Biometric)
  - OAuth/OIDC
  - PKIX (public/private key)
  - Assertion (e.g. JSON Web Token, JWT)
  - Cookie/Spengo/Kerberos





- The right application ?
  - Application id/Application secret
  - OAuth
    - Public/confidential (https://datatracker.ietf.org/doc/html/rfc6749)
  - PKIX (public/private key)
    - TLS/SSL/Signature
  - Assertion (e.g. JSON Web Token, JWT)

Authorization

- The user permission
  - Action + Resource + Who (+ context) (+ constraint) (+obligation)
  - Role based access
  - Delegate access/permission
    - E.g. OAuth – delegate to application
- The application permission
  - OAuth
    - scope
    - Type of application (grant type)

Protect against ..

- Resource exhaustion
  - CPU/Memory/subsystem resource that is needed to satisfy the API runtime
  - Cost of executing/Complexity of running the API
    - concurrently access of the related API (potentially against the same resource)
  - Type of access (READ vs UPDATE/CREATE/DELETE)
  - High availability/Disaster Recovery
- Information leakage
  - Allow list : only allow data if data is in the allow list
  - Block List : data is removed/redact if in the block list
  - **ERROR condition**
  - User's data (PII/GDPR..)
- API abuse
  - Does the request/response conform to the specification, schema validation
  - Size of data/Size of payload
  - Data format (int, string, bool)

Auditing

- Compliance
- Regulation
- Who is doing What, at When

- Consider what kind of data is being tracked
  - The retention policy
  - User's sensitive data/PII (should those be redacted/mask)

- Potential
  - This can be used to fine tune next iteration of API
  - Suspicious behavior

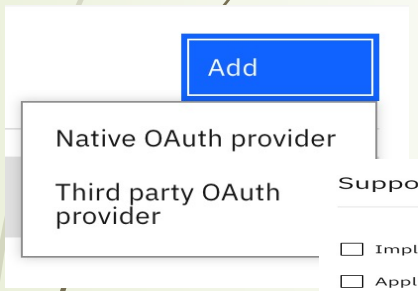
Available Security Mechanism

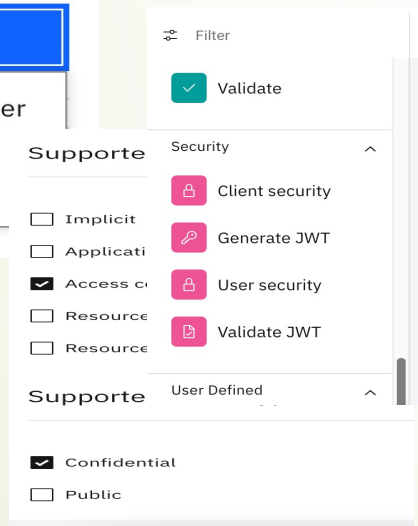
OpenAPI

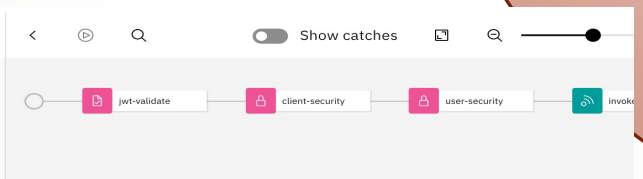
apiKey
http (basic, Bearer)
oauth2 (4 core grant type)
openIdConnect

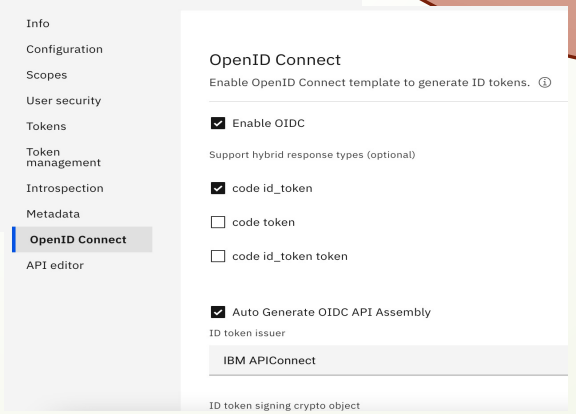
API Enforcement Gateway

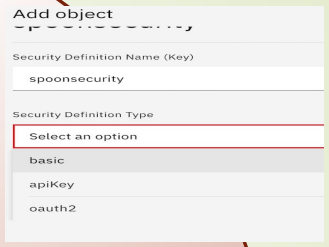
apiKey
Basic
oauth2 (4 core grant type)
openIdConnect *
Application mTLS
JSON Web Token AZ grant type
JSON Web Token
Spengo/Kerberos
SAML
Cookie (SMSession)
Custom ..



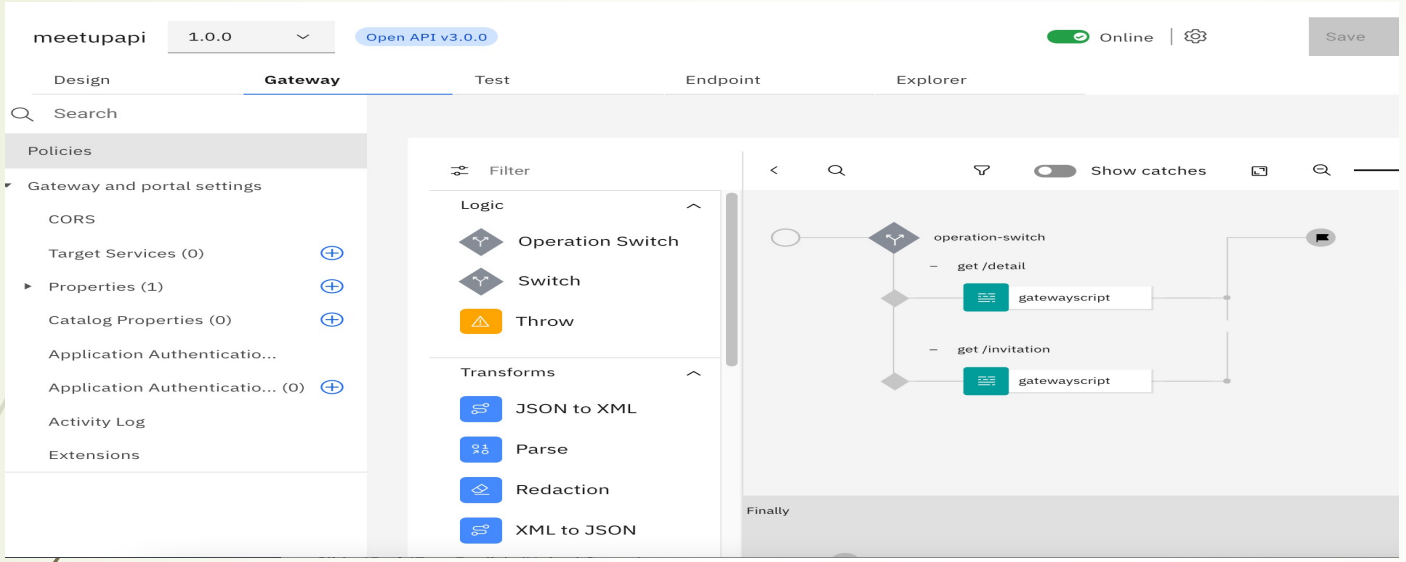


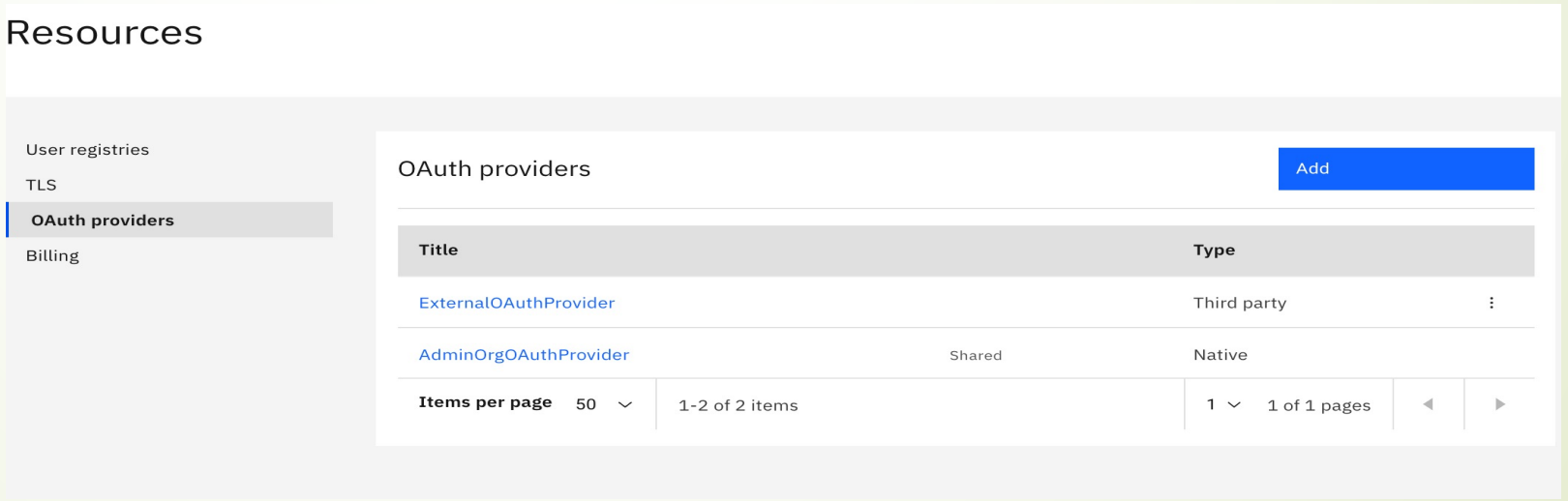




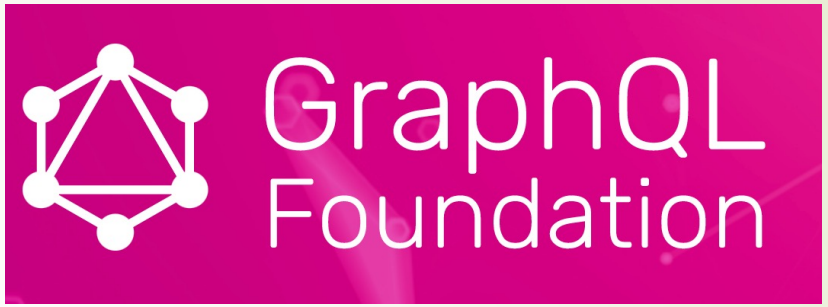


Creating OpenAPI/OAuth Provider





GraphQL

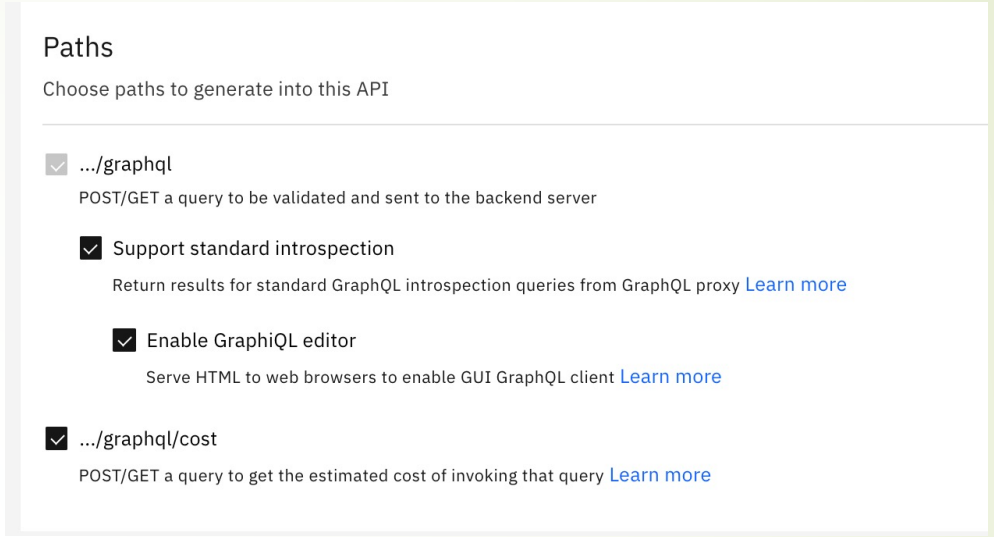


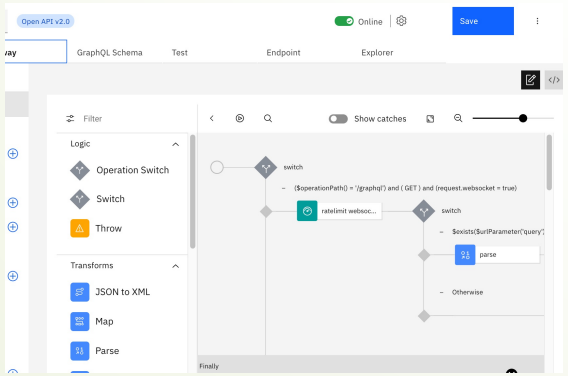
- Developed by FaceBook
- Query & Mutation language
- Standard HTTP verb/protocol
  - GET, POST
- Single endpoint
- Flexibility, and great for accessing relational data

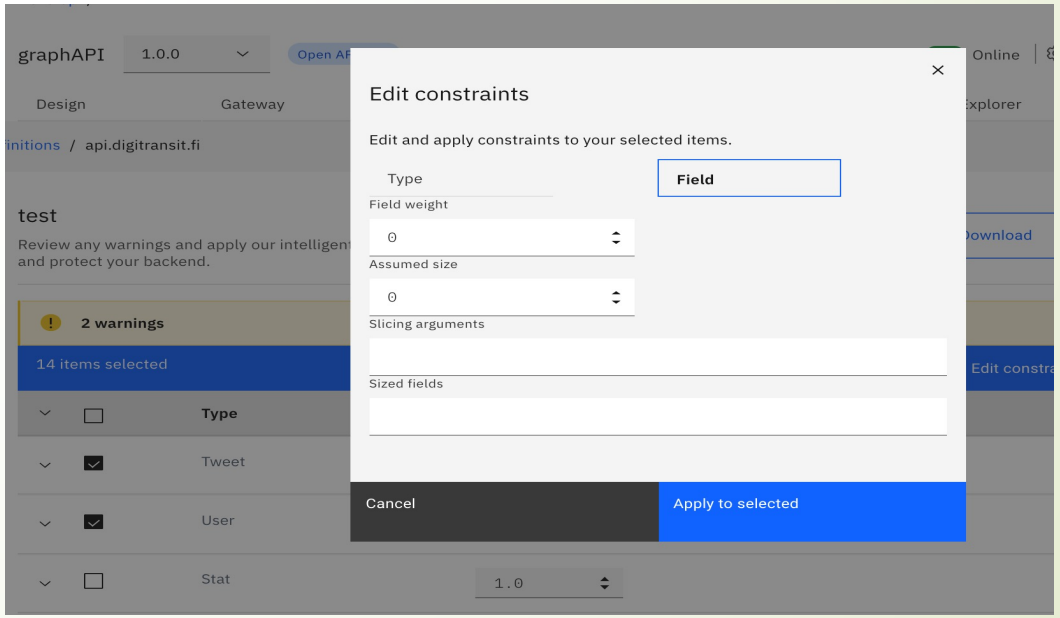
- Application developer defines interface

Similar and yet

- Cost of running the Query
  - Complexity
    - Nested data/Query depth
  - Timeout
- Data type checking
  - Schema validation
  - Data type checking
  - Encoding

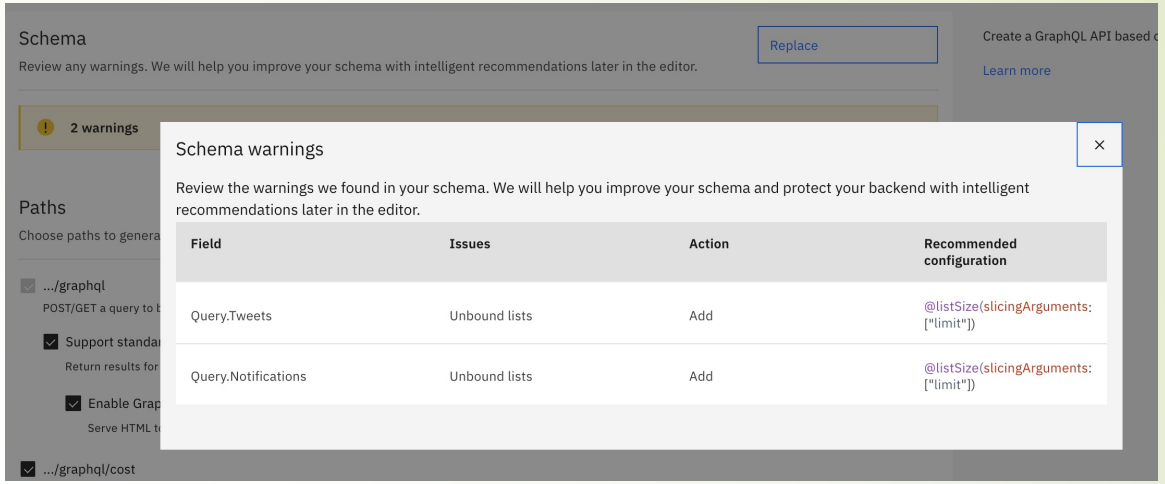


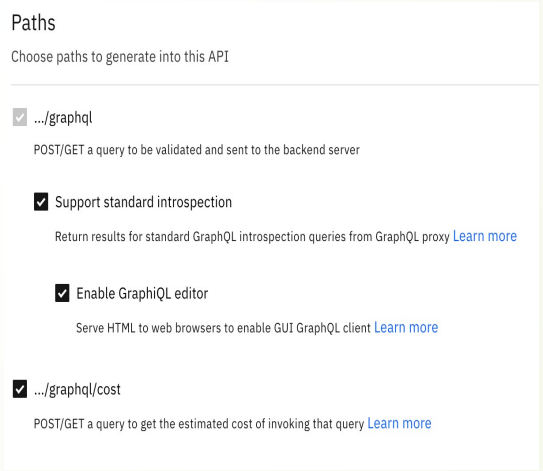


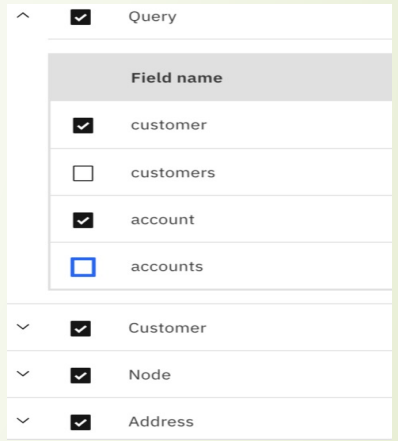


Similar and yet

- Amount of data
  - Pagination
  - Data size checking
- Authorization
  - Resolver
  - Schema filtering
- Based on the scenario/support
  - Disable introspection
  - Rename the standard endpoint (/graphql) to (/<yourchoice>)
  - Generic error response







Upcoming Meetup on GraphQL

- https://www.crowdcast.io/e/graphql-advantages

What IBM APIC offers – Manage/Develop

- Security from creation of the runtime, set up topology to runtime
- Using microservices technology, with Kubernetes
  - Allow customization
  - Provide High Availability
- Configuration is managed and stored securely
  - Sensitive configuration information is encrypted during storage
- Support Transport protection (includes TLS 1.3) with external subsystems
- Follow industry standard with OAuth 2.0 for protecting access to APIc
- Utilize Role Based Access Control
  - Allow custom role to be created to fine tune the access control
  - Allow integration with LDAP group to map to roles
- Auditing

What IBM APIC offers – Runtime of application

- OpenAPI security supports
  - Basic, ApiKey, OAuth, OIDC (*), JWT authorization grant type
  - Customize solution (e.g. customize how the APIKey can be extracted)
- OAuth Provider
  - Native (IBM APIC is the OAuth provider)
    - Customize each process in the assembly step
    - OIDC (*)
  - External OAuth Provider
    - RFC 7662 – OAuth Introspection Support
- JSON Web Token Policy (generation/validation)
- Rate Limit (Plan/per assembly)
- Custom (gatewayscript/xslt policy)

Reference

- API Security OWASP Top 10
  - https://www.youtube.com/watch?v=UtZv2pkM5Q0
- APIC v10 Demo
  - https://ibm.biz/apic-v10demos
- Securing your API with IBM API Connect
  - https://www.ibm.com/cloud/api-connect/secure