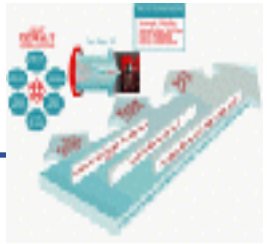
Microservices: API Security

Graeme Burnett

Jul 2017

rgb@enhyper.com

The Rise of the API - Microservices

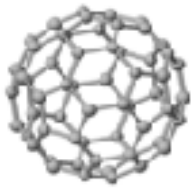


- SOAP/SASL
  - HTTP Transport
  - XML Infoset/Serialised XML
  - WS-Security
  - Advantages: Tunneling
  - Disadvantages: Slow to parse, Schema orientated
- RESTful Services
  - HTTPS Transport (stateless)
  - GET/POST - send/receive
  - JSON, BSON, YAML, XML
  - Schema-less: self-describing messages
  - Code on demand (YAML)
- The Nordic APIs
  - OAuth 2.0 - ephemeral access control (Authentication/Authorisation)
  - OpenID Connect - Identity
  - SCIM - System for Cross-federation Identity Management
  - XACML - Access Control

Data, Data Lakes and NoSQL Persistence

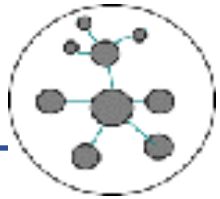
- Schema vs Schema-less
  - Schema: tightly coupled, difficult to change/evolve
  - Schema-less: Raw data is captured, timestamped, replicated
- Data Formats: XML vs JSON vs YAML
  - XML: Schema orientated, inefficient, difficult to parse
  - JSON: Self-describing, easy to parse, not as inefficient as XML
  - BSON: Binary JSON - more efficient
  - YAML: Simple format, easily parsable, human readable, can carry code. The future is readable!
- Data Lakes
  - No parsing on capture
  - Provenance: timestamp on capture, distributed ledger, PBFT
  - Transformation on use (real-time integration)
  - Machine navigable meta-data
  - Machine categorisation
  - AI: Analytics, toxic combinations, fraud detection
- NoSQL
  - Hash/Blob storage
  - Indexed fields
  - Schema-less
  - More a cache than transactional DB
  - Eventual Consistency
  - Asynchronous
  - Lack of access control
  - No Encryption

The Nordic APIs - The Neo Security Stack



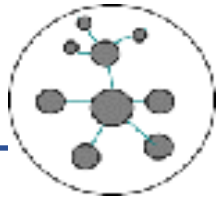
- De Facto in Web based APIs
  - OAuth 2.0
  - OpenID Connect
  - SCIM
  - XACML
- OAuth 2.0
  - Service registration using OpenID credentials
  - Near realtime authorisation and access control
- OpenID Connect
  - Session and Identity management
- SCIM
  - System for Cross-federated Identity Management
- XACML
  - Fine-grained, attribute-based access control policy language (ABAC)
  - Real-time

Microservices



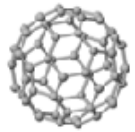
- Definition
  - Web-based functions/methods
  - Need a directory service (WSDL, UDDI)
- History
  - Exploded in 2000 when the internet was immature - the chasm was entered
  - Needs a directory service (WSDL, UDDI)
  - Current players: Mulesoft, pub nub - the second wave begins
- What Next
  - Dynamic recovery - service fails, you call another from the marketplace
  - Reputation-based market: Failure rate, performance, scalability
  - Enterprise grade: SLAs
  - Paid-for Services: microcash - one off payment, subscription
  - Anonymous Applications: Paid for by bitcoin
  - Secure Containers: inter service collaboration and orchestration

Microservices: Pros and Cons



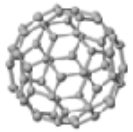
- Pros
  - Data: provenance, analytics, quality, accuracy, delivery, integrity and availability
  - Design: Service assembly/composition vs component driven service development
  - Reuse: Dynamic functionality by service discovery
  - Static Data: now becomes cached data increasing performance
  - Reduced cost: through reuse
  - Higher performance: dynamic discovery of better performing services
  - SLA: meet the SLA automatically via demand our cost
  - Secure: Real-time authentication and authorisation. Dynamic, fine-grained access control
  - Business Security: Anonymous service consumption. No one knows your applications
- Cons
  - Response overhead.

OpenAPI



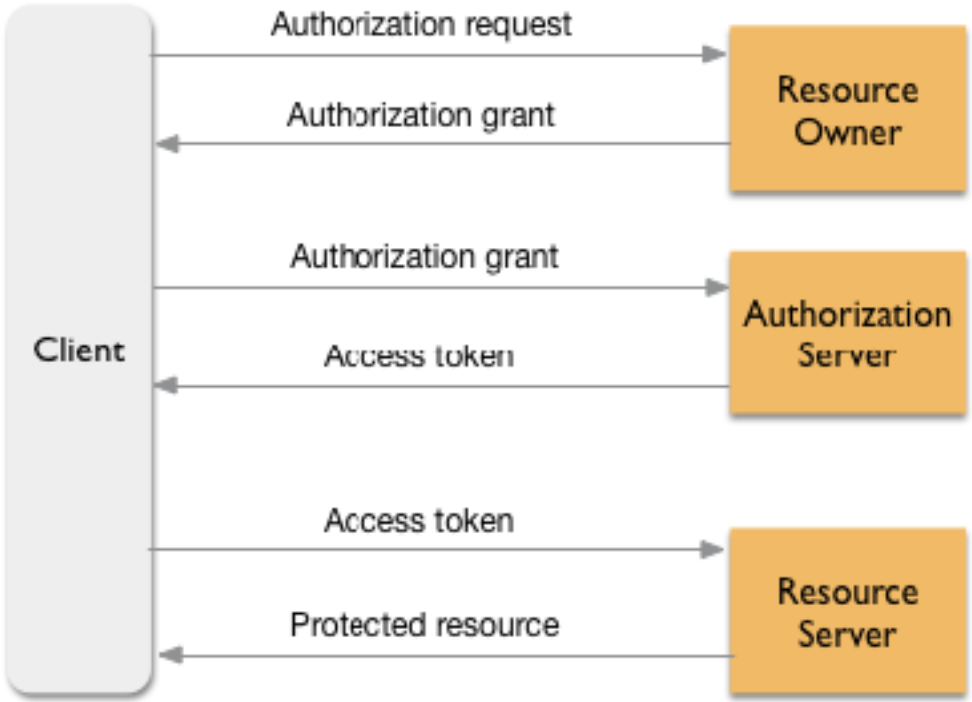
- OpenAPI
  - Attempt to standardise the API spec
  - Just reached critical mass (Jul 2017)
  - Quango driven
- Swagger.io
  - Design: Tool for designing APIs
  - Codegen: Generate API code in multiple languages
  - Document: produce documentation to assist development or server and client code
- GraphQL
  - Query Language: solves under and over fetching of data
  - Blend: fetch from multiple APIs at once

Neo Security Stack Implementation

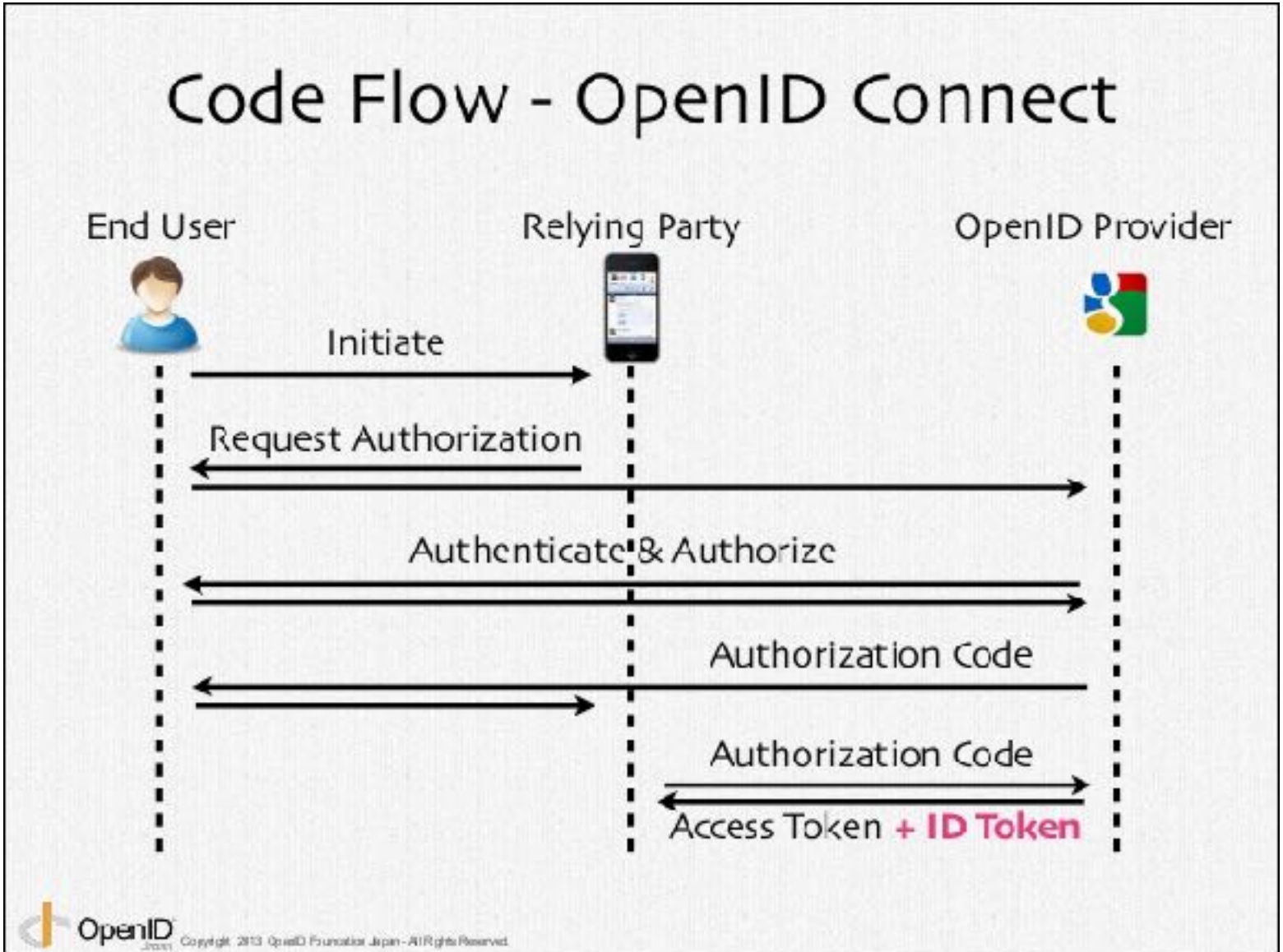


- Identity, Account, Groups, Roles Capture
  - Estate Mapping: federations, servers, groups and accounts
  - Superuser and Privileged Account discover
  - Robust Joiner/Mover/Leaver Process with Audit trail
- Applications, APIs and Services
  - Application, API and Service Inventory
    - Role mining
    - ACL mining
    - Authorised users
    - Date sources and sinks
- Identity and Access Management
  - Enterprise grade I&AM solution
  - Ping Identity, Twobo Systems, Axiomatics
- Application Integration
  - Remediation of AAA
- API Analysis, Development, Integration and Measurement
  - Quick win services
  - Integration to existing apps
  - Performance measurement
  - SOC integration

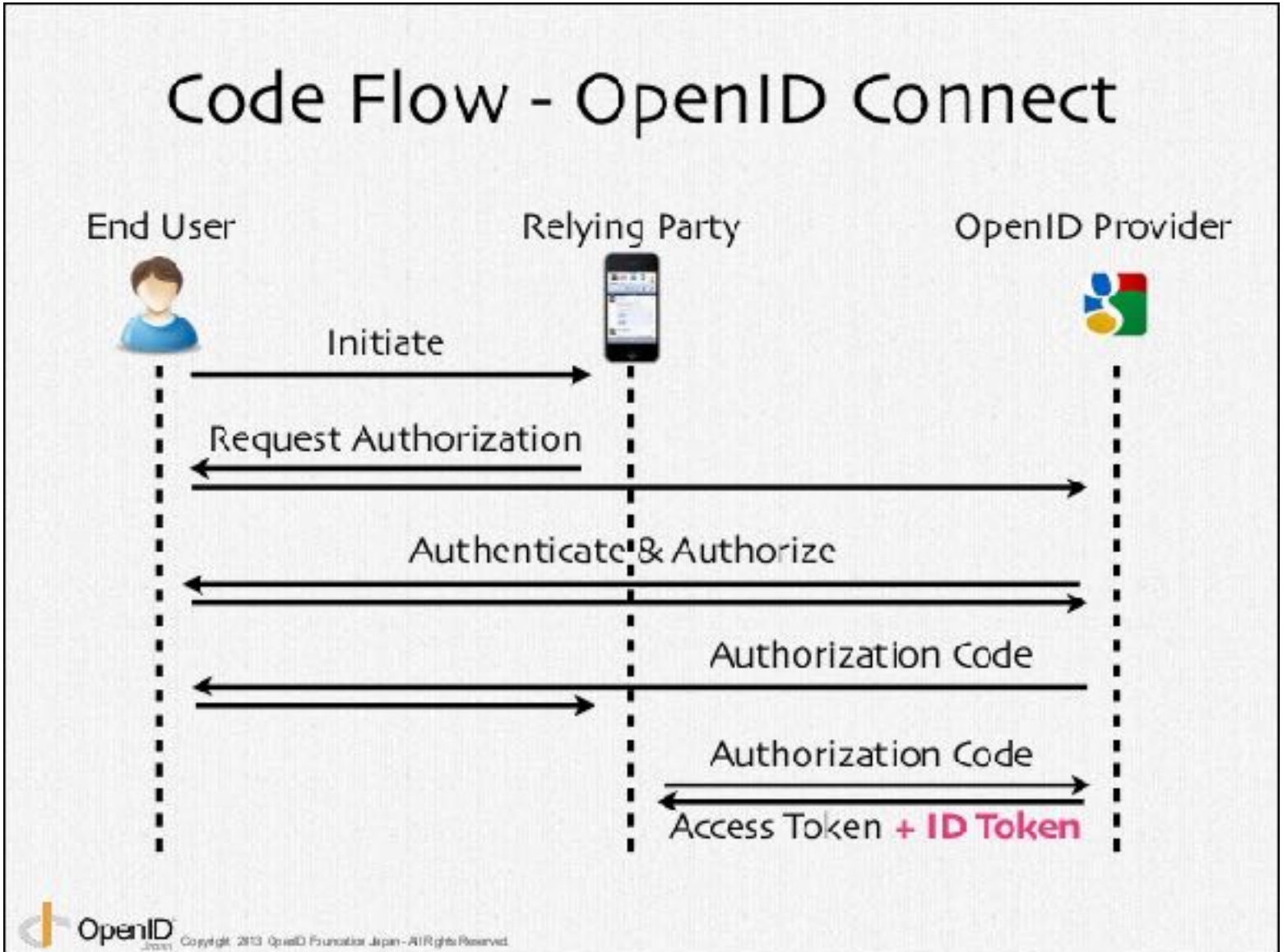
OAuth 2.0 In Action



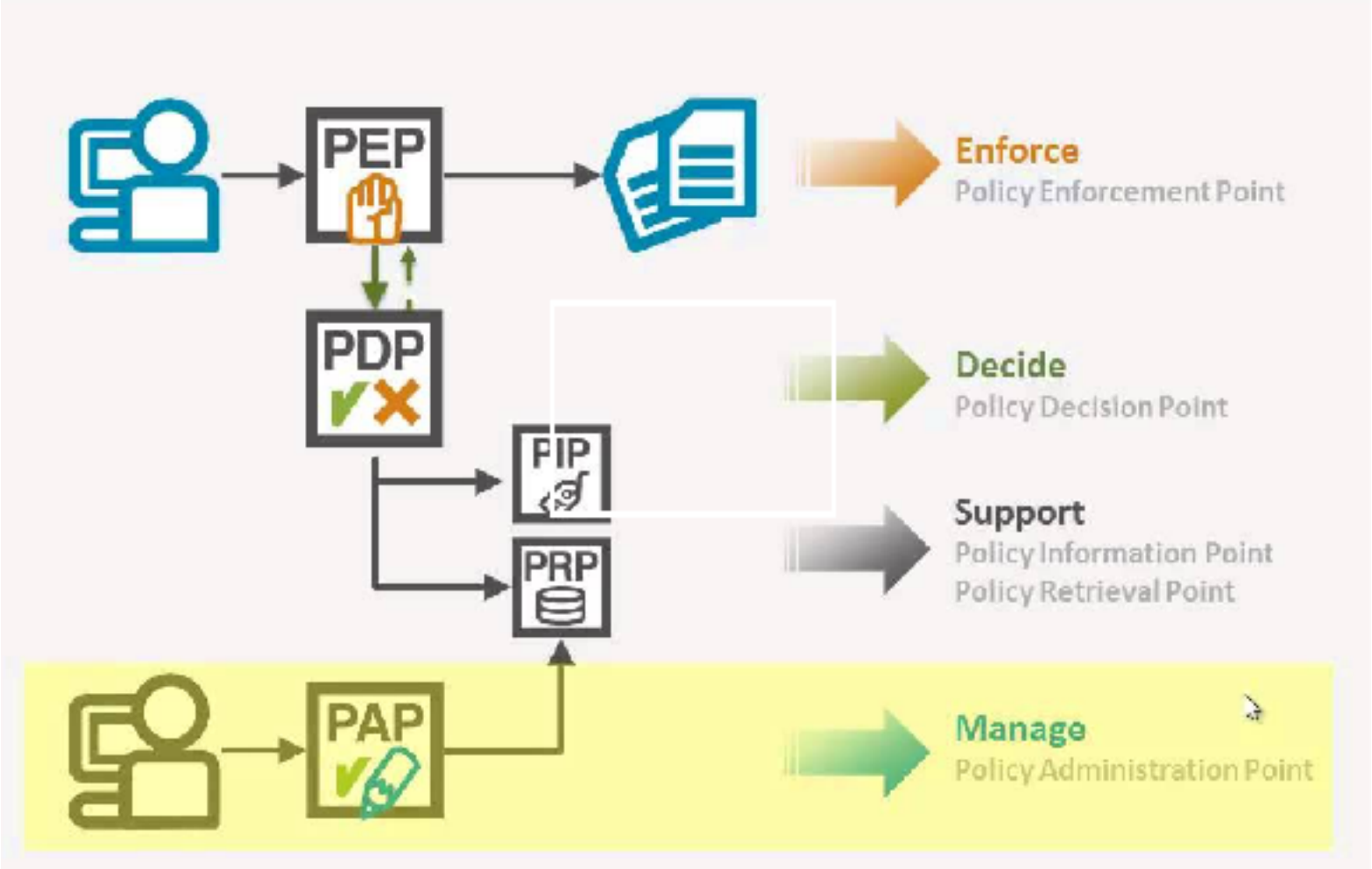
OpenID Connect



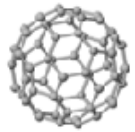
SCIM


Code Flow - OpenID Connect
End User
Relying Party
OpenID Provider
Initiate
Request Authorization
Authenticate & Authorize
Authorization Code
Authorization Code
Access Token + ID Token
OpenID
Copyright 2013 OpenID Foundation Japan - All Rights Reserved

XACML


PEP
PDP
PIP
PRP
PAP
Enforce
Policy Enforcement Point
Decide
Policy Decision Point
Support
Policy Information Point
Policy Retrieval Point
Manage
Policy Administration Point

Conclusion



- The world of application development has changed totally
- APIs and microservices combined with dynamic data filtering, decryption and presentation provide near real-time control allowing compliance with privacy regulations
- Dynamic failure handling for resilience
- Dynamic scalability to cope with service level
- Consumption of services paid for with digital currency
- Reputation-based market service marketplace
- Anonymous Applications