Enterprise Architecture

Service Security

How do we secure a service?

Securing MicroServices

- User name/password
- API Keys
  - Opaque API keys
  - Structured tokens e.g. JWT
- Protocols:
  - OAuth & OpenID
  - SAML

Securing MicroServices

- Where should we implement authentication ?
  - At gateway ?, At each service ?,..
- Where should we keep the credentials?
  - Shared DB for all services?
  - A dedicated micro service who owns it ?
- What about 3rd party? (e.g. login via Google)

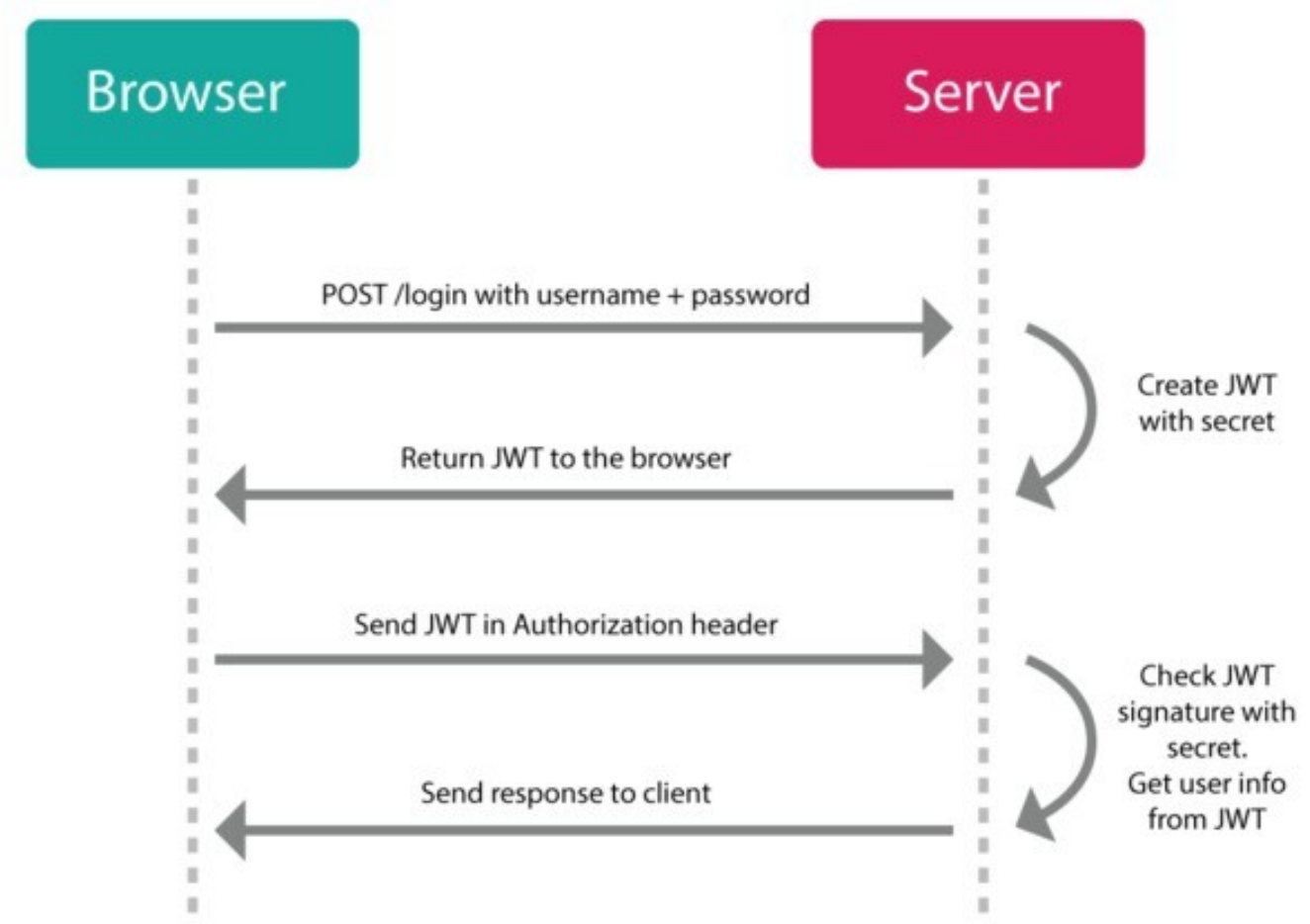
Trade offs

- Let’s check first 30 mins of
  - Securing Microservices with Spring Cloud Security| Will Tran
    - https://www.youtube.com/watch?v=USMl2GNg2r0
  - Slides:
    - https://www.slideshare.net/SpringCentral/securing-microservices-with-spring-cloud-security-53170178

Authentication as a service

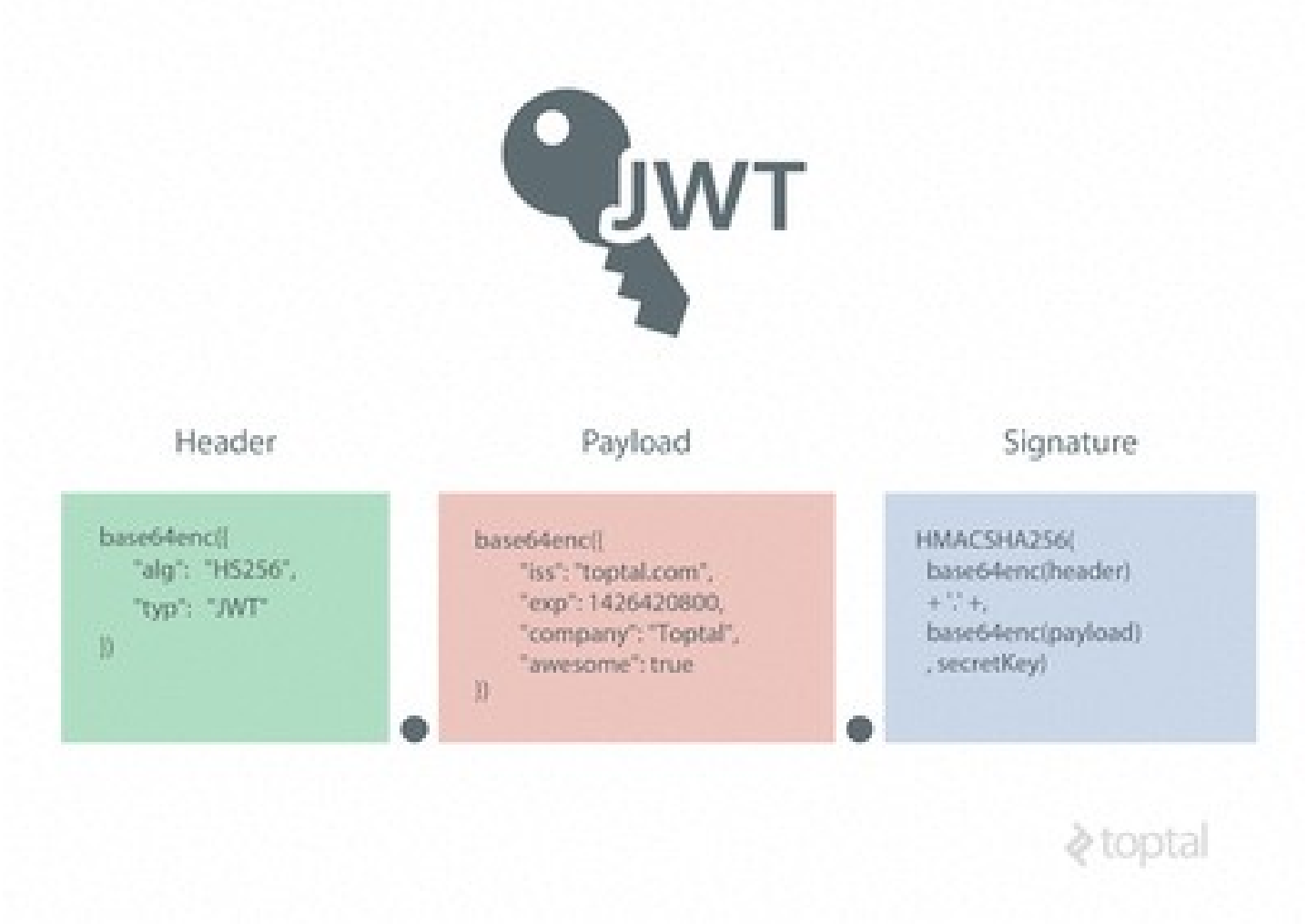
- If you got extra time:
  - Authentication as a Microservice| Brian Pontarelli
    - https://www.youtube.com/watch?v=SLc3cTlypwM

JSON Web Token (JWT)



http://robmclarty.com/blog/what-is-a-json-web-token

JSON Web Token (JWT)



http://www.toptal.com/web/cookie-free-authentication-with-json-web-tokens-an-example-in-laravel-and-angularjs

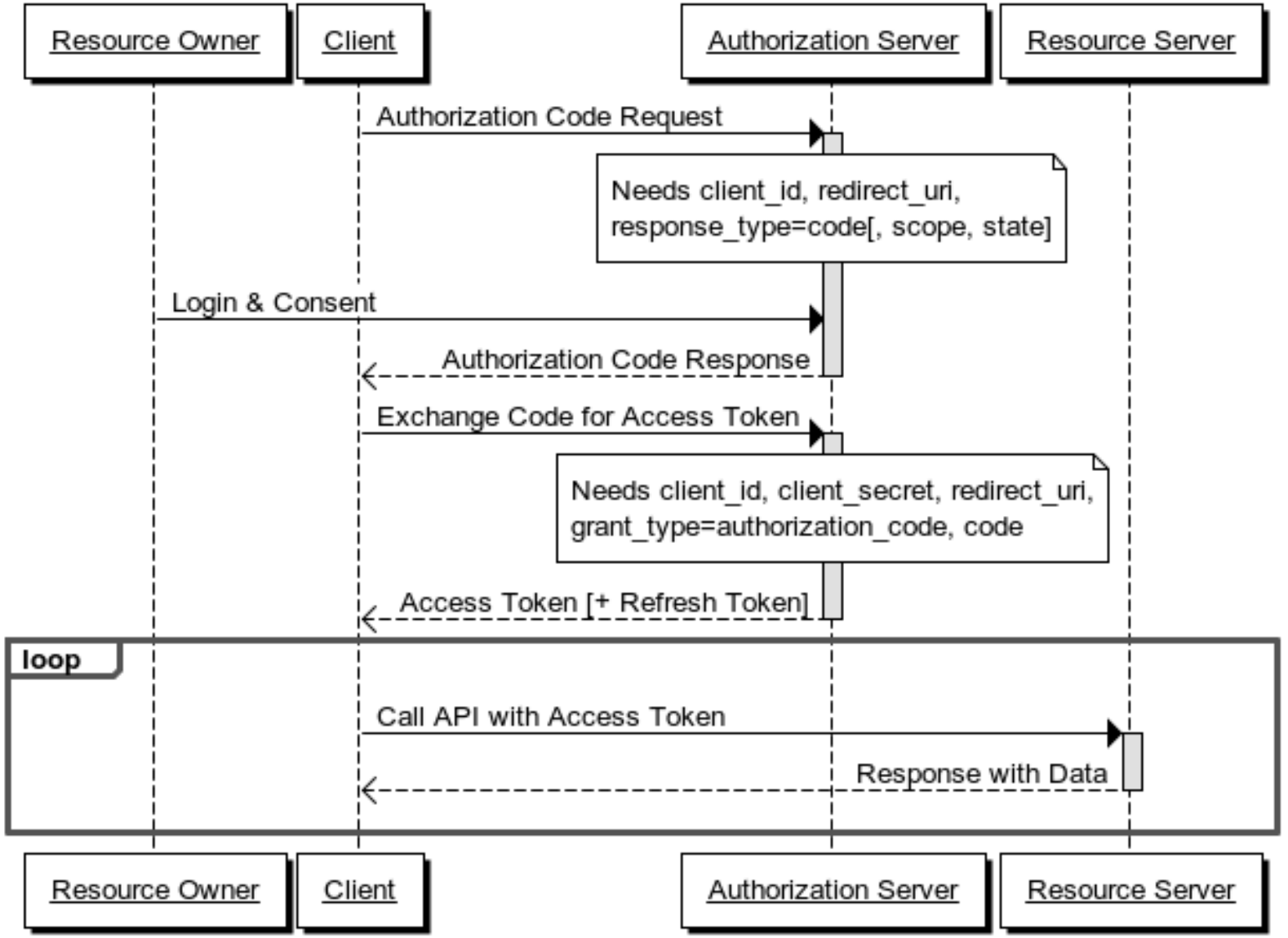
JSON Web Token (JWT)

- Checkout:
  - https://jwt.io/
- Request header:
  - Authorization: Bearer <token>
- Verification, Refresh tokens, revocation ,...

OAuth & OpenID

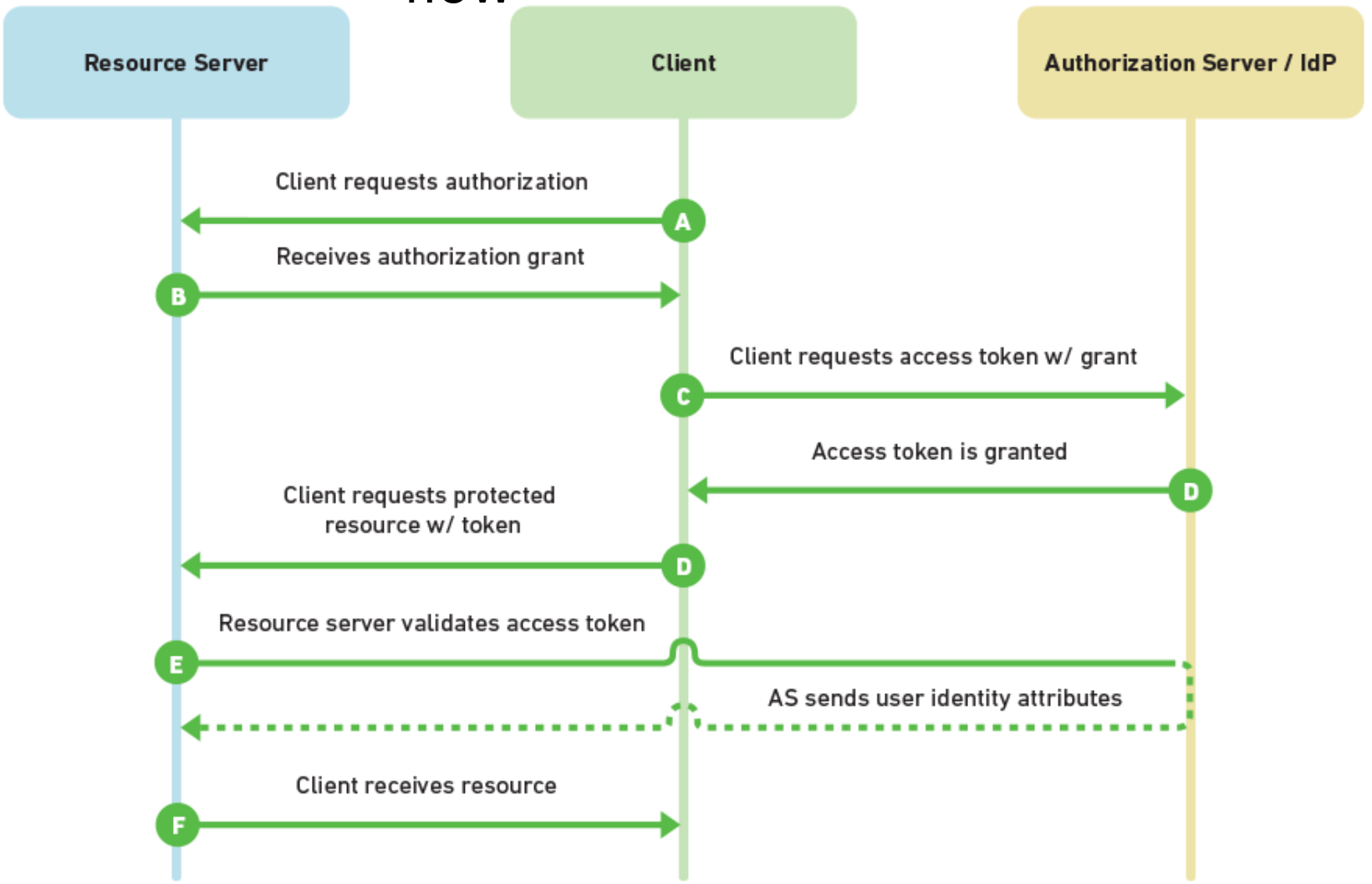
- Let’s watch OAuth 2.0 and OpenID Connect (in plain English)| Nate Barbettini
  - https://www.youtube.com/watch?v=996OiexHze0

Authorization Code Grant Flow



http://www.bubblecode.net/en/2016/01/22/understanding-oauth2/

Oauth sample flow

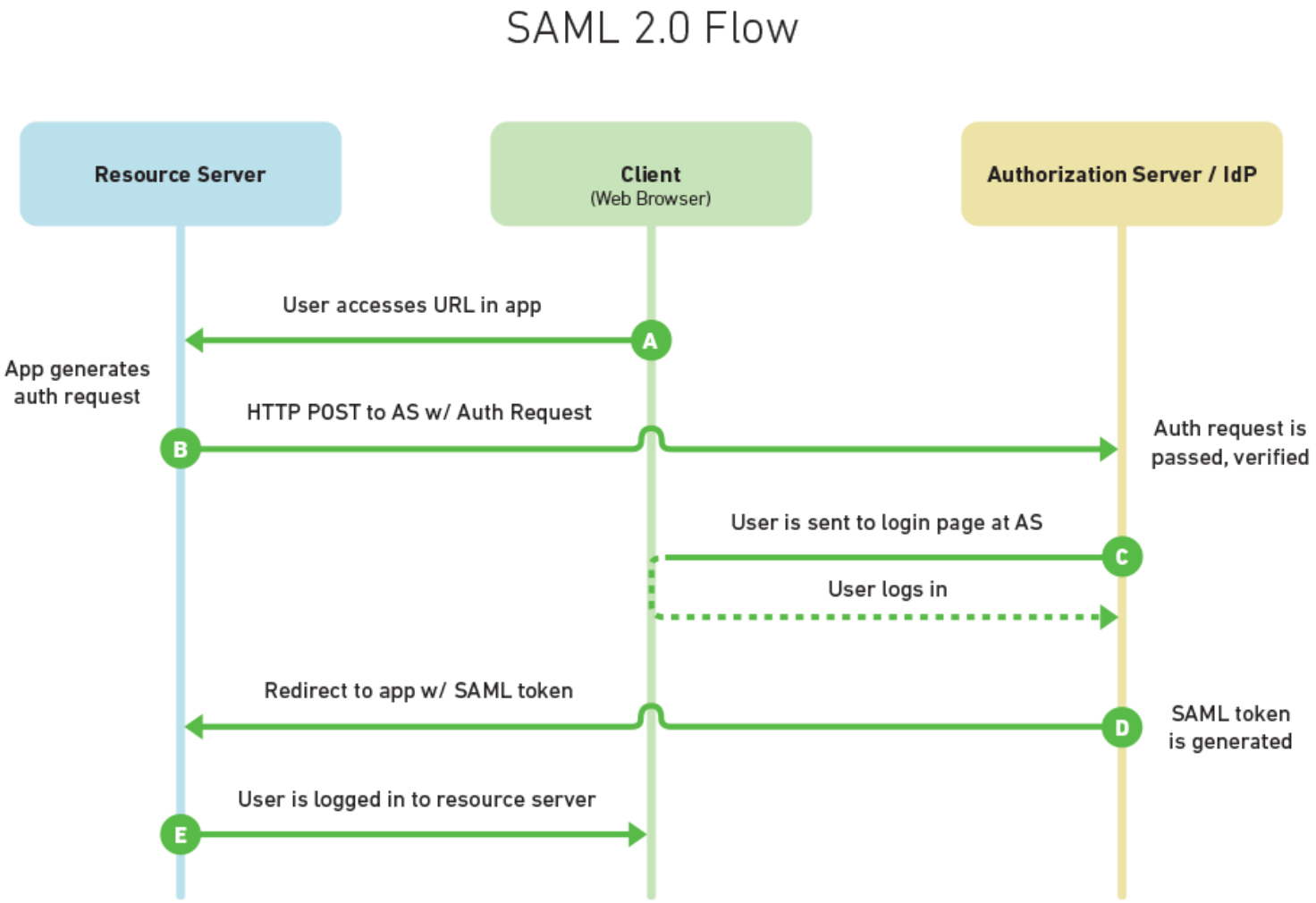


https://www.mutuallyhuman.com/blog/choosing-an-sso-strategy-saml-vs-oauth2/

SAML

- Just FYI , older spec, XML based but still common in enterprises
- Some similarities with OAuth
- If you got time checkout
  - SAML vs OAuth2
    - https://www.mutuallyhuman.com/blog/choosing-an-sso-strategy-saml-vs-oauth2/

SSO via SAML



https://www.mutuallyhuman.com/blog/choosing-an-sso-strategy-saml-vs-oauth2/

Securing Microservices

- Got time ?
  - Top 10 Security Best Practices to secure your Microservices - AppSecUSA 2017
    - https://www.youtube.com/watch?v=VtUQINsYXDM

Final Thoughts

- We can depend on other systems to provide Identity and basic user info
  - DIY Oath provider?, check (UAA) User Account and Authentication Server
- OAuth is an authorization standard
- OpenID is an authentication extension
- Spring supports these protocols
  - Checkout: Spring Boot Security OAuth 2
    - https://www.youtube.com/watch?v=wfaKvQ0qY3E