OAuth is DAC. What do you do for MAC?

Discussion paper for OSW 2018

https://docs.google.com/document/d/1ZzZ6zoOazYz1nzRYfkb9Rm1syUQIBH8ZYQsx6lGS2Yo
https://docs.google.com/presentation/d/1XvIlDfbQ9KbfGi_f5GGBTNWWr8wbt-JzVHLOMcN5WJI

About me

- Software architect
- Founder of secappdev.org
- Consultancy
- MVPs, PoCs, pilots

https://www.johanpeeters.com
@YoPeeters
yo@johanpeeters.com

OIDC rules the web

developers are disenchanted with SAML

- affiliated to SOAP and WSDL
- verbose and complex

OAuth is for authZ, not authN

authorization server vendors currently implement OIDC

- OIDC authorization servers also support OAuth - buy one, get one for free

DAC vs MAC

OAuth gives end users control over clients' access to the resources they 'own'

businesses want control over data they hold, regardless of 'ownership'

in other words, they want MAC

they are familiar with RBAC

∴ authorization server extensions to support MAC

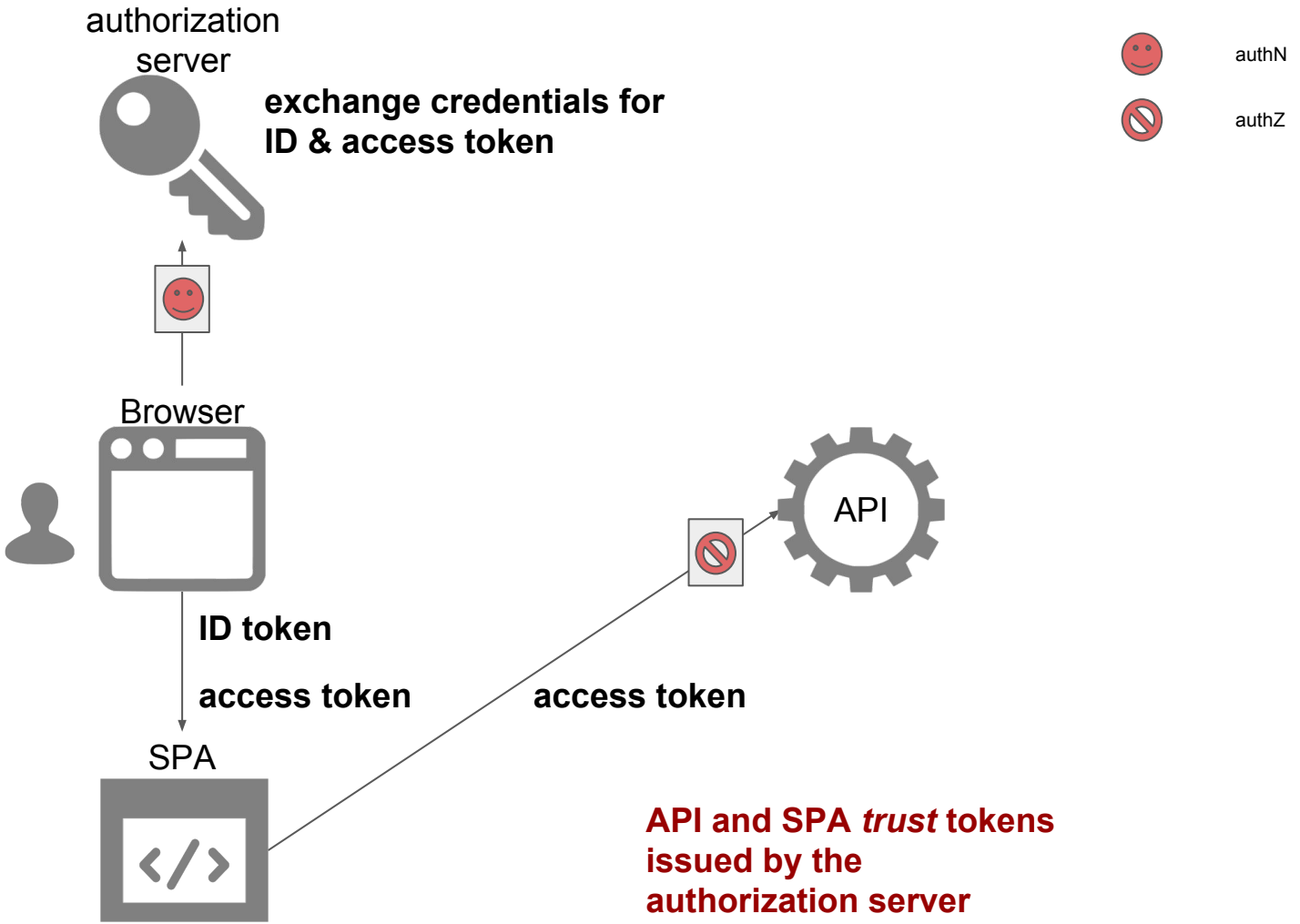
authorization server extensions

emerging consensus?

- roles
- JWT

opportunities for leveraging existing constructs

- scope
- JWT
- audience and authorized party


authorization
server
exchange credentials for
ID & access token
authN
authZ
Browser
API
ID token
access token
access token
SPA
API and SPA *trust* tokens
issued by the
authorization server

Motion I: JWT as the access token format

OIDC specifies that the ID token must be a signed JWT

an ID token may contain several kinds of claims:

- standardized
  - mandatory
  - optional
- custom

OAuth does not standardize an access token format

JWT seems to be the emerging consensus for access tokens

but what claims should they contain?

Motion II: support RBAC

gigantic installed base

emerging consensus re. `roles` claim

roles are sets of permissions granted to the **end user**

Motion III: steal some of the ID token claims

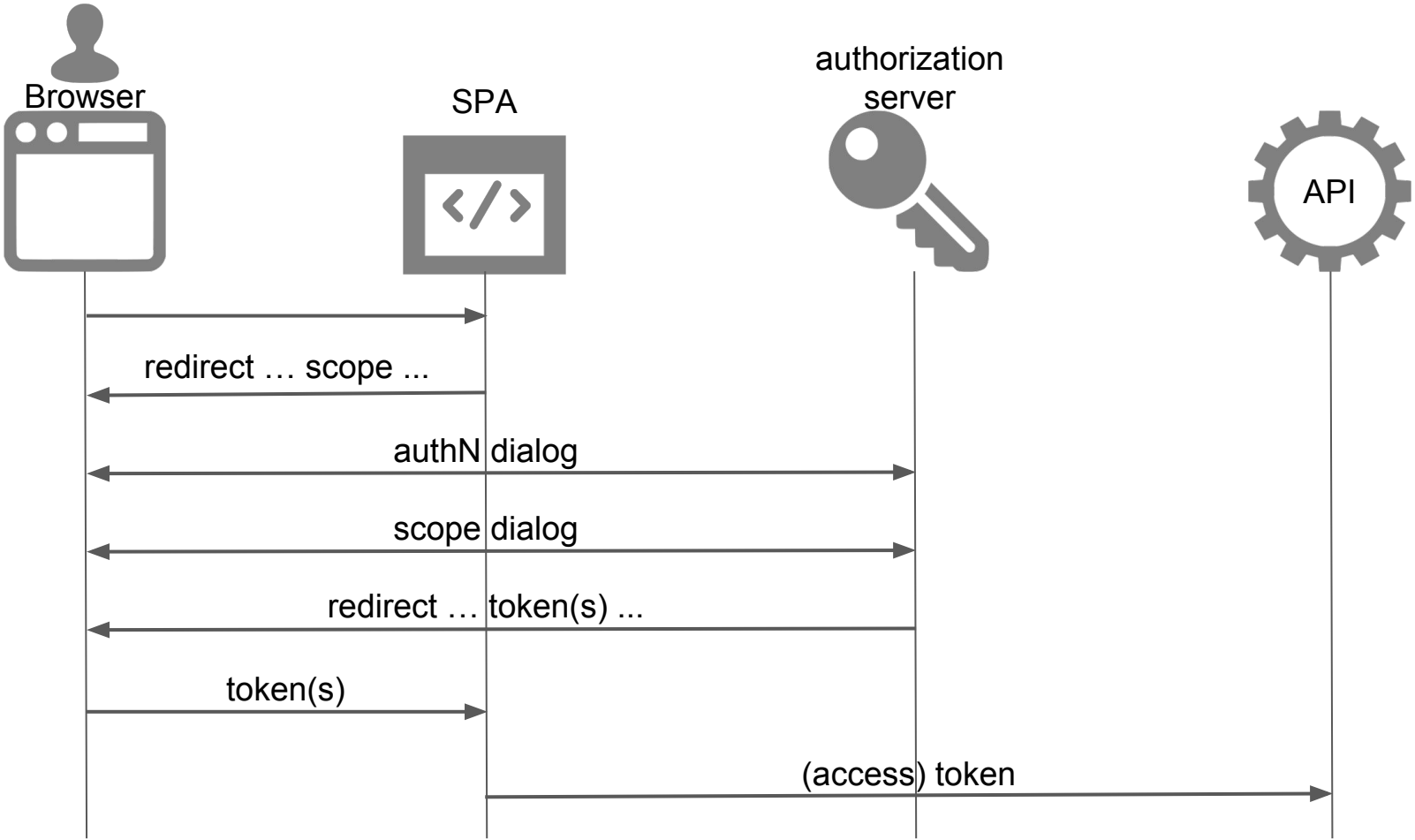
aud

> REQUIRED. Audience(s) that this ID Token is intended for. It MUST contain the OAuth 2.0 client_id of the Relying Party as an audience value. It MAY also contain identifiers for other audiences. …

azp

> OPTIONAL. Authorized party - the party to which the ID Token was issued. If present, it MUST contain the OAuth 2.0 Client ID of this party. This Claim is only needed when the ID Token has a single audience value and that audience is different than the authorized party. …

From OpenID Connect Core ©The OpenID Foundation


Browser
SPA
authorization server
API
redirect … scope ...
authN dialog
scope dialog
redirect … token(s) ...
token(s)
(access) token

Motion IV: syntax and semantics for scope token

OIDC defines scopes: `openid`, `profile`, `email`, `address` and `phone`

`<action>:<resource>` is often suggested for access token scope

- what actions? CRUD verbs?
- is resource related to URL? How?
- what impact on access token?
- what processing model in resource servers?
- what programming model in authorization servers?

References

OpenID Connect Core 1.0, https://openid.net/specs/openid-connect-core-1_0.html

JSON Web Token (JWT), https://tools.ietf.org/html/rfc7519

The OAuth 2.0 Authorization Framework, https://tools.ietf.org/html/rfc6749