AXIOMATICS

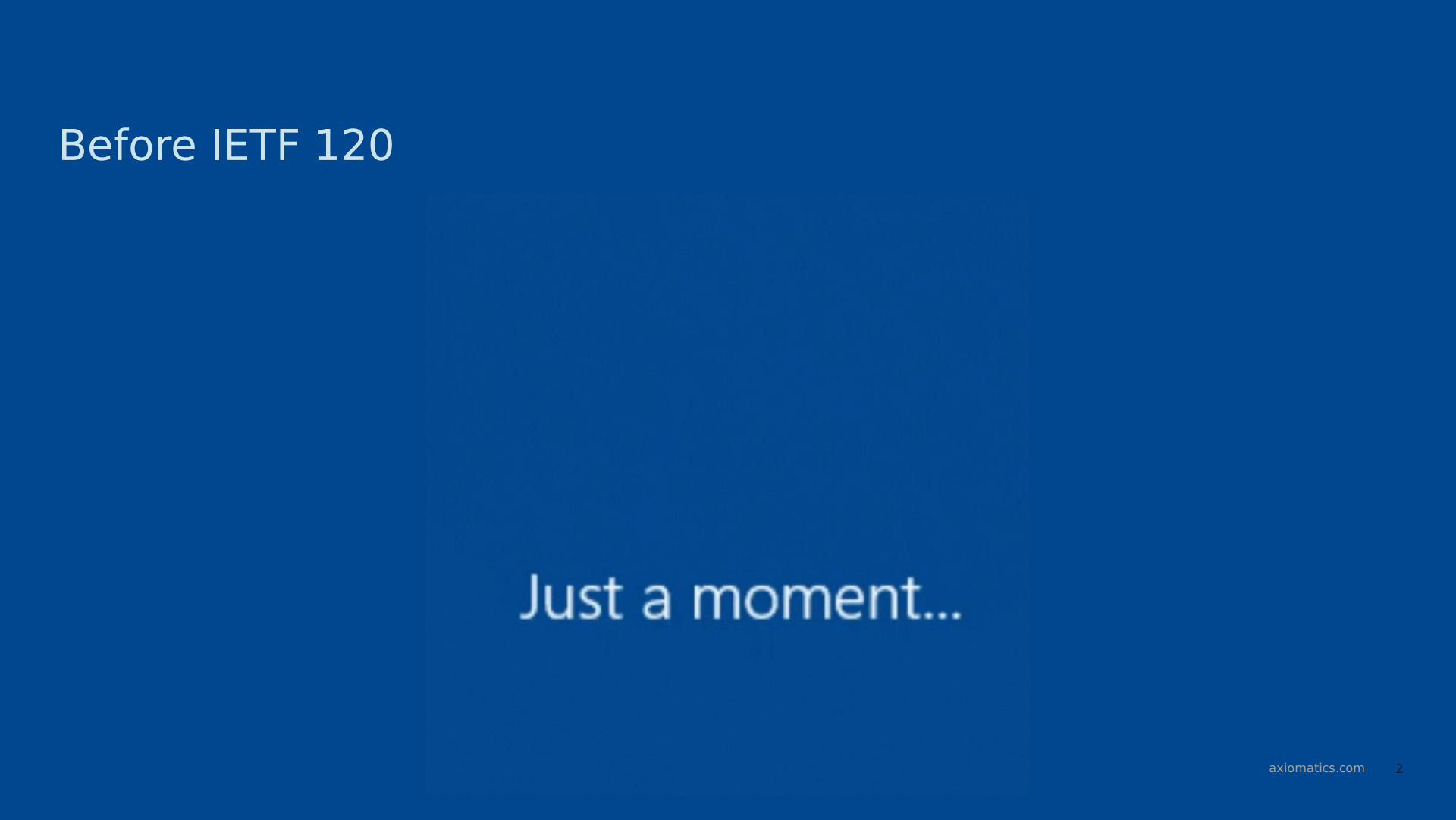
IETF 120 - OAuth WG - AuthZEN Profile of RAR

David Brossard

https://datatracker.ietf.org/doc/draft-brossard-oauth-rar-authzen/

July 21st 2024

Before IETF 120




This is not a
Cedar

Interoperability matters

What is OpenID AuthZEN

Why

- The #1 issue on OWASP's Top 10 is A01:2021-Broken Access Control

Goal

- AuthZEN is a protocol under OIDF to standardize the interaction between PEPs and PDPs
  - 12 compliant OSS and proprietary PDP implementations (and counting)
- Increase interoperability between existing standards and approaches to authorization
- Standardize interoperable communication patterns between major authZ components
- Establish and promote the use of externalized authZ as the preferred pattern

API

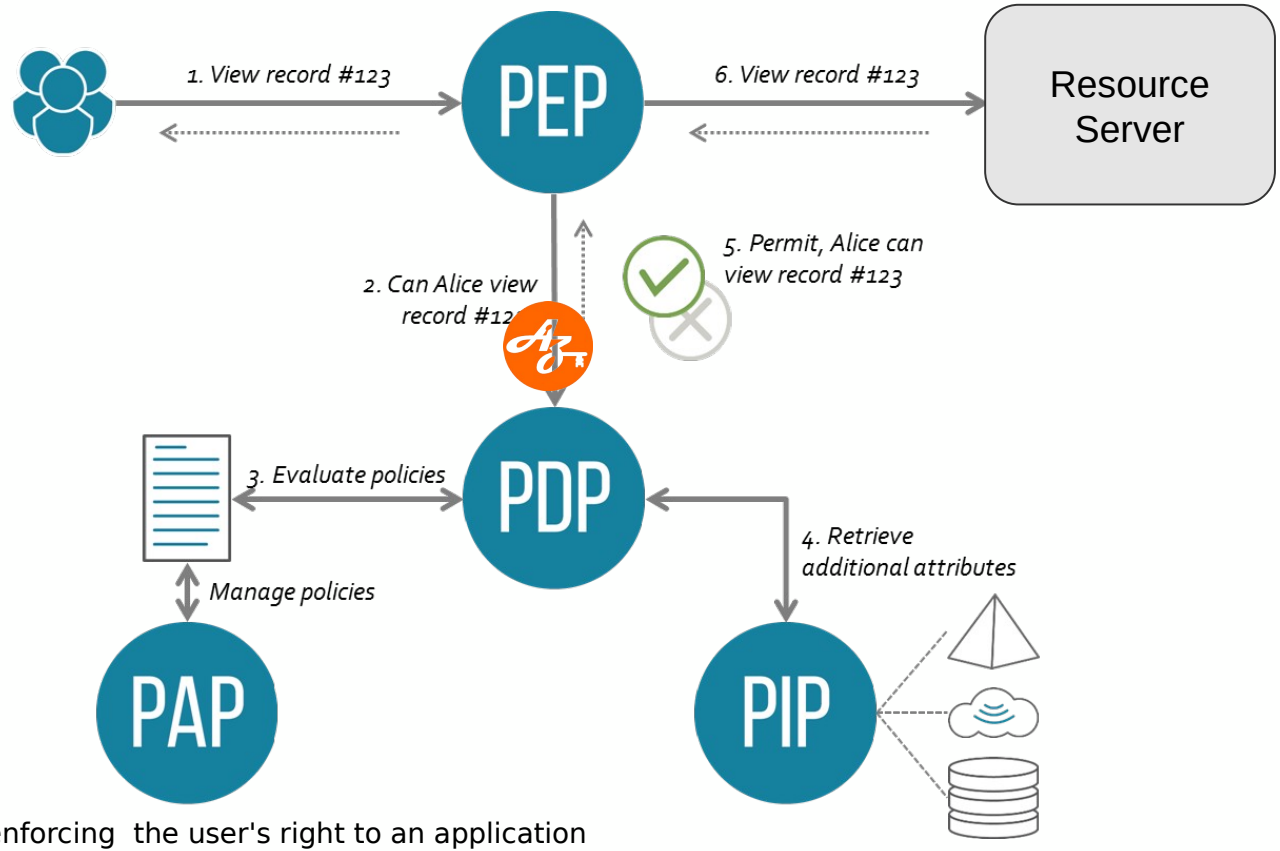
- AuthZEN defines a request/response schema & protocol:

OpenID AuthZEN Sample Request & Response

```
{
  "subject": {
    "type": "user",
    "id": "Alice"
  },
  "resource": {
    "type": "account",
    "id": "123"
  },
  "action": {
    "name": "read"
  },
  "context": {
    "time": "1985-10-26T01:22-07:00"
  }
}
```

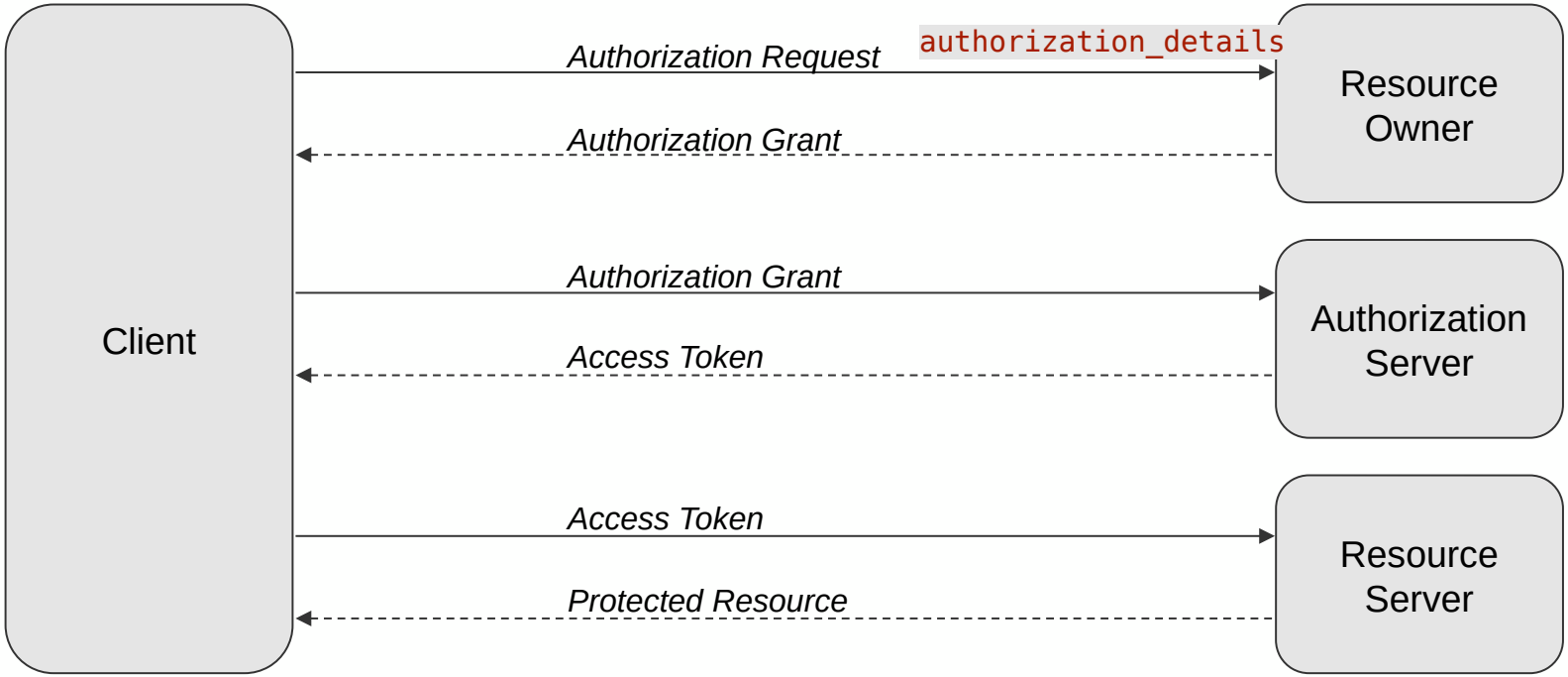
```
{
  "decision": true
}
```

The P*P Pattern: Access Control



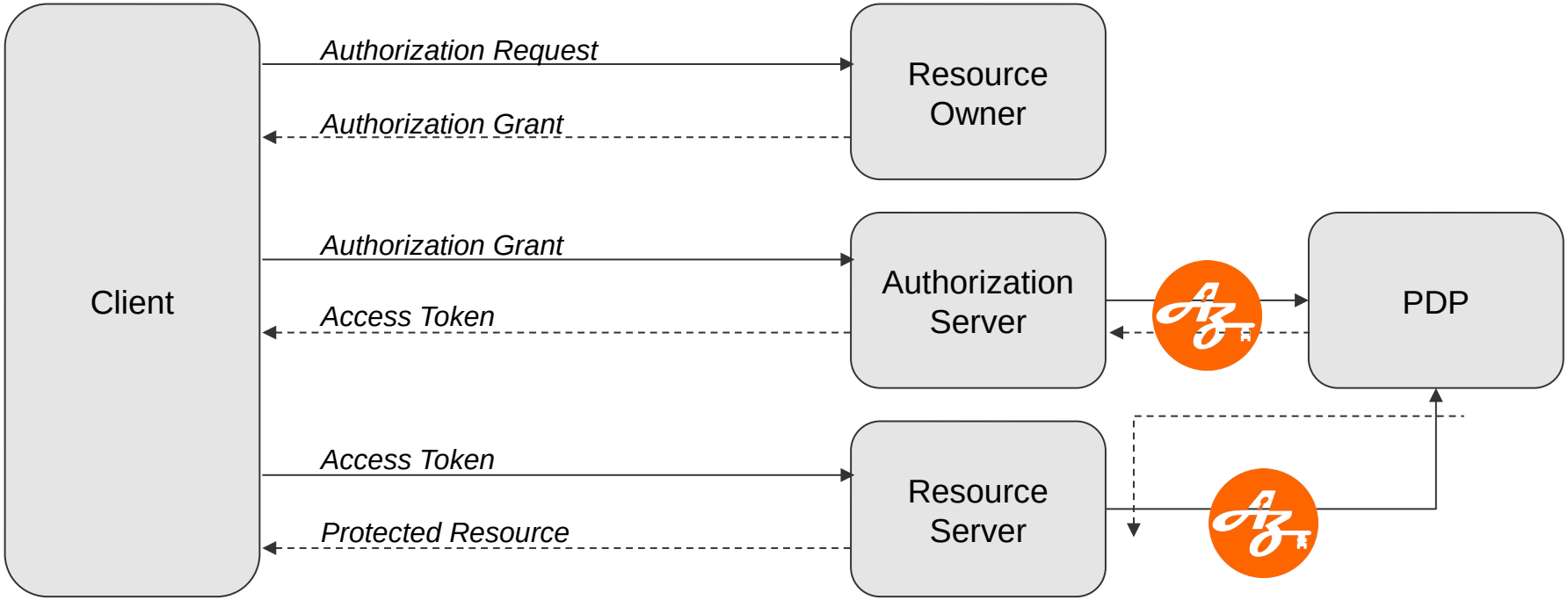
- ABAC is about controlling/enforcing the user's right to an application

The RS/AS Pattern: Access Delegation



- OAuth is about delegating the user's right to an application

Combined Architecture? (See IIW XXXVII)

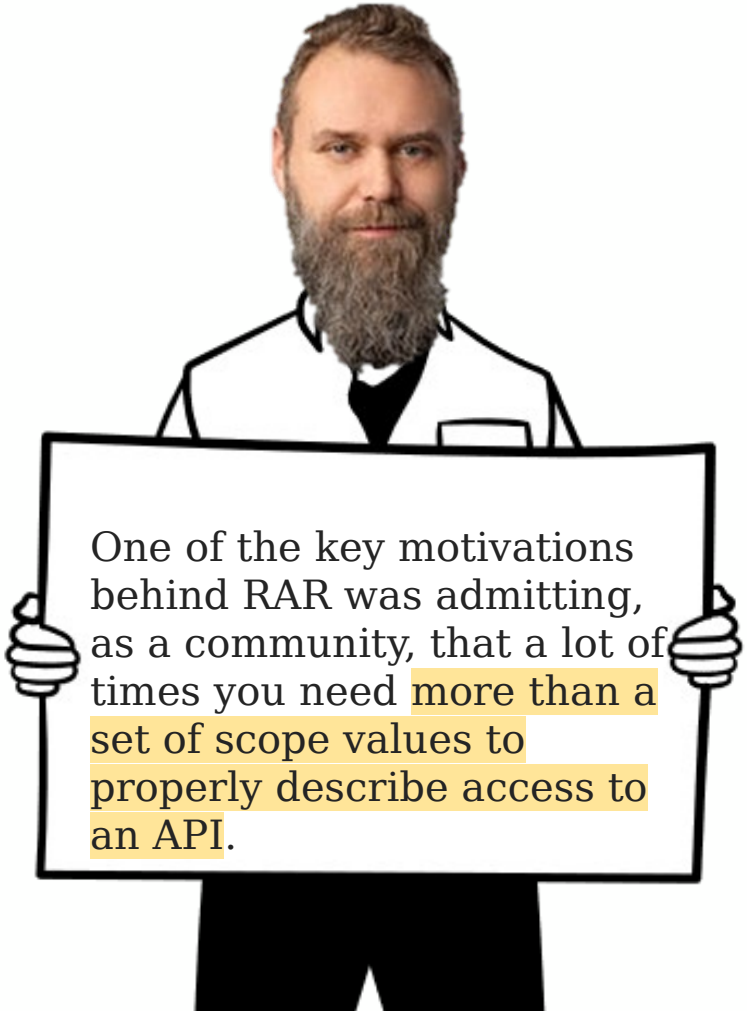


Rich Authorization Requests (rfc9396)

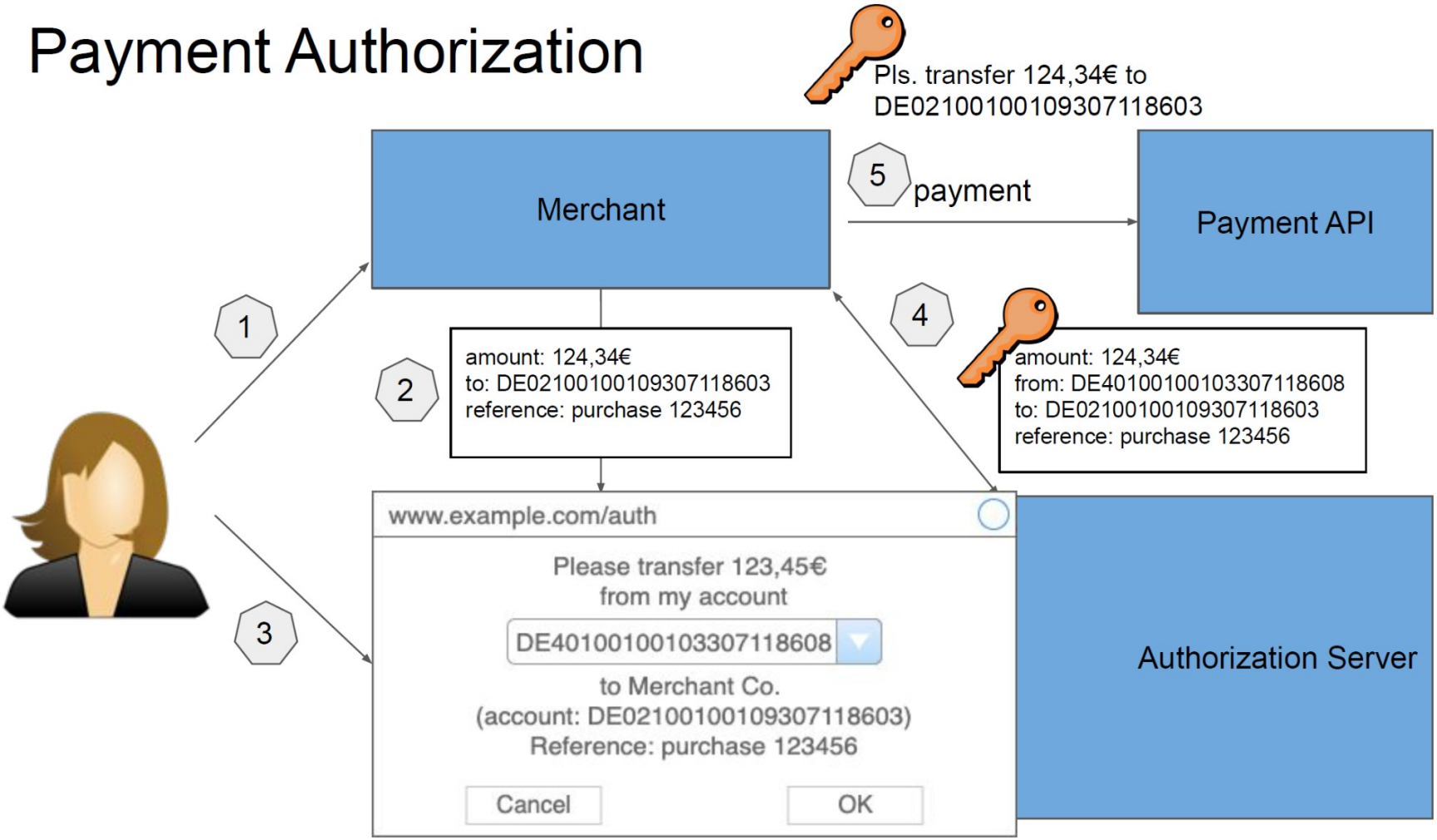
OAuth 2.0 defines the scope parameter that allows OAuth clients to specify the the limited capability of an access token.

- Sufficient to implement static scenarios and coarse-grained authorization requests
- Not sufficient to specify fine-grained authorization requirements

RFC 9396 introduces a new parameter `authorization_details` that allows clients to specify their fine-grained authorization requirements using the expressiveness of JSON [RFC8259] data structures.


One of the key motivations behind RAR was admitting, as a community, that a lot of times you need more than a set of scope values to properly describe access to an API.

Payment Authorization



Source: https://datatracker.ietf.org/meeting/106/materials/slides-106-oauth-sessb-rich-authorization-requests-httpstoolsietforghtmldraft-lodderstedt-oauth-rar-00


Bridge between
OAuth & AuthZ

AuthZEN Request/Response Profile for OAuth 2.0 Rich Authorization Requests

- https://datatracker.ietf.org/doc/draft-brossard-oauth-rar-authzen/
- The aim of this profile is to define an AuthZEN-conformant profile of the OAuth 2.0 Rich Authorization Requests [RFC9396]

Why?

- While RAR is about constraining access delegation, it still expresses it in terms of a request that is in line with the AuthZEN format
- We should leverage AuthZEN therefore as a format
- It can help the AS pass the request through to a PDP for fine-grained decision-making

Some feedback (already)

- The use of the “type” field
  - In our proposal we use it to indicate the type of request (AuthZEN) vs. ‘plain’ JSON
  - But our understanding is that the type is useful for the business purpose (see FAPI)
- The RAR spec was intended to provide a mechanism for an AS to communicate to an RP the details of a consent granted by resource owner.
  - Allow the AS to communicate back to the RP any constraints - limits etc, that the resource owner set
  - Allow the RP to understand the bounds of the context that it presents to the user through the various flows they offer
- The RAR type is used a like a scope. i.e. from a Open Banking POV, participants will be registered with the scheme and as part of the registration be enabled as an RP that can initiate payment, open

Some feedback (cont’d)

- Ralph
  - Pushing what in my opinion an entirely AS<->RS concern out to the RP will struggle to be adopted by most developer communities as RP's will justifiably view this complexity as being unnecessary and primarily an AS/RS concern.
  - If the AS/RS want to agree a standard to make policy decisioning by the RS/PEP easier then the AS can model the AT Conent or Introspection content in whatever model it wants. If there's a standard for it then great! But it's not an RP's concern how or which standard a bank uses to provide information (PIP) to the RS/PEP.

Future AuthZEN Work Relevant to RAR

AuthZEN is planning a Search API

- Alice wants to list accounts. Which accounts can she view?
- This can be extremely useful to enrich access tokens or the RAR `authorization_details` object itself

```
"authorization_details": [
{
    "type":
"account_information",
    "access": {
        "accounts": [],
        "balances": [],
        "transactions": []
     },
   "recurringIndicator":true
}]
```

```
"authorization_details":[
         {
            "type":"account_information",
            "access":{"accounts":[
                  { "iban":"DE23…9"},

{"maskedPan":"123456xxxxxx1234"}
               ],
               "balances":[{"iban":"DE23…9"}
               ],
               "Transactions":[
                 {"iban":"DE23…9"},

"maskedPan":"123456xxxxxx1234"}]},
```

Beyond the proposed profile, other questions

- Relationship to Transaction Tokens
- Relationship to other areas of OAuth that could query authorization engines
  - Dynamically generated claims (where an AS asks a PDP which claims can be inserted inside a token during the issue flow)
  - Deciding overall whether a token should be issued
  - Selective disclosure
- Relationship to Identity Assertion Authorization Grant

Further Reading

- Rich Authorization Requests https://tools.ietf.org/html/draft-lodderstedt-oauth-rar
  - IETF-106, 21.11.2019, Singapore
  - Brian Campbell, Justin Richer, Torsten Lodderstedt
- AuthZEN Request/Response Profile for OAuth 2.0 Rich Authorization Requests
  - IETF submission
- Applying RAR in OAuth 2 (and GNAP) | by Justin Richer
- IIW37_S7I_PDP & PEP vs. AS/RS Smackdown (How to map them properly?)

AXIOMATICS

Thank you