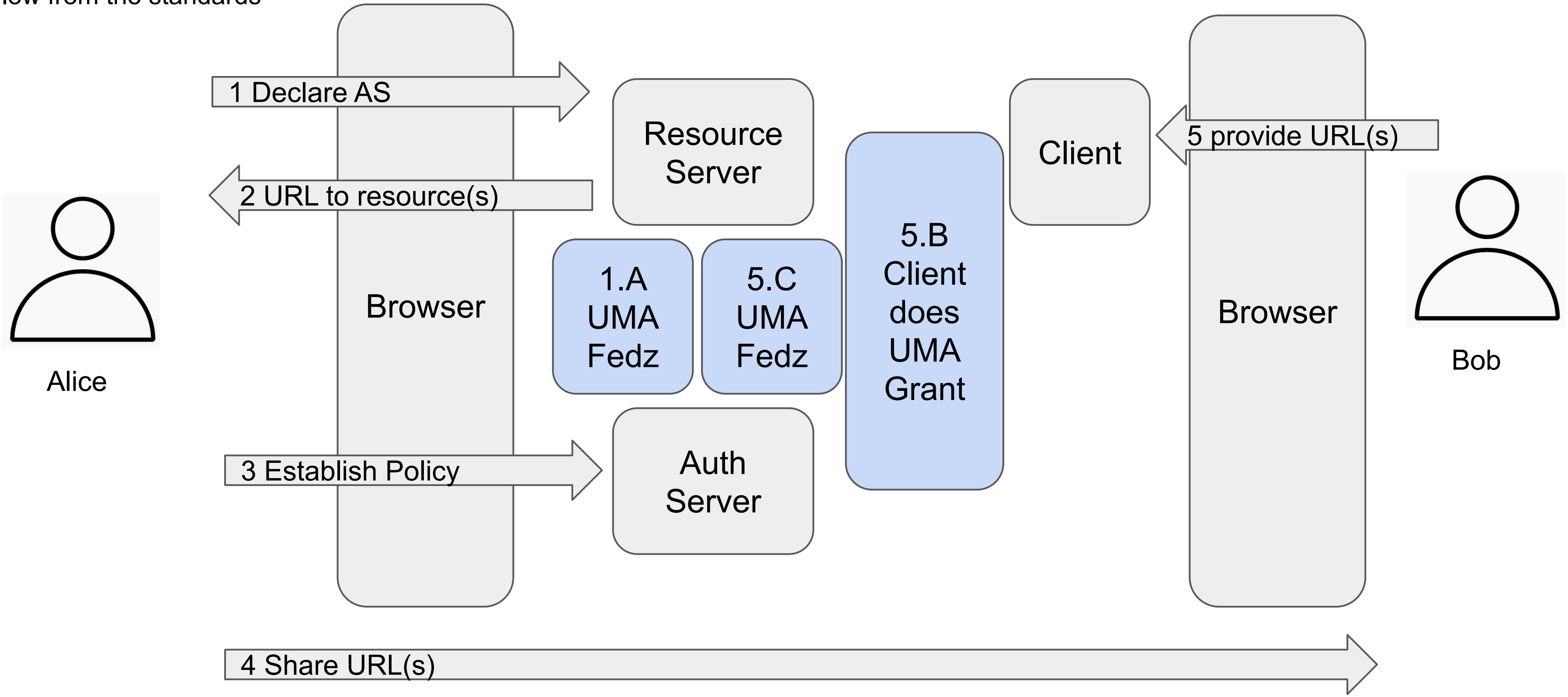
UMA 2 scope (ABC)

A Federation to establish PAT + resource registration
B www-authenticate, claims push/gather
C permissions, introspection

All the grey arrows are out of scope!

* this is not the ONLY UMA flow, it’s an implied flow from the standards

IDPs *exists*



Challenges with UMA Scope

1. *Alice must know the RS exists*
2. *The RS may not be able to trust ANY AS*
3. *The RS MUST provide UX for the user to receive URLs*
4. *The AS MUST provide UX to establish policy*
5. *Alice must collect and share resource URLs with Bob*
6. *The Client must understand the type of the resource at the URL*
7. *The RS must determine the acceptable scope for the client from a URL*
8. *The AS may not be able to trust ANY Client*

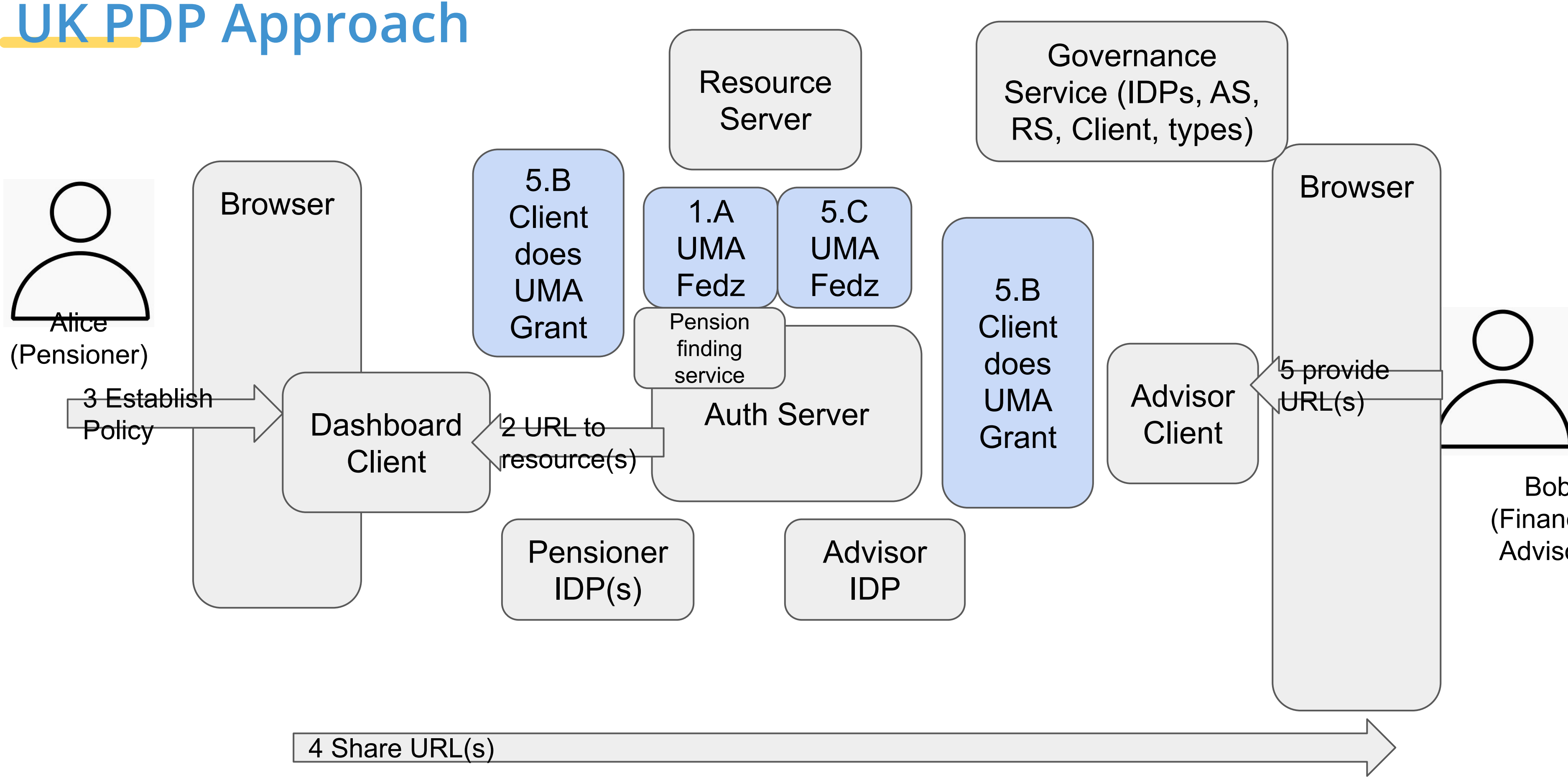
1. As Alice, I need a way to discover available RSs, in order to learn about resources I own
2. As an RSO, I need to trust a limited set of compliant ASs, in order to meet my obligations to protect resources
   a. As Alice, I need a way to work with many ASs, in order to use ones required by my RSs
3. As an RSO, I want to allow Alice to bring a resource management UX, in order to not provide this myself
4. As an ASO, I want to allow Alice to bring a resource management UX, in order to not provide this myself
5. As Alice, I want a way to grant Bob access to my resources without knowing the URLs, in order to a) not deal with URLs b) share more complex resources (ex not a PDF, a health record)
6.

Challenges with UMA Scope 2

1. *Alice must know the RS exists*
2. *The RS may not be able to trust ANY AS*
3. *The RS MUST provide UX for the user to receive URLs*
4. *The AS MUST provide UX to establish policy*
5. *Alice must collect and share resource URLs with Bob*
6. *The Client must understand the type of the resource at the URL*
7. *The RS must determine the acceptable scope for the client from a URL*
8. *The AS may not be able to trust ANY Client*

1.
2.
3.
4.
5. As Bob, I want to be able to discover resources available/shared with me, in order to not need URLs sent by Alice
6. As a Client, I want to be able to declare types I understand, in order to successfully use complex APIs
7. As an RS, I want to defer permission ticket creation, in order to a) not have to understand the Client b) not make authZ decisions (tell me don’t make me think)
8. As an ASO, I want to pre-register Clients, in order to assess their appropriateness, capability and complete non-technical activities
    a. As a Client, I want to pre-register with ASs, in order to a) test my UX and technical integrations b) declare my capabilities

UK PDP Approach



PDP Challenges Addressed

1. *Alice must know the RS exists*
2. *The RS may not be able to trust ANY AS*
3. *The RS MUST provide UX for the user to receive URLs*
4. *The AS MUST provide UX to establish policy*
5. *Alice must collect and share resource URLs with Bob*
6. *The Client must understand the type of the resource at the URL*
7. *The RS must determine the acceptable scope for the client from a URL*
8. *The AS may not be able to trust ANY Client*

1. AS provides a finding service that searches RSs registered in a Governance Service
2. RSs and ASs are registered with a Governance Service
3. The RS registers URLs at the AS, the Dashboard is able to see the registered URLs from the AS
4. The Dashboard client provides this UX
   a. There is some IDP federation and consent UX at the AS
5. Still true?
6. There are limited types in the ecosystem, specified at the GR
7. Limited scopes and types, are pre-defined
8. Clients are registered at the GR