
INTERNET2
2022
TECHNOLOGY
exchange
The Rise of Middlethings
Albert Wu
INTERNET2

Topics

- Introduction
- What is middlething
- Considerations for Federation
- Questions and Discussion
- Next Steps

Goals for today

Framing a Discussion to Foster SP Middlething Deployments
https://docs.google.com/document/d/1RwWn2oXJqa3YwFF_vKuTsqoJkLQ7BJ9hYFOUStbJ1IY/edit?usp=sharing

We are at the start of this journey. We are really here to ask questions. As you listen to this conversation today, we'd like to hear from you:

- Are these the correct considerations?
- Are these considerations important to address?
- Which considerations are most important to address?
- How do we address (each) consideration – in detail?
- *What are we missing?*

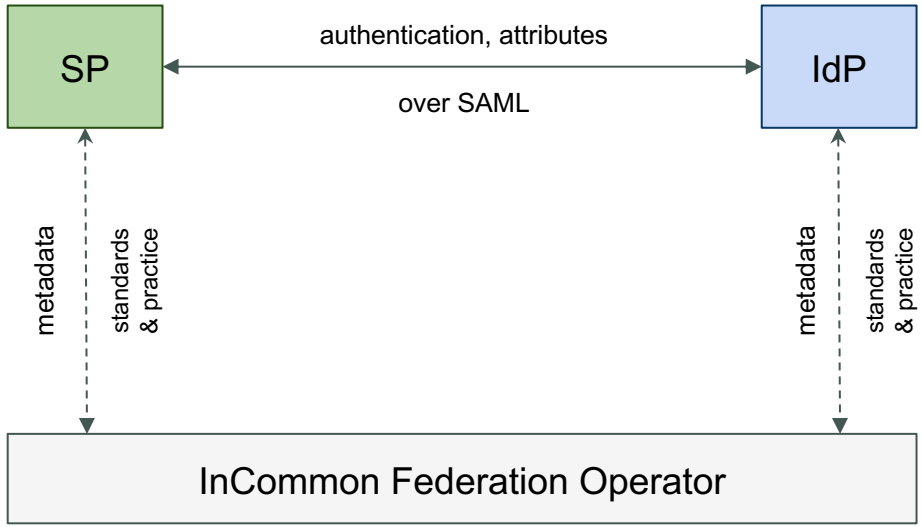
Recap: the Federation Trust model

The InCommon Federation creates multilateral trust among all federation Participants to exchange identity information in a secure manner.

Adherence to interoperability profiles scale that trust to thousands of participating organizations with millions of users.

Service Providers trust Identity Providers to securely authenticate users and provide and accurate user information.

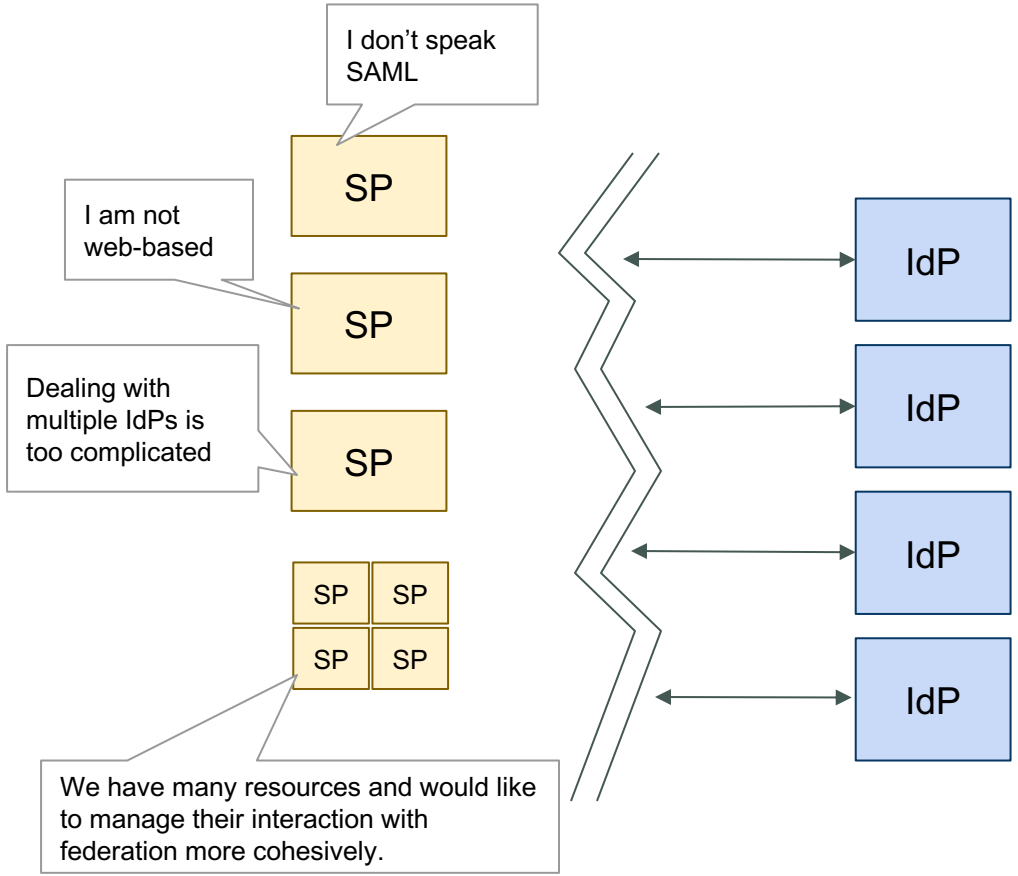
Identity Providers trust Service Providers to respect user privacy and to not misuse the information they receive.



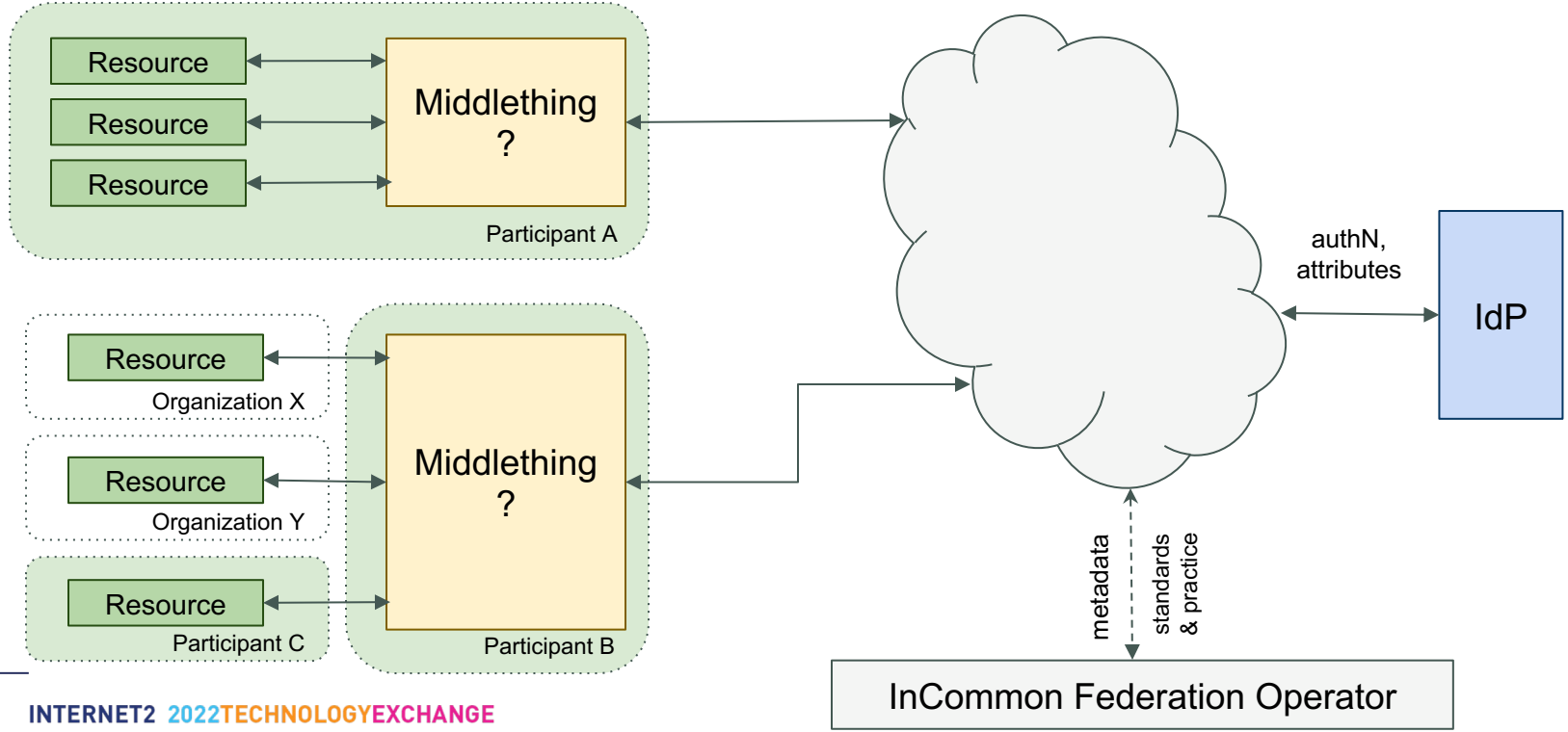
The Federation Operator provides services to broker and facilitate this multilateral trust

Our world is more complex

Real world challenges such as protocol translation, identity linking, and complex access management point to a need for something in the middle to help mediate interactions between resources and federation.



Middlethings come to the rescue



What is a “Middlething”?

“Middlething” is a deliberately ambiguous term, referring to anything that exists along the path between two communicating things.

In this conversation, we are specifically using “middlething” to refer to a component that actively translates, transforms, filters, or enhances the information exchanged between identity providers and the resource a user actually wants to access[1]. In particular, we are focusing on the “middlething” that exists primarily for the benefit of the resource.

For this conversation, we are referring to these:

- ✓ SP-IdP Proxies (AARC Blueprint Architecture)
- ✓ Access Gateways
- ✓ Science / Data Hubs
- ✓ Journal publishing platforms

Not these:

- ✗ Network Routers; NATs
- ✗ IP Proxies; application appliances
- ✗ Digital Wallets; micro-credentials

1. In the report, we use the term “mediated service provider” to refer to such resource

Characteristics and Functions of a Middlething

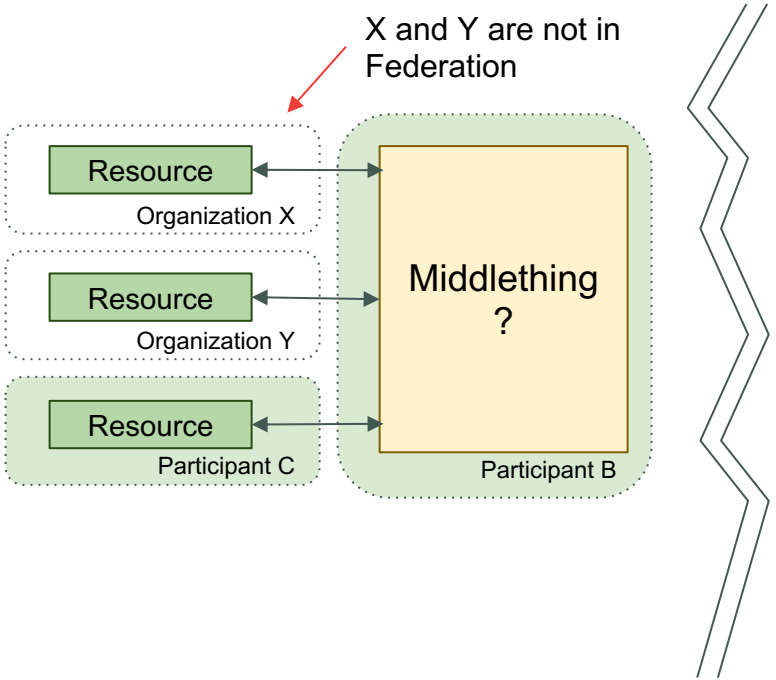
- Protocol normalization
- Protocol translation
- Enhancement of identity information.
- Enforcement of access control and other policies.
- Integration / aggregation of multiple SPs.

- May or may not be operated by the same organization(s) operating the resources behind it.
- May register 1 entity in federation; may register multiple (e.g., 1 per resource)
- May or may not shield resource operator from federation community participation
- May pass user information it receives from IdP on to resource operator behind it

Middlethings raise added considerations - trust

Federation Trust

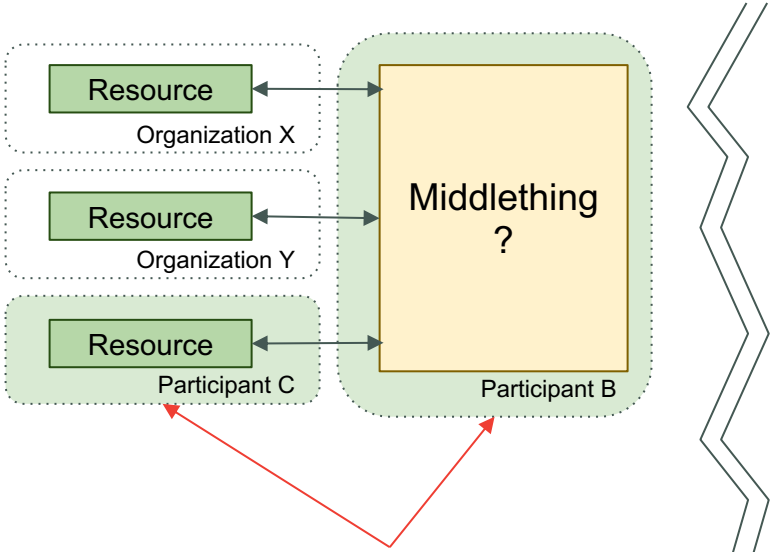
Trust is formed among participating organizations as opposed to software components. When a middlething is operated by a different organization than the one operating the resources behind it, does the current Federation trust model have the appropriate vocabulary and mechanism to describe the parties' roles and responsibilities?



Middlethings raise added considerations - operation

Participation and Operation

Does the Federation have the appropriate tooling, practices (participation model), support structure, and language (architectural pattern, standards, etc) to properly support middlethings in Federation? Transparency



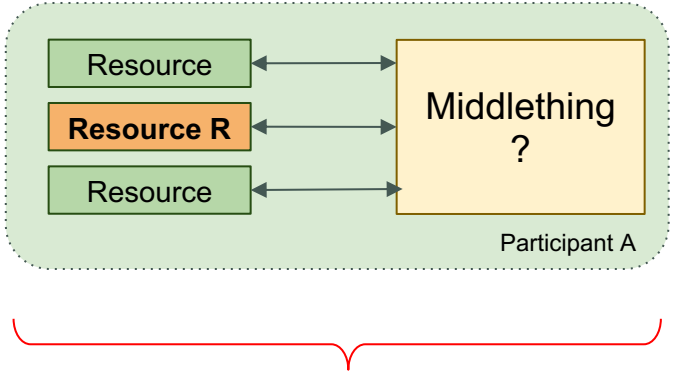
(How) Do we consistently recognize, register, and support this relationship?

Middlethings raise added considerations - UX

User Experience

“Federated Identity is confusing for users …
We’ve got to do our best to help.” - JB

Are users aided or confused by the proliferation of middlethings? Does the Federation need to do anything to help improve user experience?



I want to know if I can access Resource R via Federation, how and where do I find that information?

Middlethings raise added considerations - implementation

Implementation ~~Guidance~~ Consistency

Is there a generalizable “right” architecture for a middlething? Does the federation operator have a role in advocating standardized implementation and deployment guidance for middlethings within the federation?

As we investigate this topic, we have encountered plenty of questions. These are some examples…

Questions around functions

- Protocol translation (SAML->OIDC or PKI)
- Easier integration into federation for RP
- Identity linking
- Incident handling
- Locally minted attributes and groups
- Domain-specific resource aggregation
- Controlled access to research computing, large data sets, research instruments, or others
- Democratization of science

These are the key/typical functions middlethings commonly perform. Do they accurately capture what a “middlething” is and does?

How can we define/describe “middlething” so that we have shared clarity in discussions and solution development?

Questions around user experience

- We created federations to enable trusted and streamlined user access to scholarly collaborations. Are we focusing enough attention on user experience matters?
- What are the middlething and federation operators' roles and responsibilities in helping users locate and discover which resources they can access via Federation?
- How important/useful is it for middlethings to have similar/consistent user access experience (e.g., using common vocabularies, similar navigation patterns, etc) so that users have familiar, therefore easier experience when accessing federated resources?
- What are the roles and responsibilities around federated user support when middlethings are involved?

Questions around Trust and Transparency

- Do we have clear, shared understanding of who are involved in a federated transaction, who does what, and who to trust?
- Does the user understand the role a middlething plays in security and privacy?
- Does the user understand how to seek recourse in case of a problem?
- Does a resource (mediated service provider in the report) know who to contact in case of an incident?
- Does the IdP know who to contact in case of an incident?
- Does the federated operator know who to contact?
- Is the assignment of entity tags by a federated operator auditable?

Questions around business, policy and legal

- When a user accesses a resource via a middlething in Federation, and that resource isn't operated by the same organization as the middlething operator, does the resource operator have a obligation to join Federation (therefore adhering to federation policies)?
- Between the middlething and the resource, who is responsive to which regulatory mandates, from GDPR and CCPA to FISMA and NIST?
- Is it important to differentiate between "resource" and "middlething" at an organizational/logical level, i.e., "SP" might be too vague?
  - the party with the stuff a user wants to access
  - the party operating tools/services connecting the resource federation and performs key transformations/IAM functions on the resources' behalf

Questions around operations

- Middlethings are already common in federations. They are valuable and needed. Yet they are not recognized in today's federation model. If federation operators were to update practices and tooling, what kind of changes would significantly improve UX, trust, and ease of participation and operation for all parties involved?