Cybersecurity Management
GCS 2.1 - Identity Federation

2022-2023
Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu

Outline

- Preliminary Concepts
- Identity Federation (IdF) definition and models
- Academic IdF initiatives
- Protocols and workflows
  - SAML2
  - OpenID
  - Oauth
- Security-related concerns

Preliminary concepts

Physical Identity vs eID

- Real Identity is hold by physical or legal persons
  - Name
  - Gender,
  - Work position,
  - place of Residence,
  - Organisation, OU,
  - Phone, ISDN numbers,
  - Skills, etc.
  - Legal name
  - Official address
  - CIF / Tax Number
  - Code of Activity
  - Website
  - Brand Trademark
- **eID is the virtual representation of a real identity**
  - Ownership of information
  - Access rights to data and applications
  - Link to real identity

Profiling

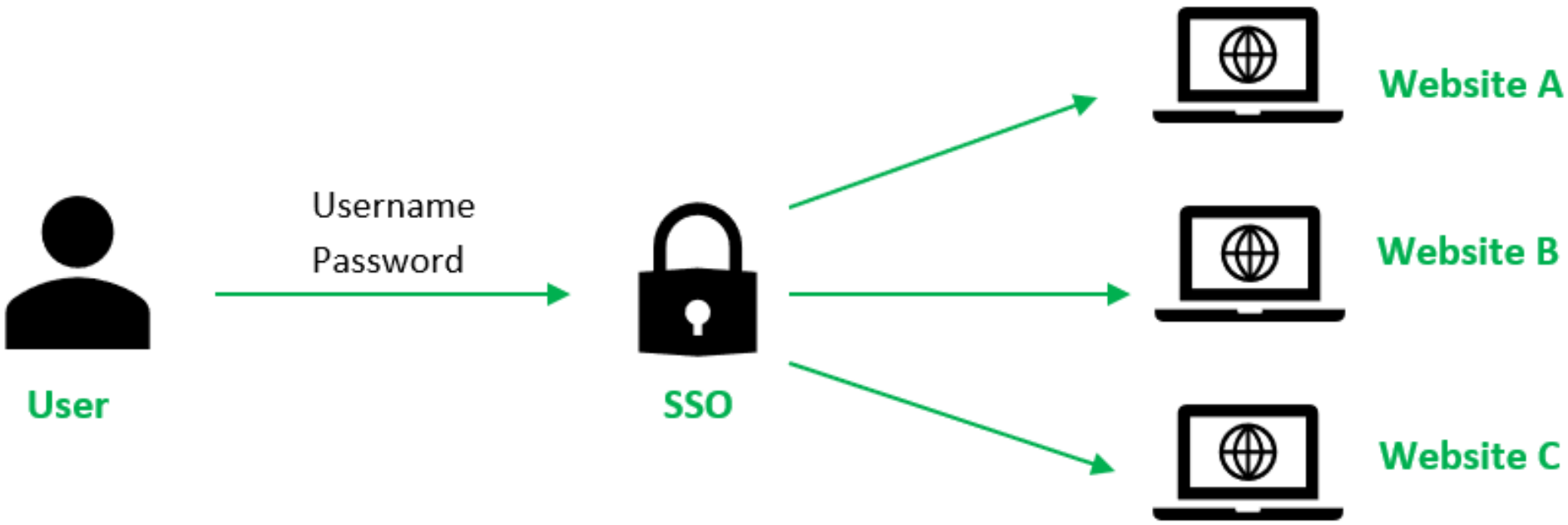
Physical persons may have several eIDs, depending on the relationships and attributes that the person wants to associate to that eID:

- "member of this community",
- "Alice Smith", or
- "licensed under contract A“

Attribute set standards:

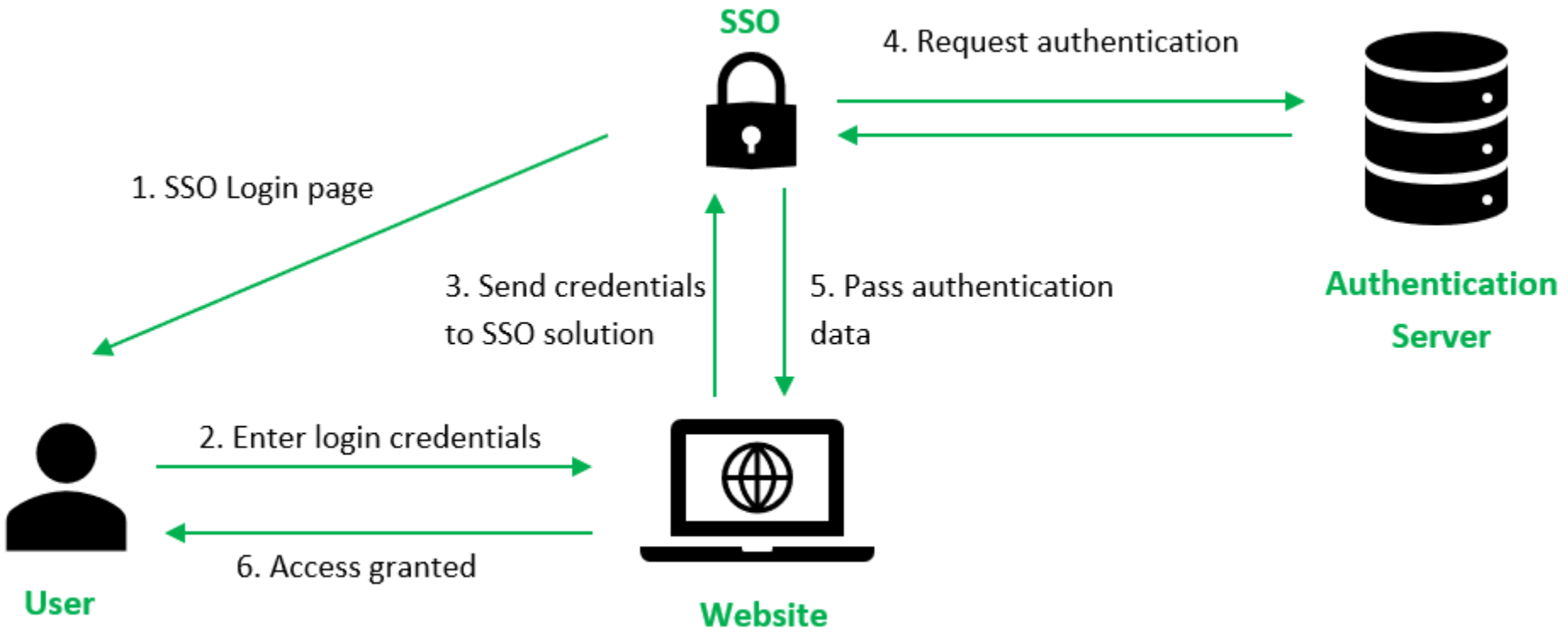
- DAP X520
- RFC2798 inetOrgPerson LDAP Object Class
- RFC3671 Collective Attributes in LDAP

Single Sign-On



Source: https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso

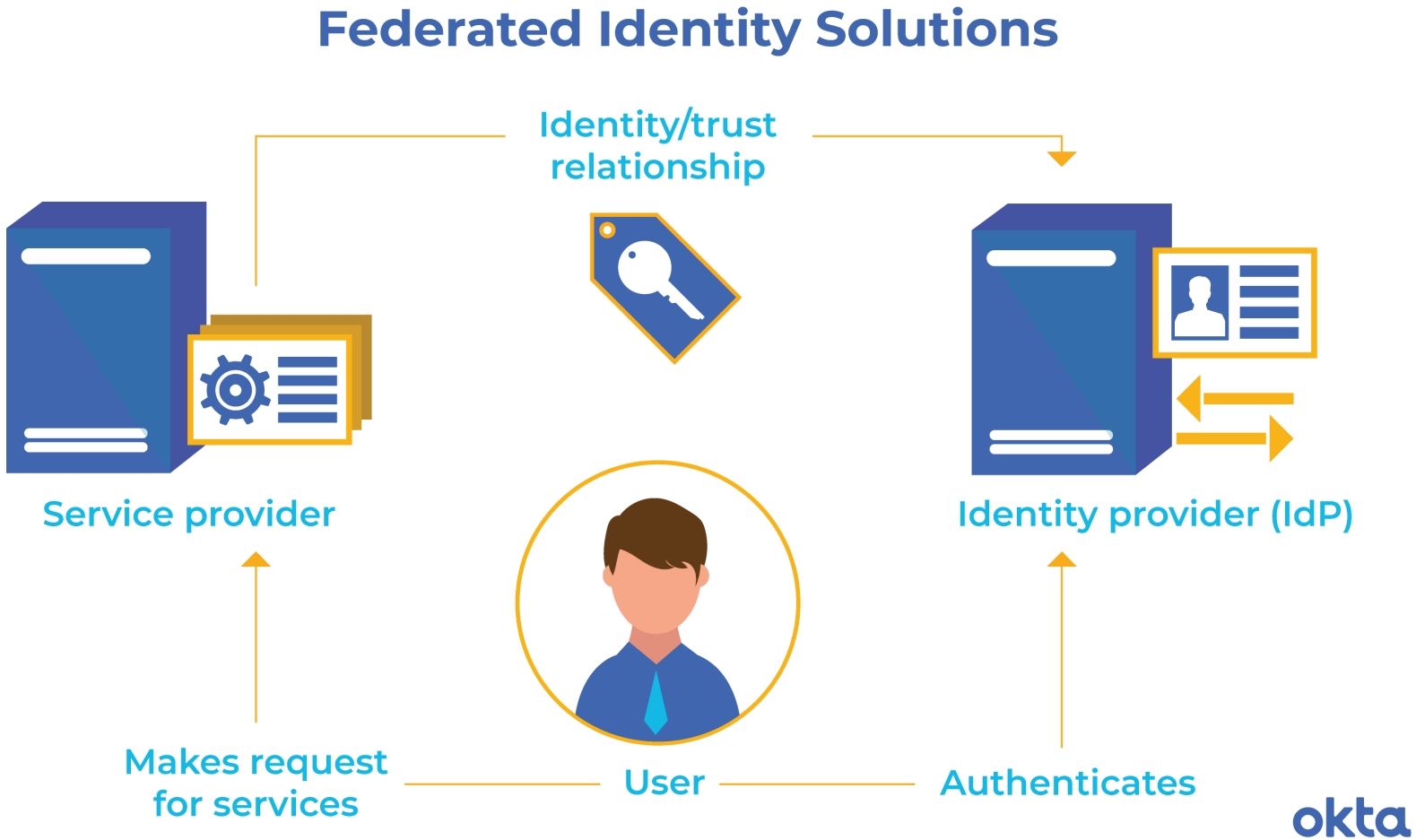
Single Sign-On



Source: https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso

Identity Federation (IdF)

Basic Concept

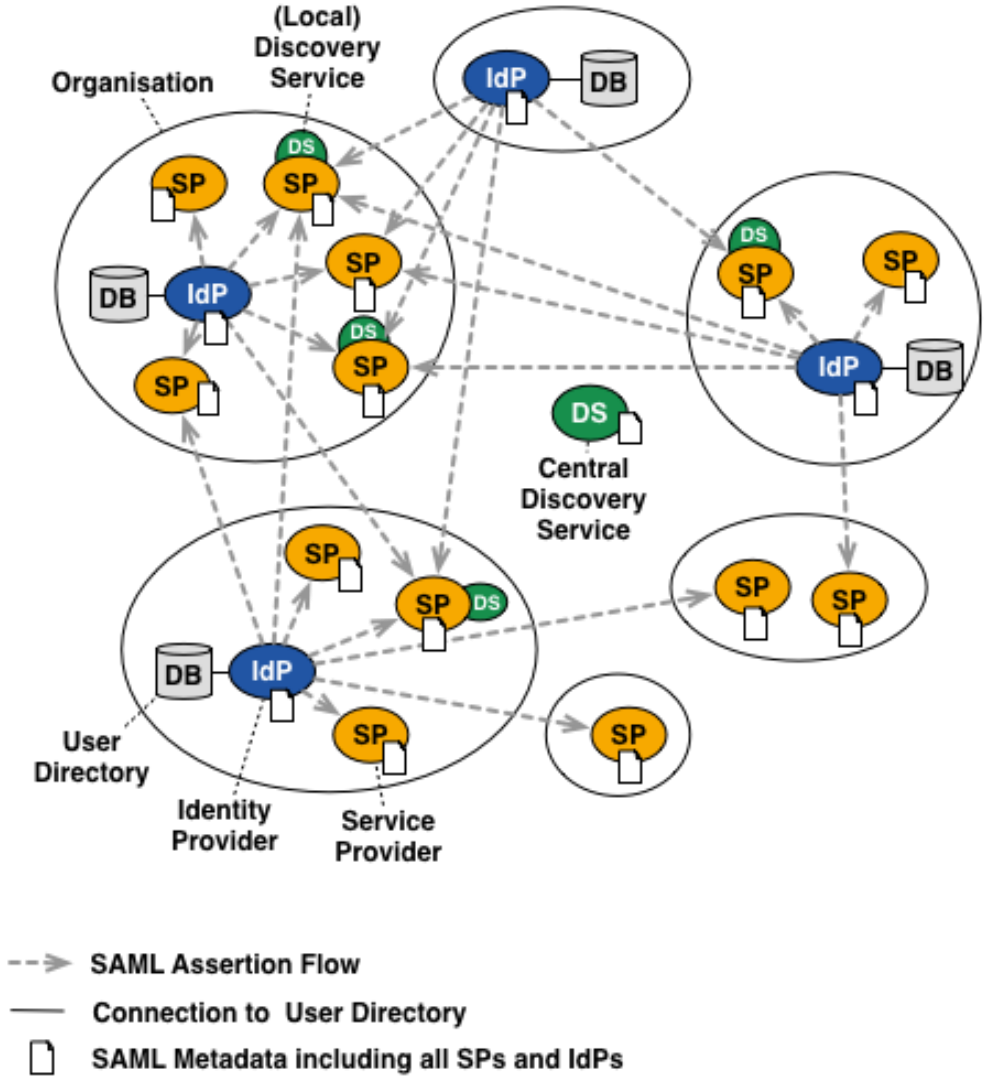


IdF in 5 minutes

https://www.youtube.com/watch?v=BFkFRnaylYY

Full Mesh

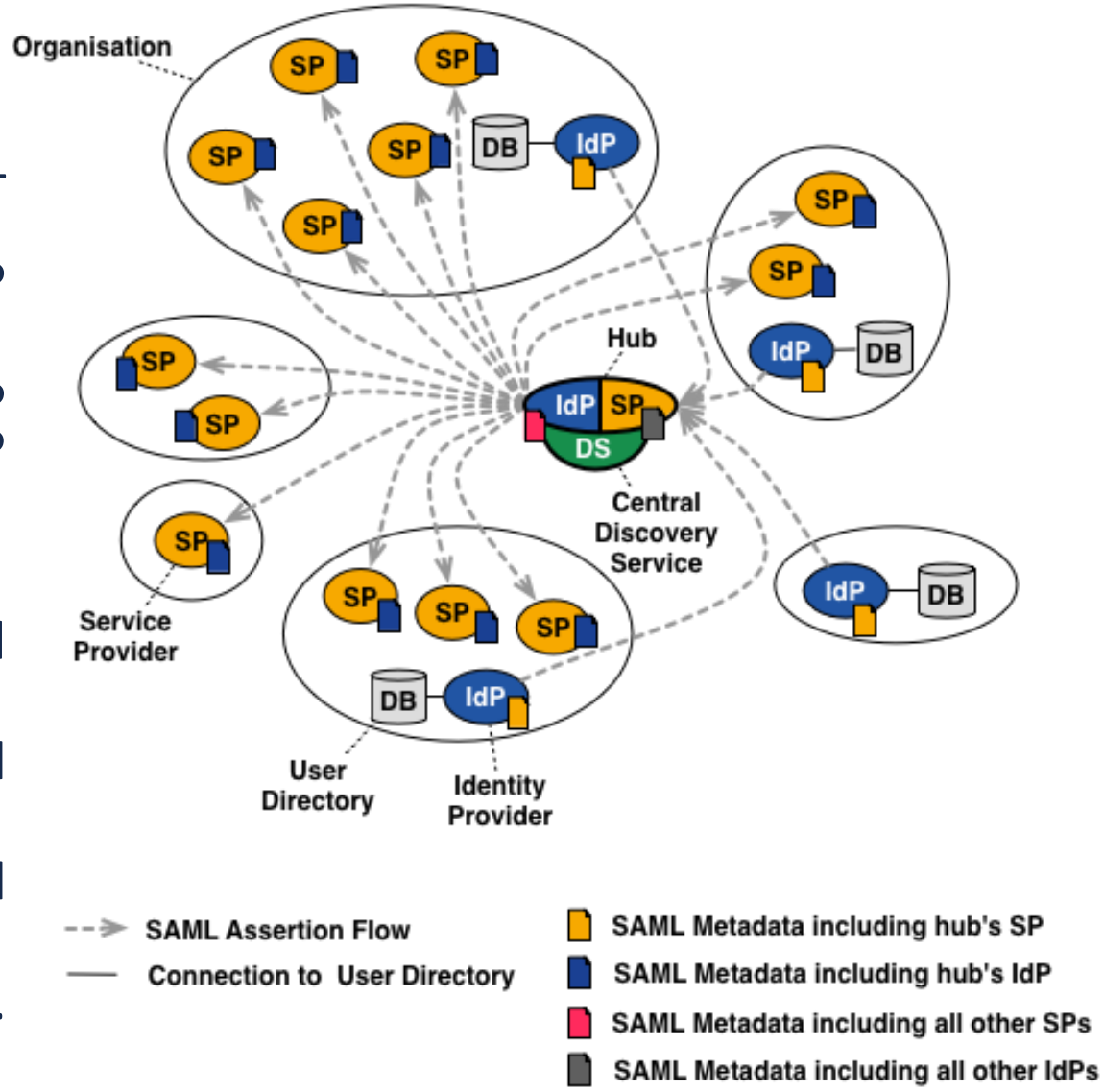
- Most common and straight forward to implement federations
- Everything is distributed and there is no need for a central component (failover management distributed as well)
- Every organisation operates their own IdP
- Centrally distributed SAML metadata file including all entities
- Requires efficient management of the metadata file
- E.g. , some federations use a web based service to register all entities, others rely on a set of scripts to compose the SAML2 metadata for the federation.
- Most federations also operate a central IdP Discovery Service/WAYF (not strictly needed).



Source: https://wiki.geant.org/

Hub-And-Spoke with Distributed Login

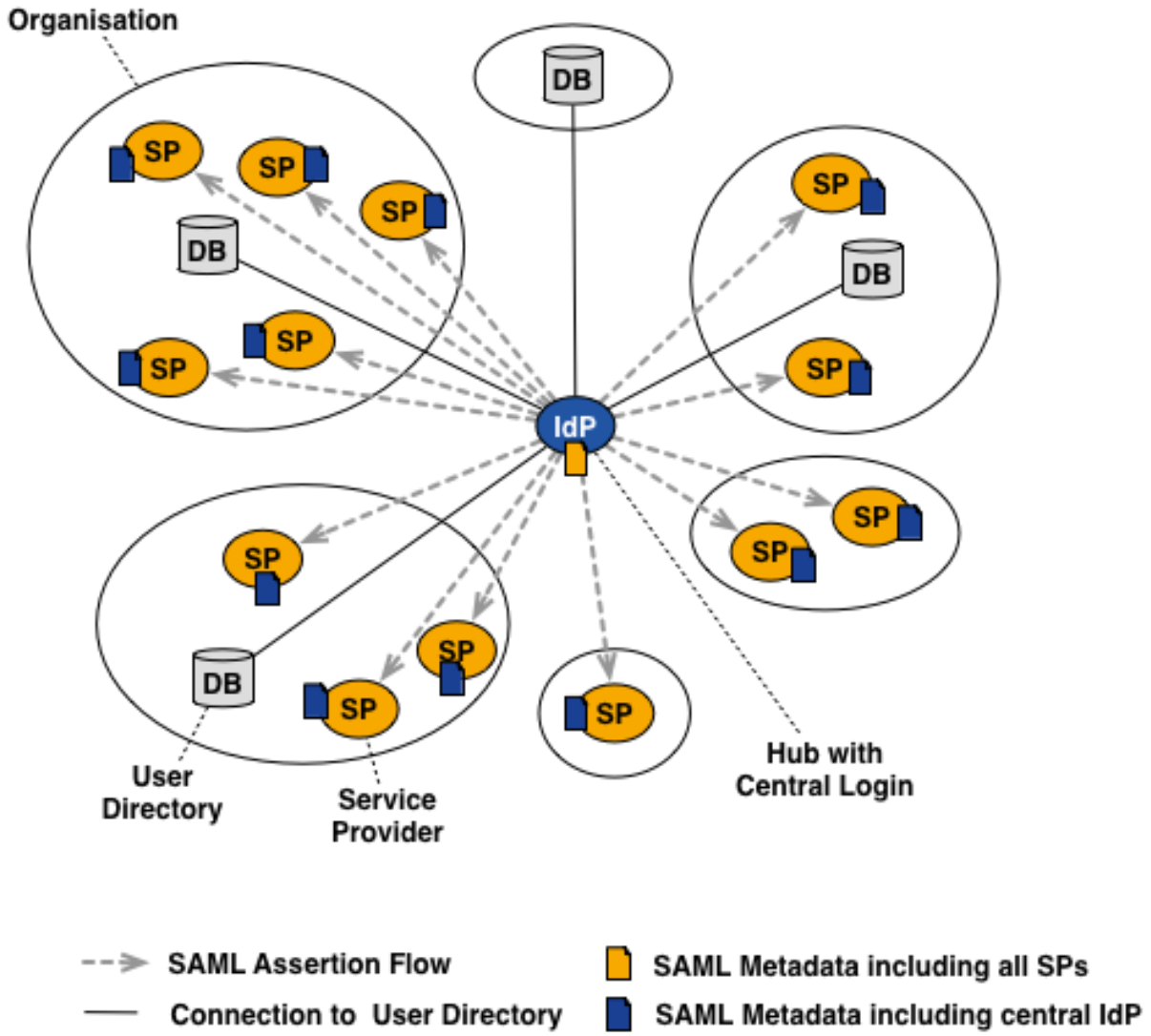
- Rely on a central hub or proxy via which all SAML assertions are sent.
- The hub serves as a SP versus the IdP and as an IdP versus the SP in the federation.
- Each organisation still operates their own IdP connected to a local user database but the IdP typically only needs metadata of the hub.
- SPs only need metadata for the hub.
- Hub has to be carefully secured and protected (single-point of failure).
- The hub never learns about the user's credential (only knows which entities are in the federation)
- The hub can be used to "connect" individual SPs and IdPs using for example a web interface.
- Interfederation scenarios are non trivial to handle.



Source: https://wiki.geant.org/

Hub-And-Spoke with Centralized Login

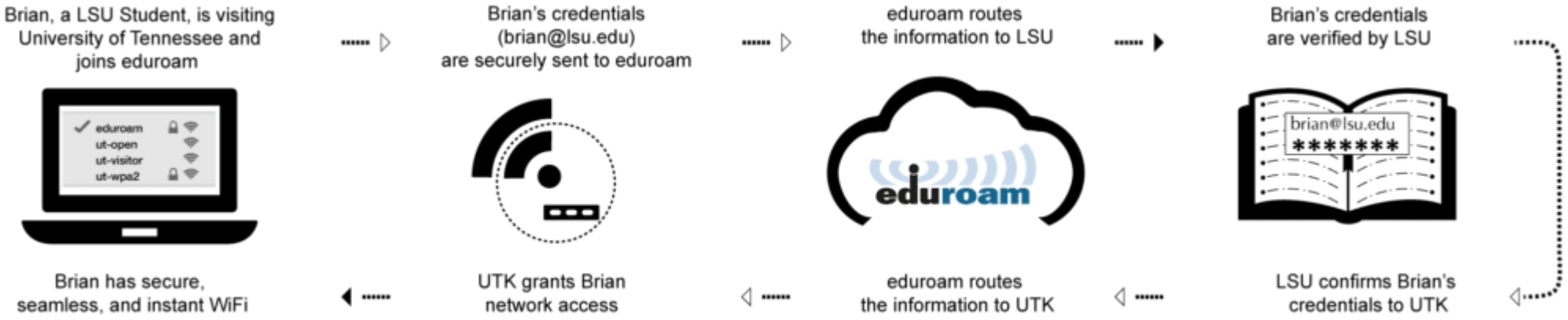
- Only one single IdP in the federation.
- All user databases are connected to a central IdP where users enter their organisation credentials on.
- IdP especially trusted by all organisations and highly available.
- Depending on the number of logins, scalability issues may arise.
- Very easy to support new authentication protocols on the hub thanks to the central login.



Source: https://wiki.geant.org/

Example : Eduroam

- Users from participating academic institutions secure Internet access at any other eduroam participating location.
- The mechanism by which authentication and authorisation works:
  - The authentication of a user is carried out at their Identity Provider (IdP), using their specific authentication method.
  - The authorisation decision allowing access to the network resources upon proper authentication is done by the Service Provider (SP), typically a WiFi hotspot (University campus, etc.).



Example: SIR - The RedIRIS Identity Federation

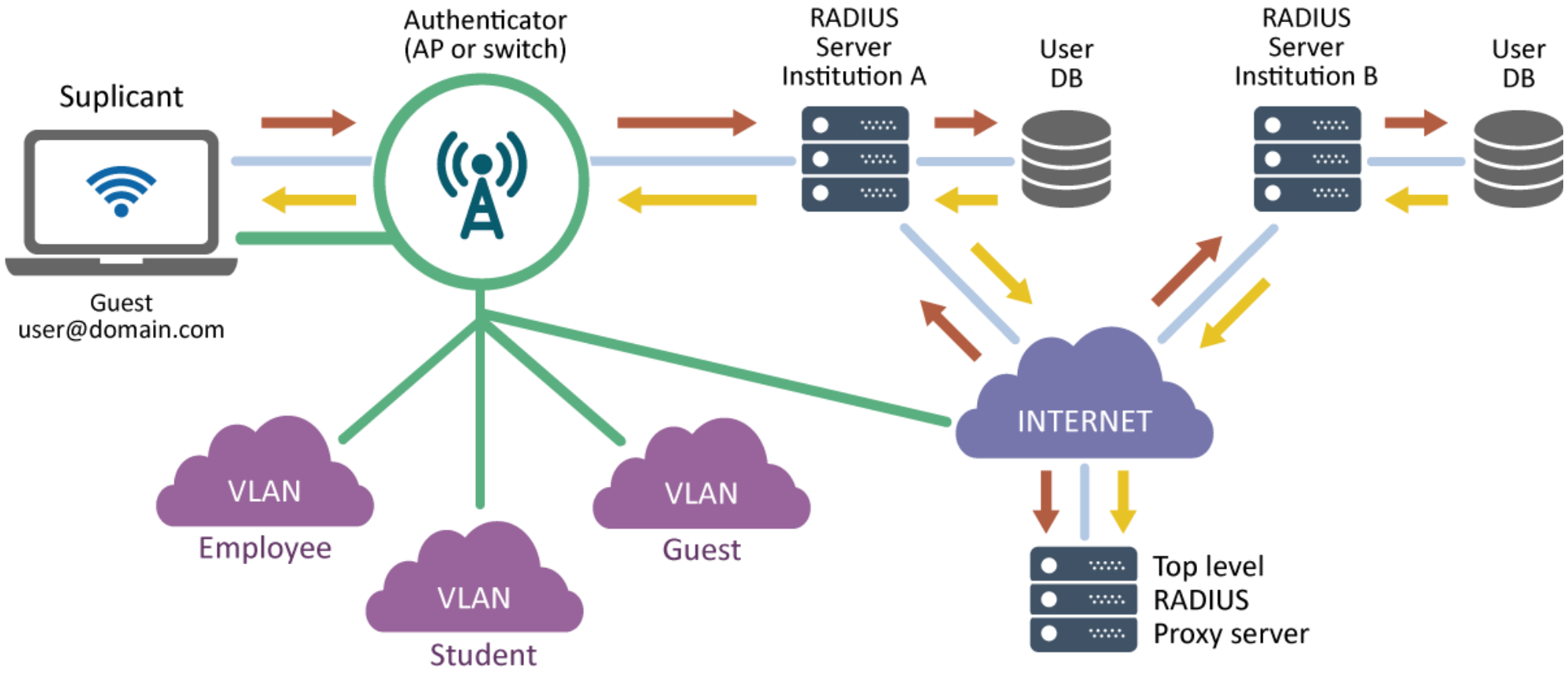
- Current version of SIR uses internally the **PAPI v.1 federation protocol** and is able to exchange data according to the following protocols:
- PAPI v.1
- SAML 1.1 / Shibboleth 1.3
- SAML 2 / Interoperable SAML2 Profile / Shibboleth 2
- eduGAIN, SAML 2.0 Int profile
- OpenID (version 1 and 2)
- Proprietary protocols:
  - Microsoft Live@Edu SSO
  - MSDN Academic Alliance
  - Wiley Trusted Proxy Server

IDP in SIR:

CSUC CTTC BSC ALBA Bibl.Cat
ESADE i2Cat ICFO UAB UOC
UPC UPF URL URV

https://www.rediris.es/sir/index.html.en

Example: RADIUS insfrastructure



Source: https://www.bsc.es/

Protocols / Workflows

Main Protocols

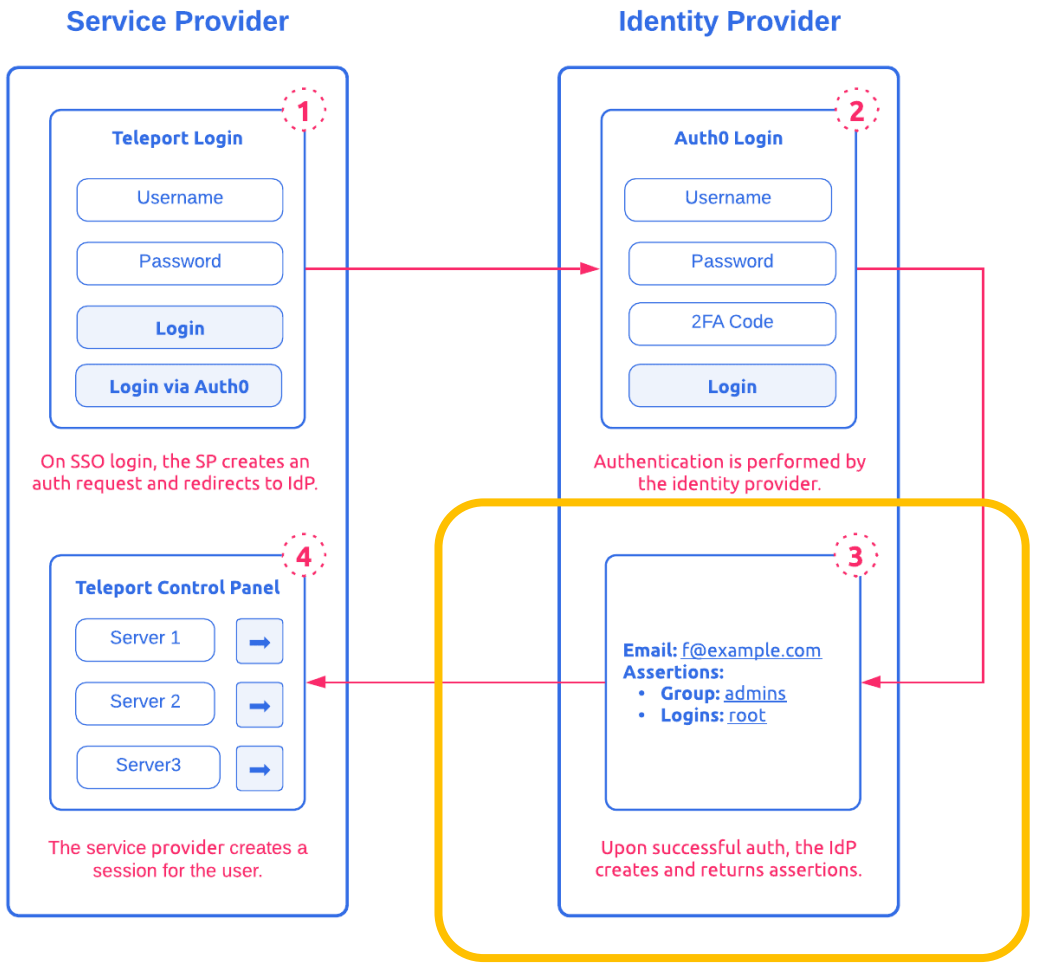
- Intra-federation, between IdP: SAML2Int
- Between SPs:
  - ▸ SAML2 & SAML1.1
  - ▸ PAPI
  - ▸ OpenID v1, v2 y OpenID Connect
  - ▸ OAuth2
  - ▸ CAS
  - Shibboleth

SAML2: Security Assertion Markup Language

- Open standard
- Exchanging authentication and authorization data between parties
- XML-based markup language
- Key components/elements
  - Roles (principal, IdP and SP)
  - Assertions
  - Protocols
  - Bindings
- Profile = use case + assertions + protocols+ bindings
- Typical use case: Web SSO

SAML2 assertion

- Statements transferred from IdP to SPs
- SPs use to make access-control decisions
- Three main types:
  - Authentication statement
    - Asserts that the user is authenticated
    - Specifies IdP, time, method,…
  - Attribute statement
    - Asserts that a user is associated with certain attributes
  - Authorization decision statement
    - Asserts that user is permitted to perform some action

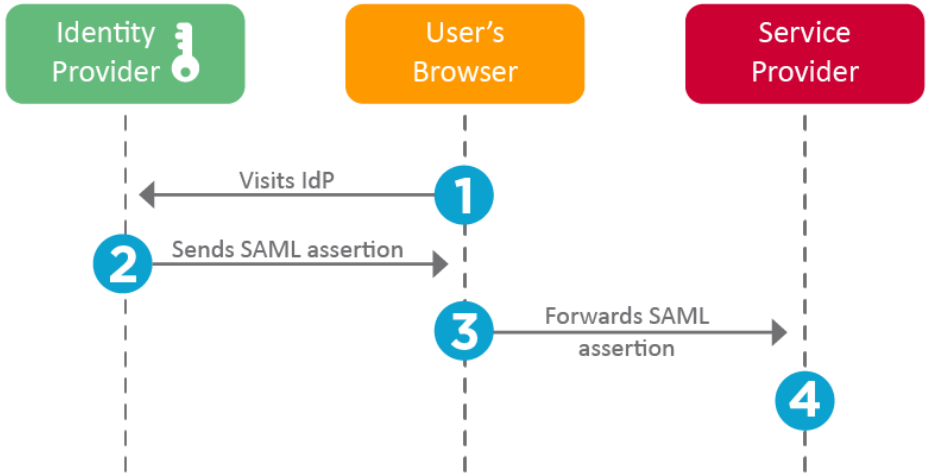


SAML2 protocols and bindings

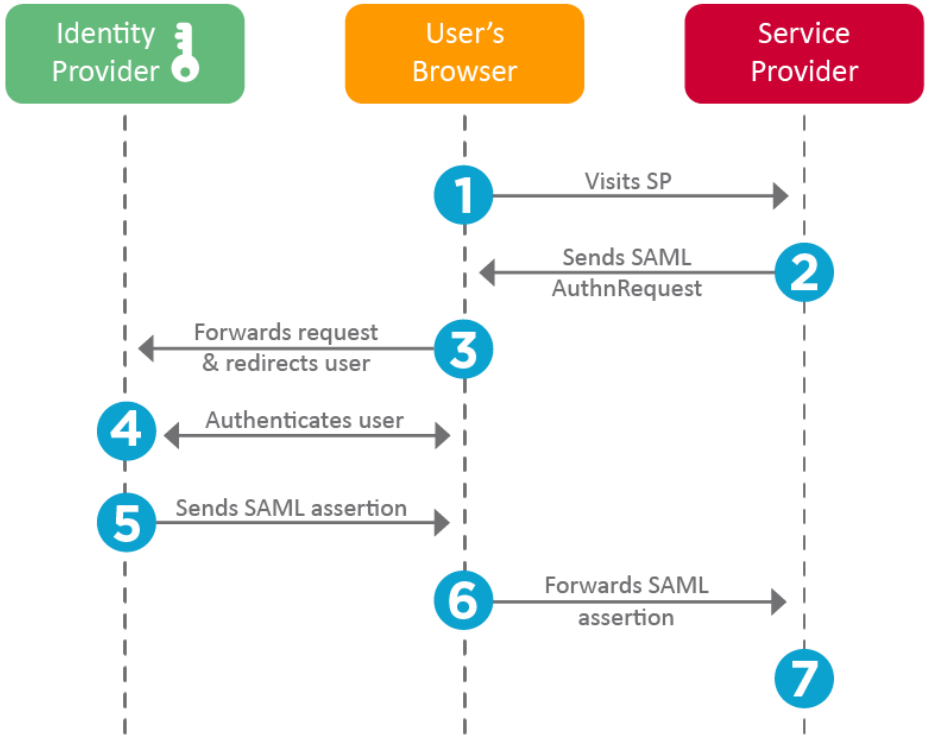
- **Protocol: What** is transmitted
  - Describes the way assertions are packaged and sent (workflows) in request/response elements
  - Main protocols
    - Authentication Request Protocol
    - Artifact Resolution Protocol
- **Binding: How** is transmitted
  - Map request/responses onto standard messaging protocols
  - HTTP redirect (browser redirect)
  - HTTP POST
  - HTTP artifact
  - SOAP

SAML2 workflows

IdP-initiated workflow



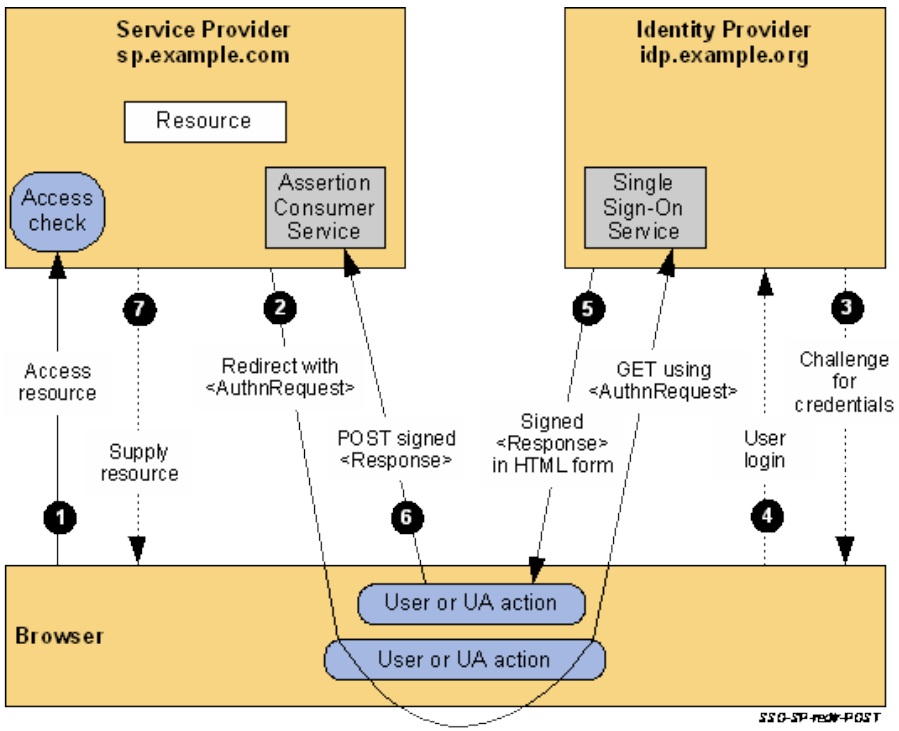
SP-initiated workflow



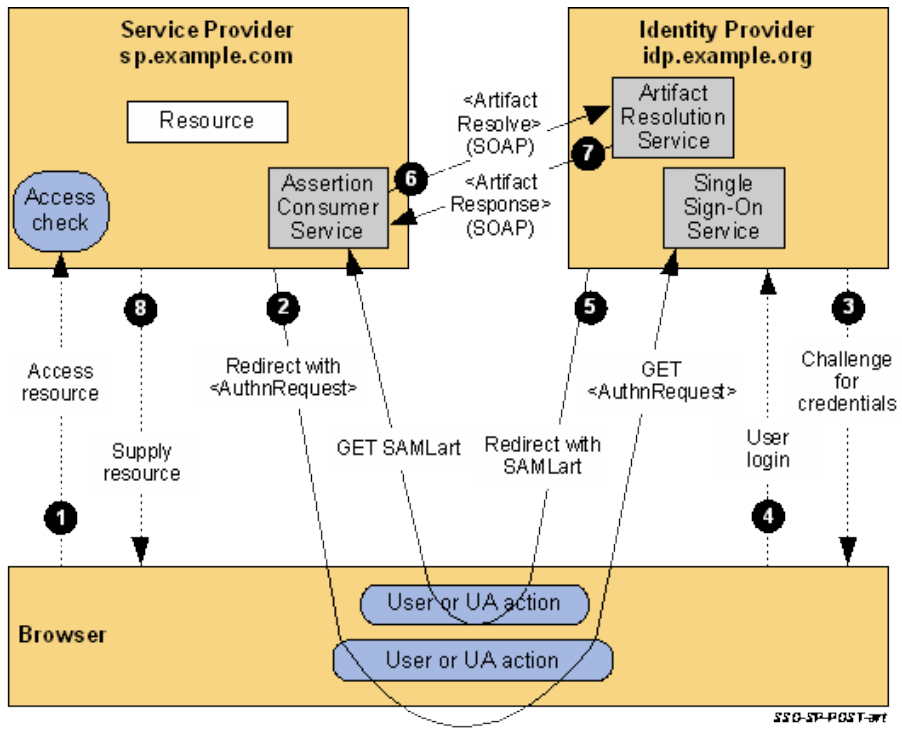
Source: https://developer.fourth.com/

Artifact Binding

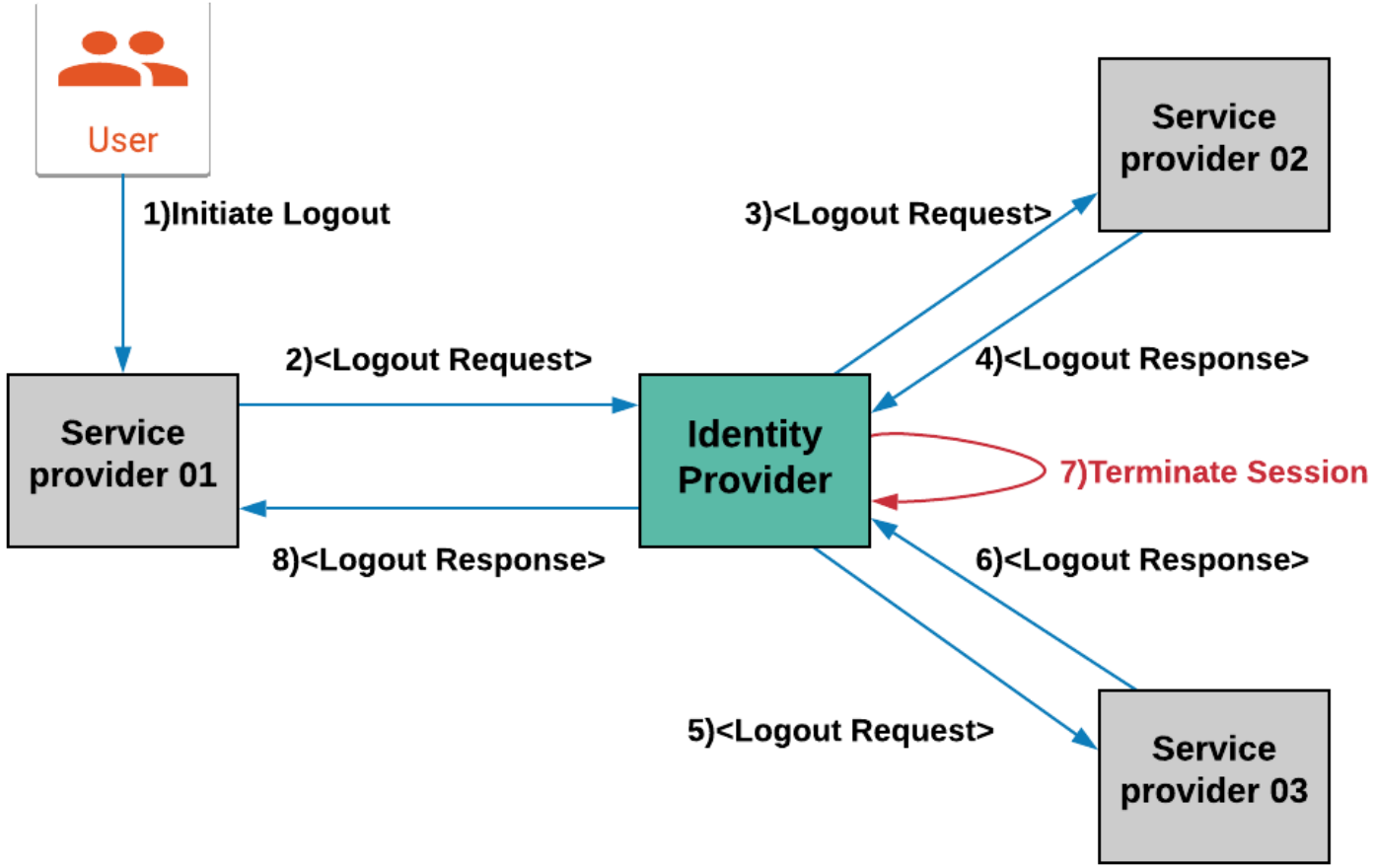
without



with

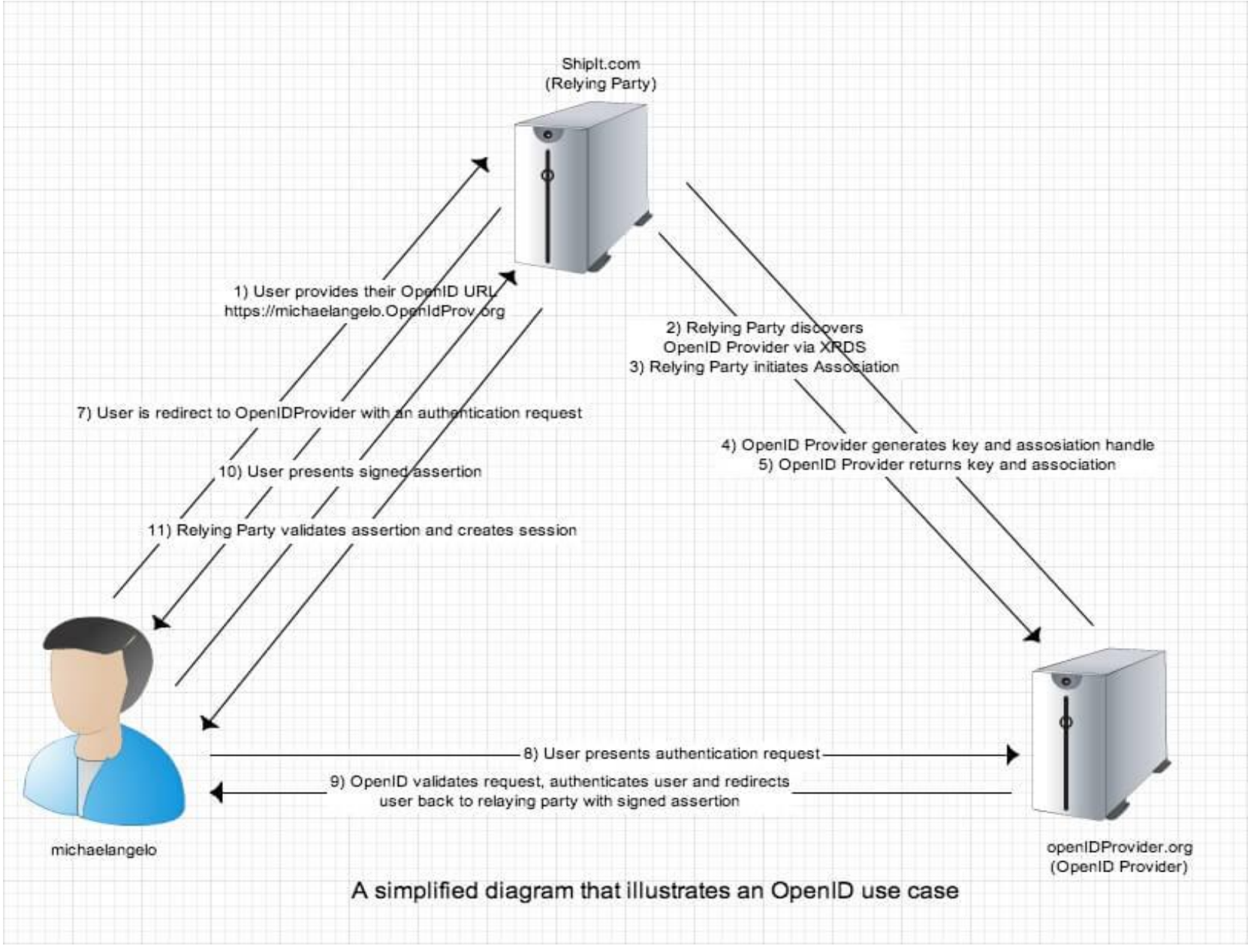


SAML2 Single Logout (SLO)



OpenID

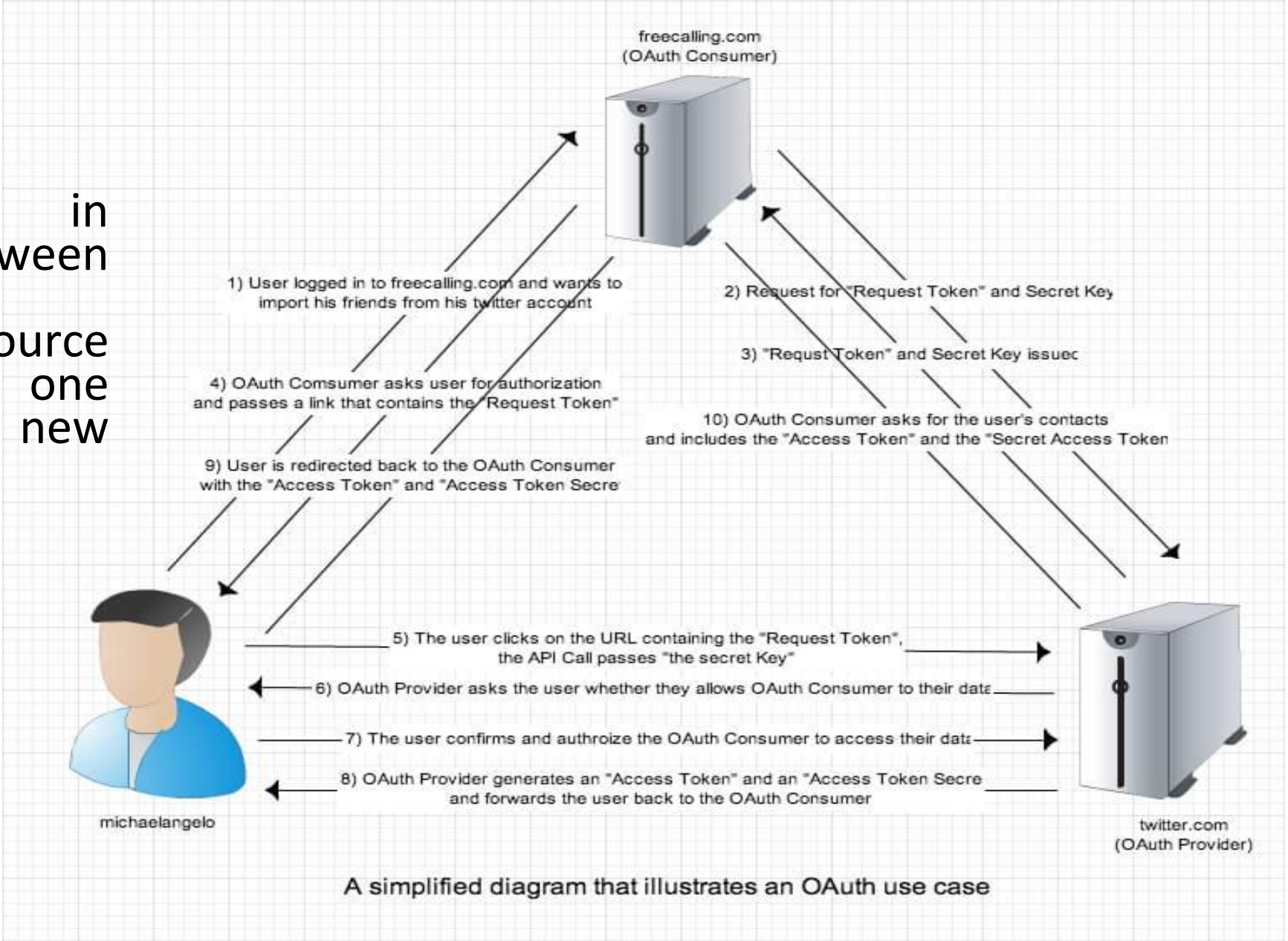
- Authentication
- Widely used in SSO for consumers
- E.g. Google Sign-in to apps like Youtube



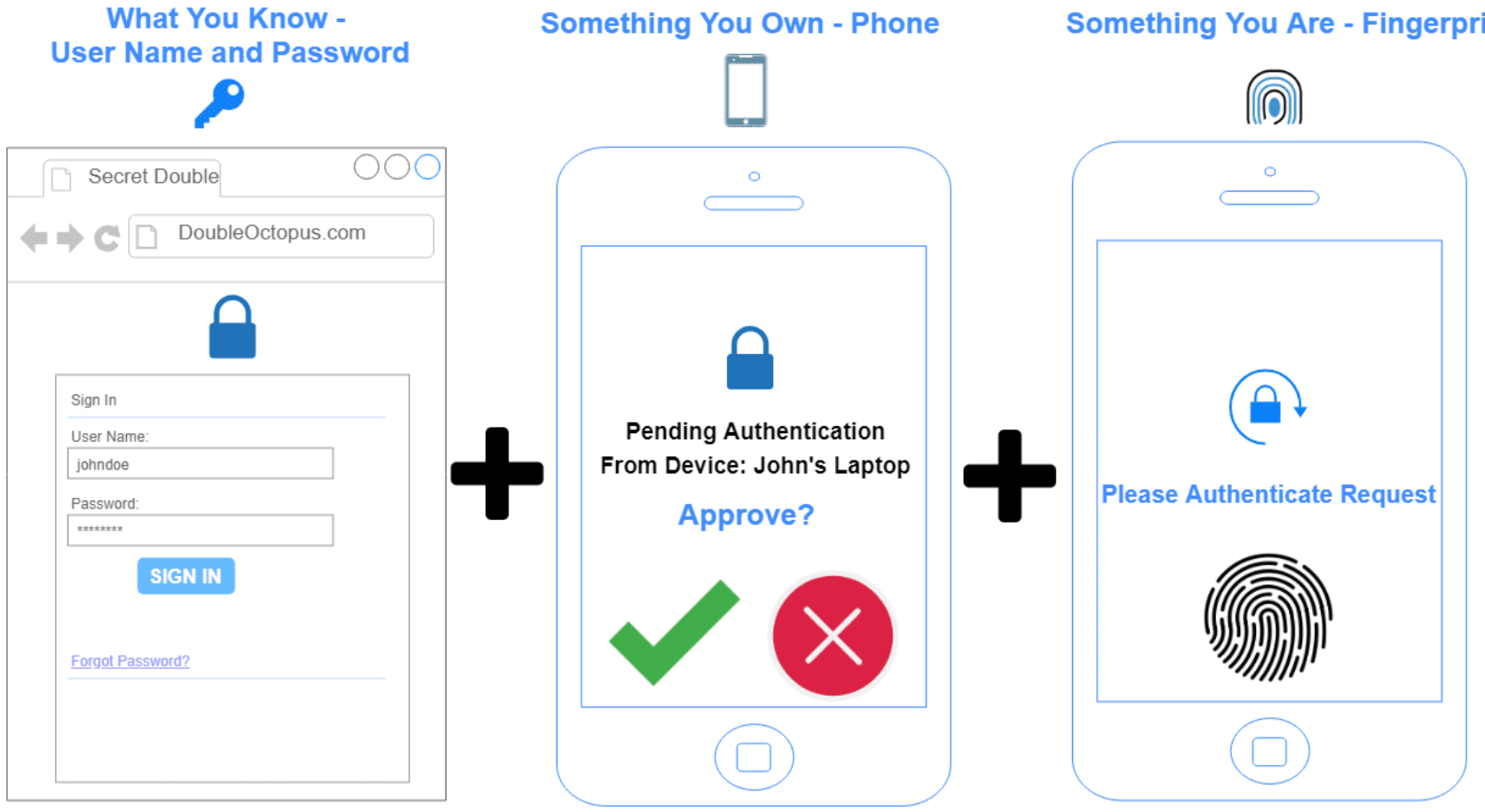
A simplified diagram that illustrates an OpenID use case

OAuth

- Authorization
- Widely used in authorization between applications
- E.g. automatically source contacts from one Facebook to a new application



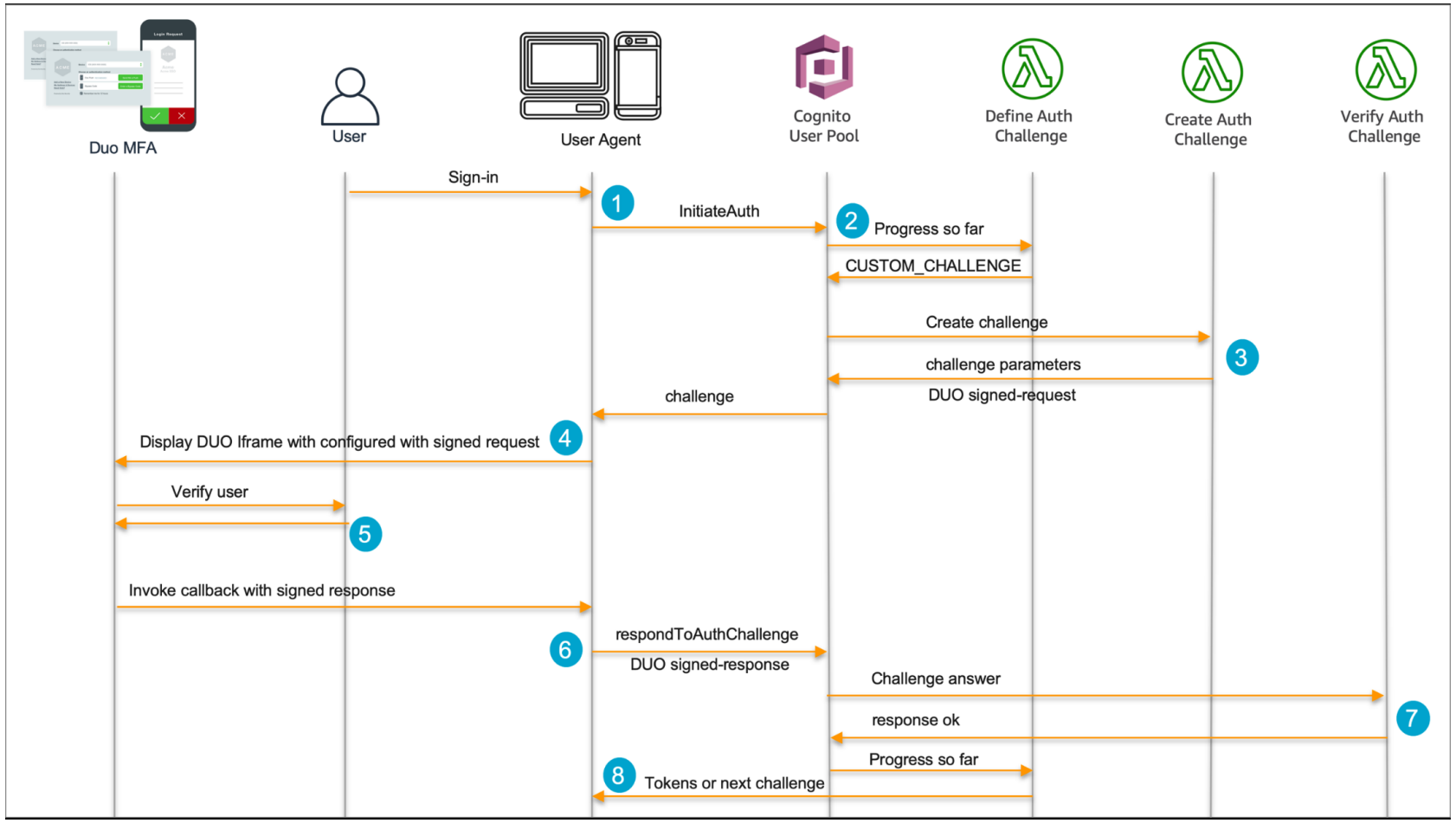
Multi-Factor Authentication (MFA)



https://doubleoctopus.com/security-wiki/authentication/multi-factor-authentication/

SECRET DOUBLE OCTOPUS

Multi-Factor Authentication (MFA)



https://aws.amazon.com/blogs/security/how-to-configure-duo-multi-factor-authentication-with-amazon-cognito/

Wrap-up

Security concerns of IdF

- Breaches caused by the use of weak passwords.
- A single compromised set of federated credentials can grant hackers access to multiple applications
- Lack of federated identity management plans in many businesses.
- User information must be shared with the third party entrusted with authentication.
- Not all providers within a federation conform to the same security standards
- The use of multiple providers creates additional points of vulnerability.
- Insider threats and identity theft remain problematic even with the use of a federated system.
- Companies need to be completely certain of the trustworthiness of users in the network and have authentication protocols designed to ensure each user is who he or she claims to be.
- Employee education is necessary to minimize the risk of human error
- Improper provisioning leading to privilege creep can also leave the door open for devastating breaches.
- Any temporary access necessary for short-term projects should be revoked as soon as it’s no longer needed.

References

- M. Aldosary and N. Alqahtani, “A Survey on Federated Identity Management Systems: Limitation and Solutions,” IJNSA, vol. 13, 2021.
- A. Armando et al., “Formal analysis of SAML 2.0 web browser single sign-on,” in Proc. ACM FMSE, 2008.
- W. Li and C.J. Mitchell, “Analysing the Security of Google’s implementation of OpenID Connect,” Lecture Notes in Computer Science, 2016.

Cybersecurity Management
GCS 2.1 - Identity Federation

2022-2023

Prof. Marc Ruiz

marc.ruiz-ramirez@upc.edu