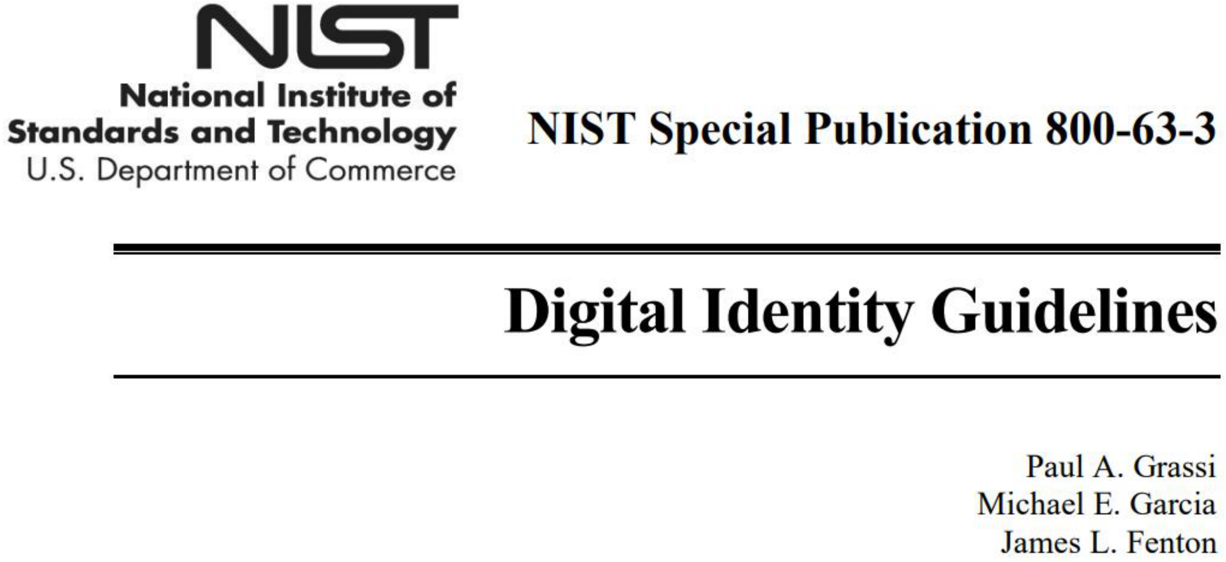
Cybersecurity Management
T5- Identity Management

marc.ruiz-ramirez@upc.edu

Outline

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

Basic concepts



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

Basic concepts

- **Digital Identity**
  - Unique representation of a subject engaged in an online transaction.
  - Always unique in the context of a digital service…
  - …but not necessarily need to uniquely identify the subject in all contexts
- **Identity proofing**
  - Establishes that a subject is who they claim to be
- **Digital authentication**
  - Process of determining the validity of one or more authenticators used to claim a digital identity
  - Establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate
  - Provides reasonable risk-based assurances that the subject accessing the service today is the same as that which previously accessed the service

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

Accessing a digital service may not mean that the subject's real-life identity is known

Profiling

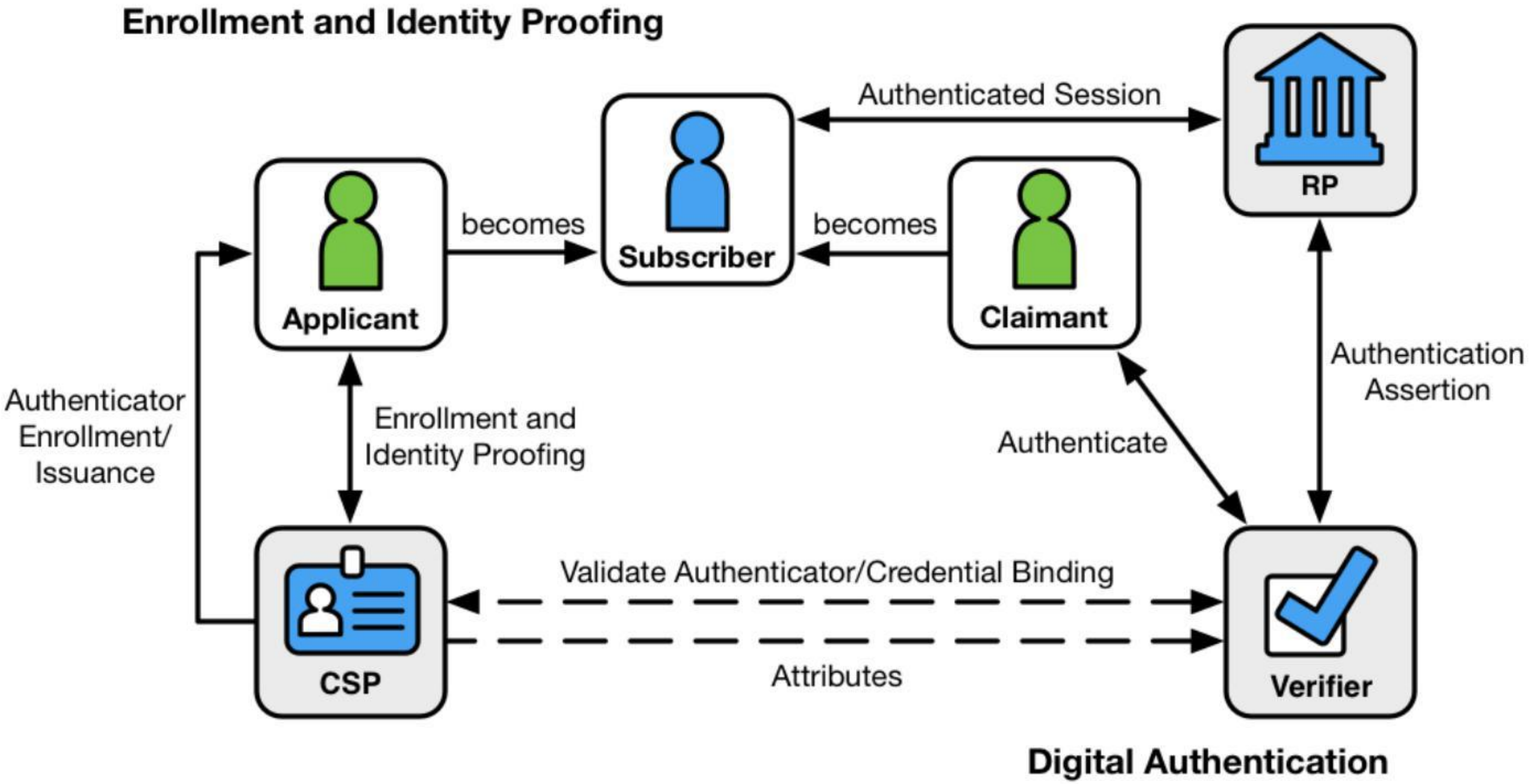
Physical persons may have several eIDs, depending on the relationships and attributes that the person wants to associate to that eID:

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

Attribute set standards:

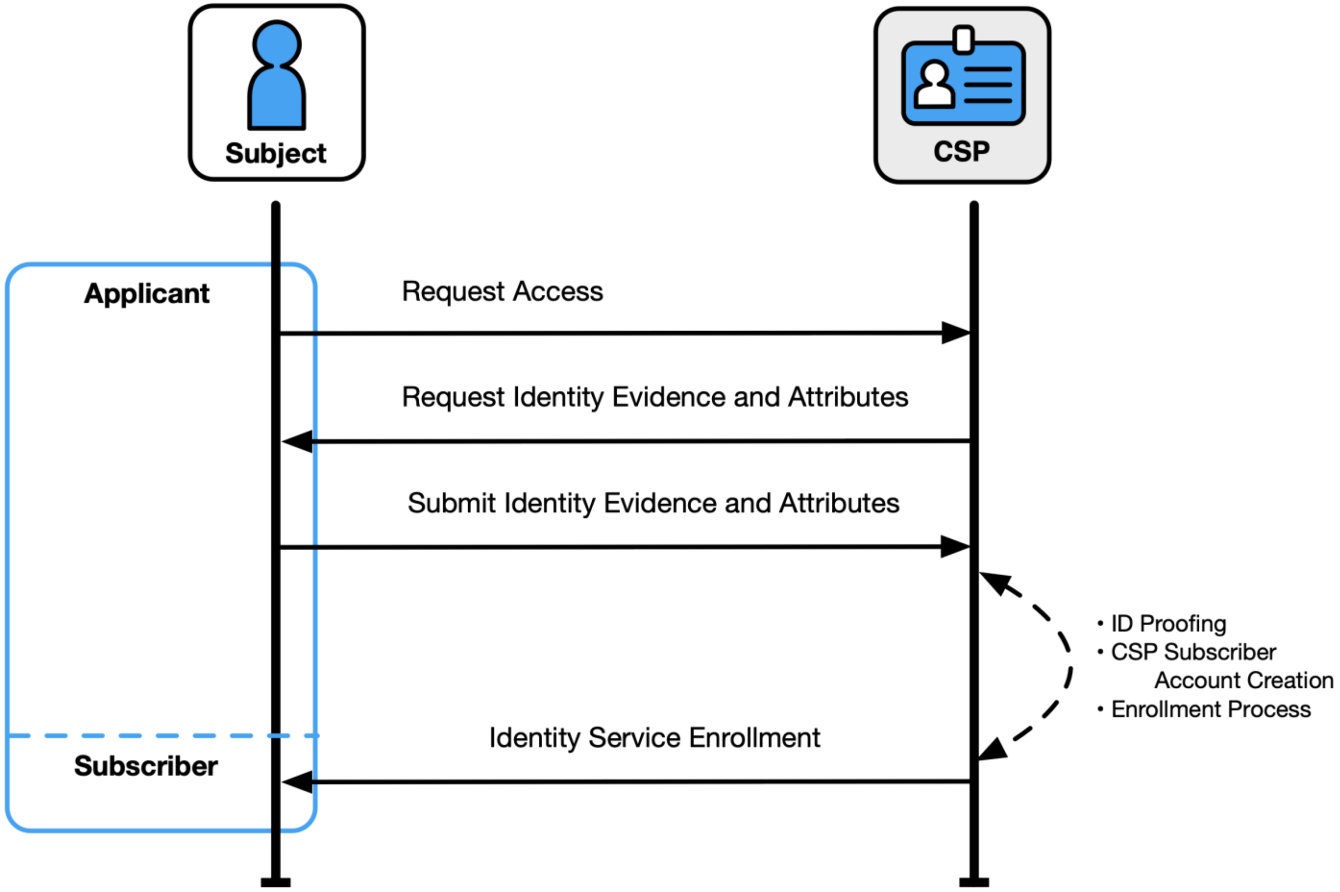
- DAP X520
- RFC2798 inetOrgPerson LDAP Object Class
- RFC3671 Collective Attributes in LDAP

Digital Identity Model (NIST)



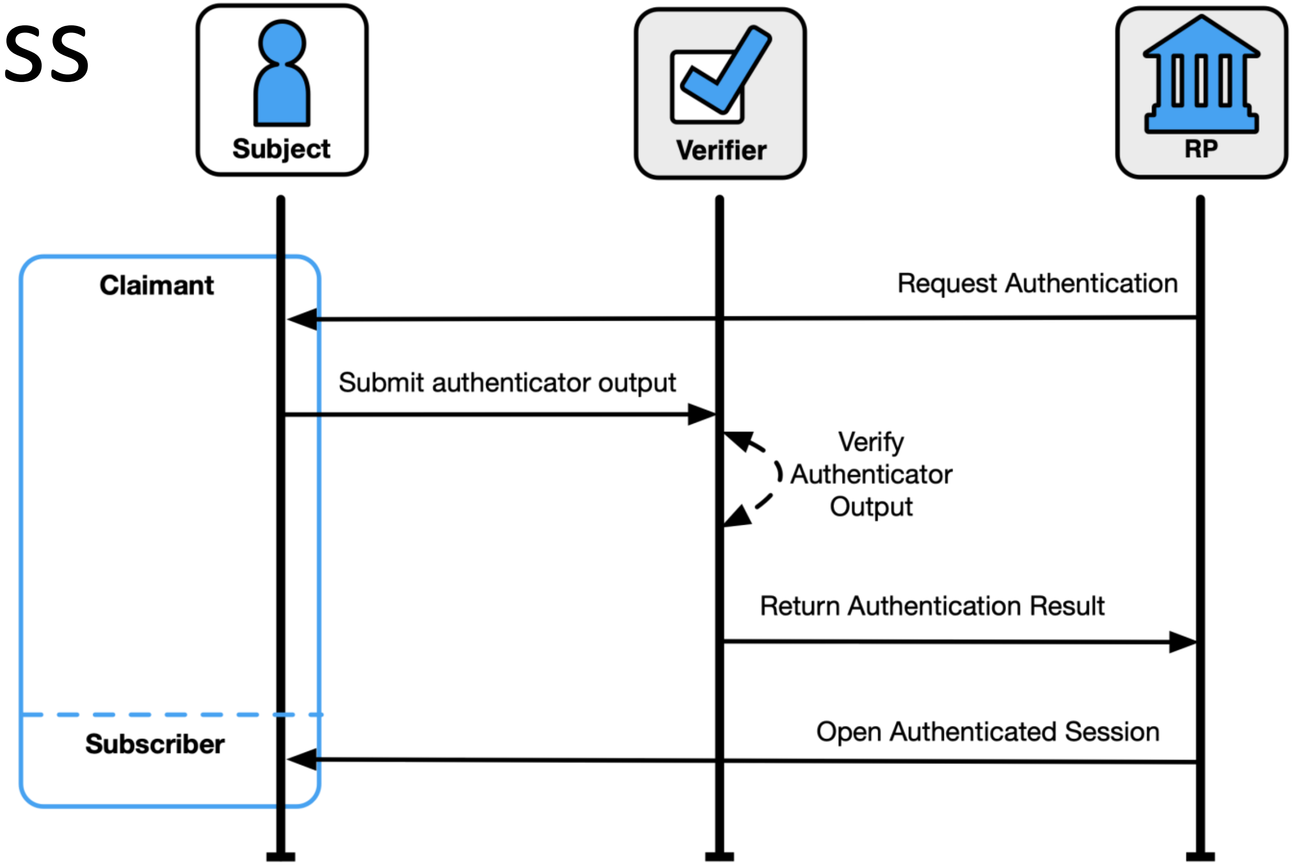
Enrolment and Identity Proofing

- **Applicant:** the party whose identity needs to be proofed (undergoing the processes of enrollment and identity proofing.)
- **Subscriber**: Applicant after successfully proofing process is completed
- **CSP (Credential Service Provider)**: A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers



Subject
CSP
Applicant
Subscriber
Request Access
Request Identity Evidence and Attributes
Submit Identity Evidence and Attributes
• ID Proofing
• CSP Subscriber Account Creation
• Enrollment Process
Identity Service Enrollment

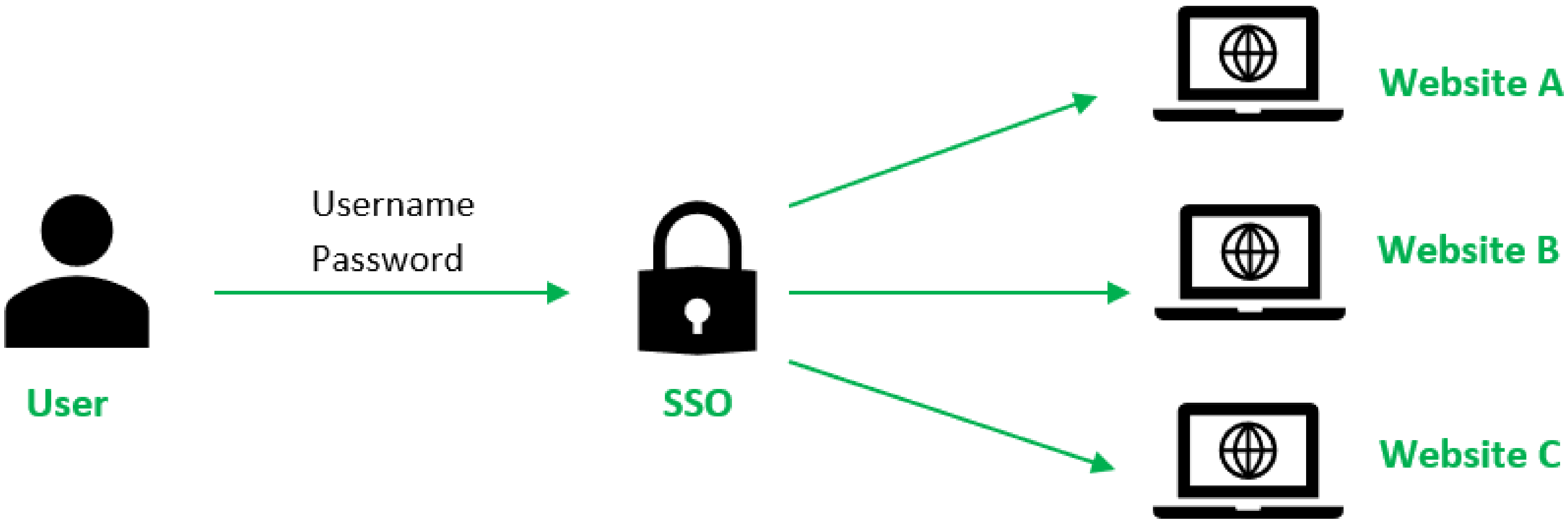
Authentication Process


Subject
Verifier
RP
Claimant
Request Authentication
Submit authenticator output
Verify Authenticator Output
Return Authentication Result
Subscriber
Open Authenticated Session

- **Claimant:** A subject whose identity is to be verified using one or more authentication protocols.
- **Subscriber**: A claimant who has received successful authenticator from a verifier
- **Verifier (aka CSP)**: entity that verifies the claimant's identity by verifying the claimant's possession and control of one or multiple authenticators using an authentication protocol.

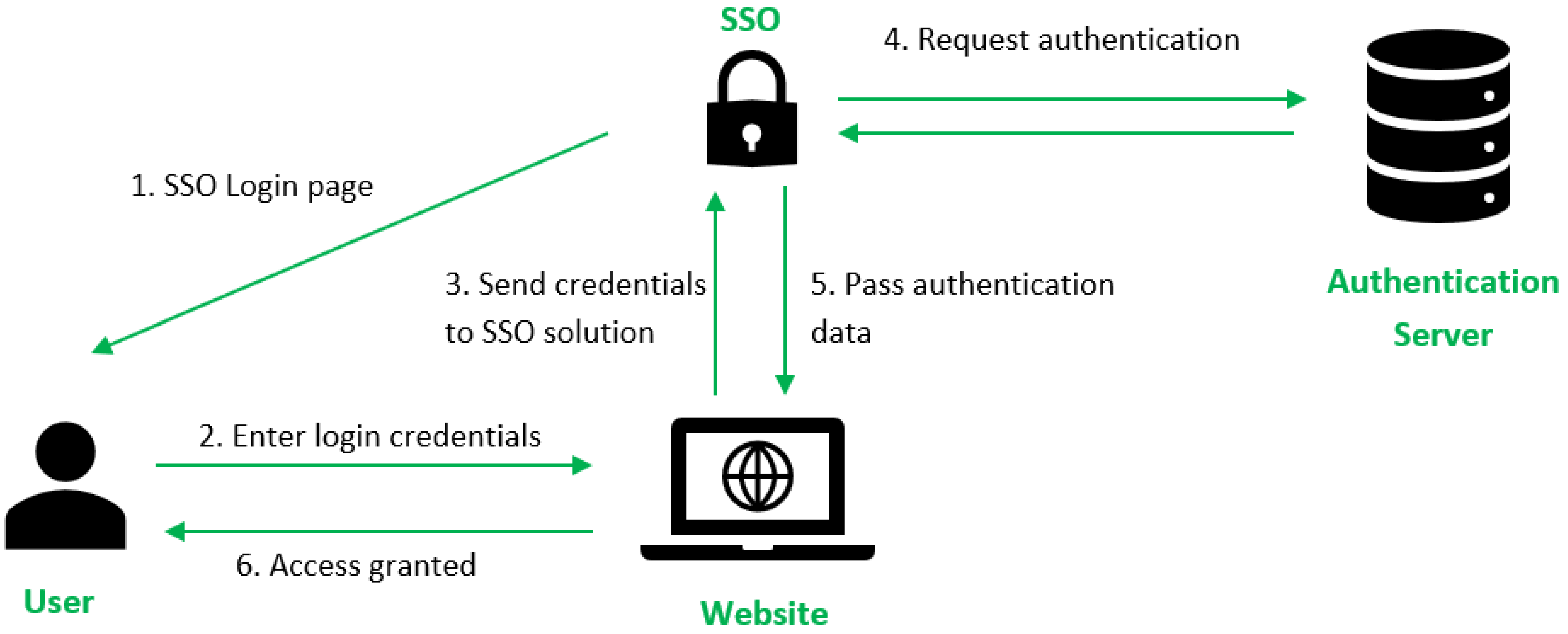
- **Relying Party (RP):** An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

Single Sign-On Authentication



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

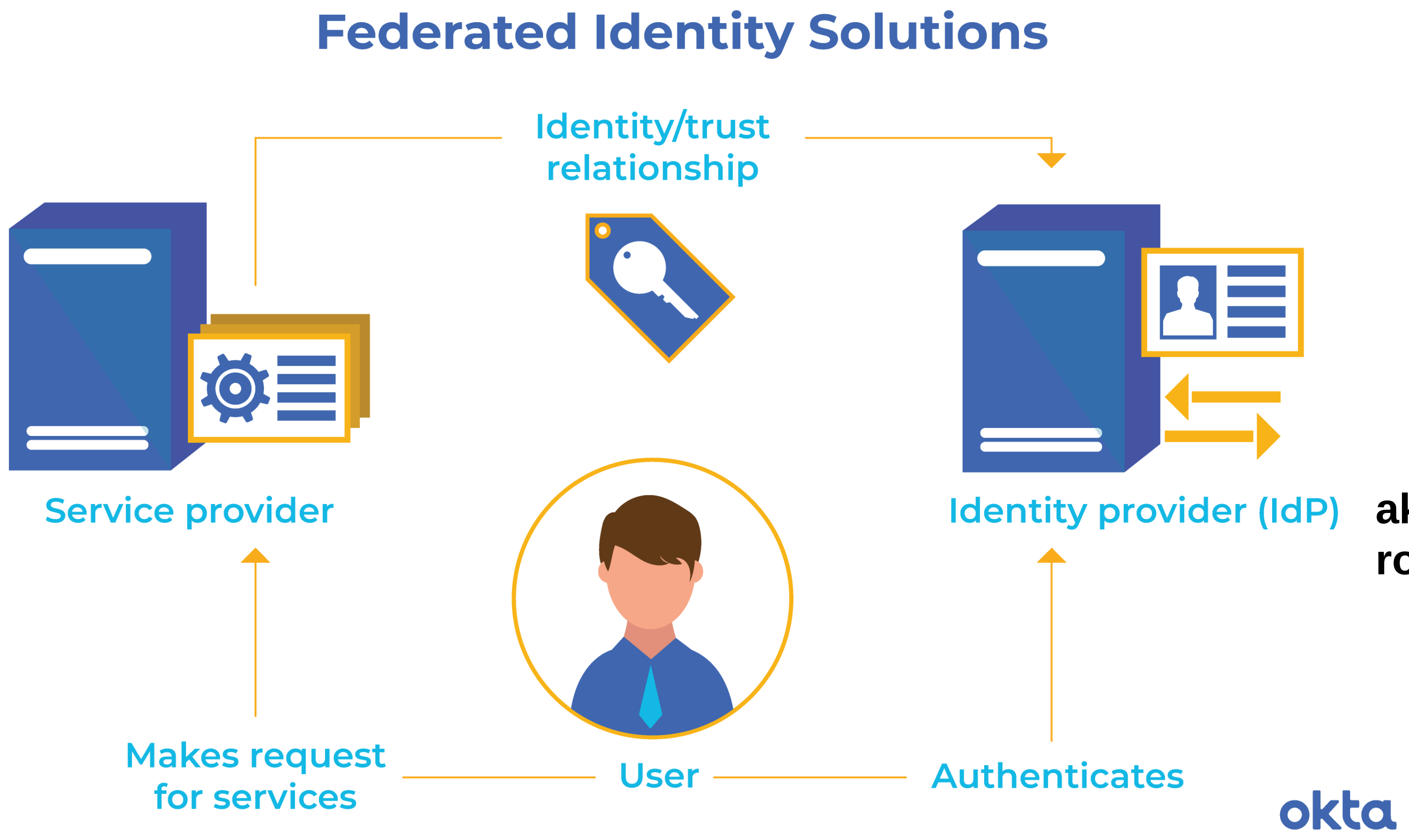
Single Sign-On Authentication


SSO
4. Request authentication
1. SSO Login page
3. Send credentials to SSO solution
5. Pass authentication data
Authentication Server
2. Enter login credentials
User
6. Access granted
Website

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

Identity Federation (IdF)

Basic Concept


Federated Identity Solutions
Identity/trust relationship
Service provider
Identity provider (IdP)
Makes request for services
User
Authenticates
okta

aka RP

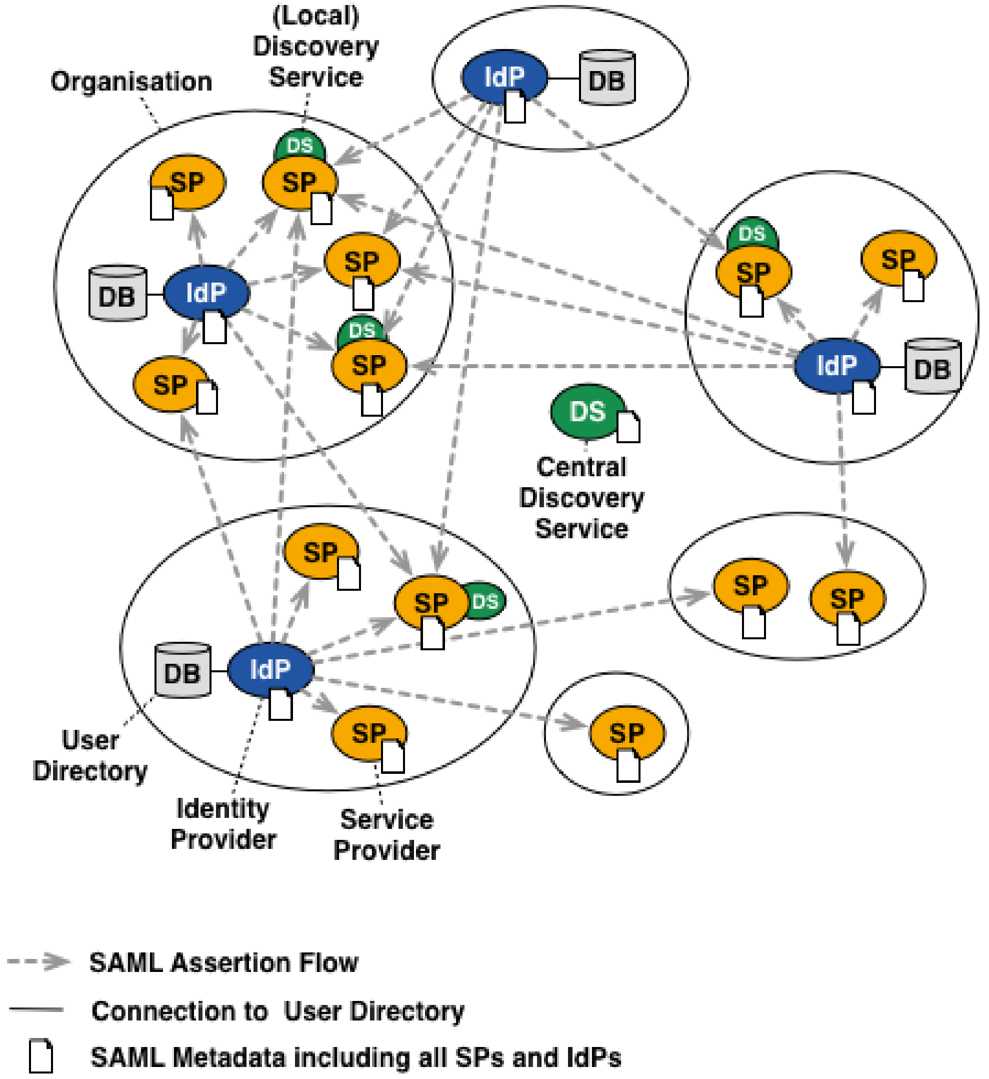
aka CSP, includes role of verifier

IdF in 5 minutes

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

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).

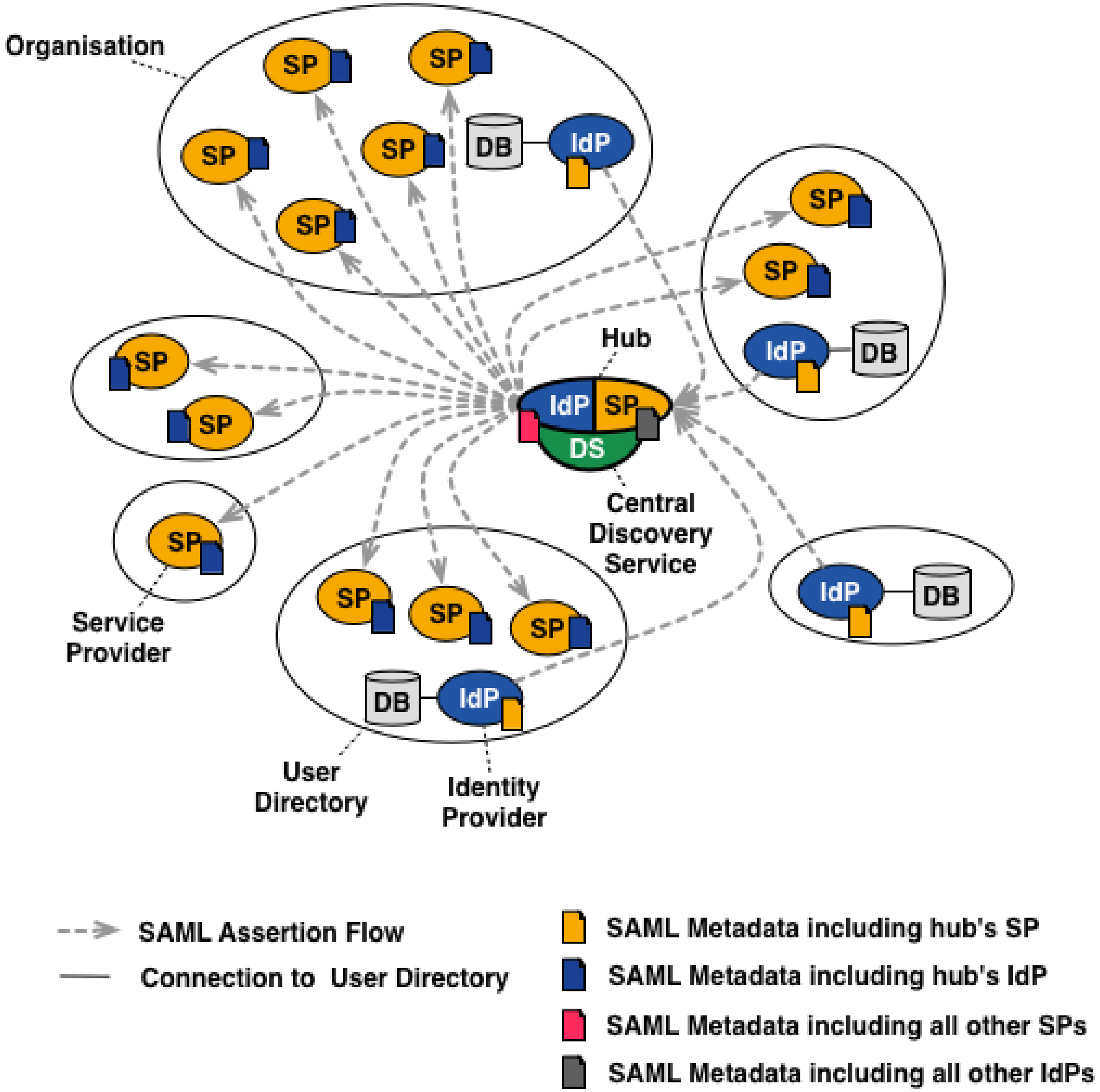


(Local) Discovery Service
Organisation
IdP
DB
SP
DS
Central Discovery Service
User Directory
Identity Provider
Service Provider
SAML Assertion Flow
Connection to User Directory
SAML Metadata including all SPs and IdPs

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.

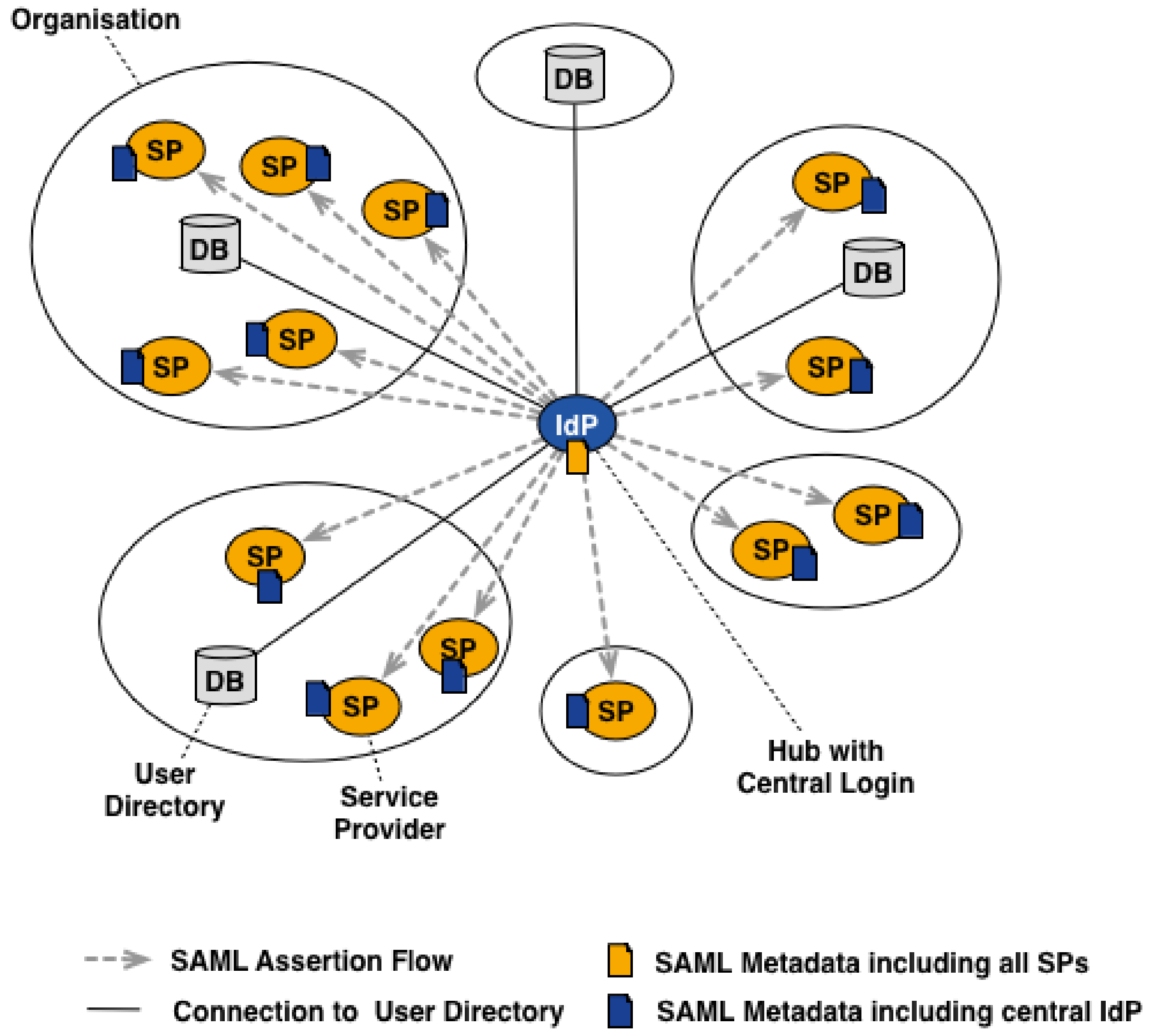


Organisation
SP
IdP
DB
Hub
IdP
SP
DS
Central Discovery Service
Service Provider
User Directory
Identity Provider
SAML Assertion Flow
Connection to User Directory
SAML Metadata including hub's SP
SAML Metadata including hub's IdP
SAML Metadata including all other SPs
SAML Metadata including all other IdPs

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.

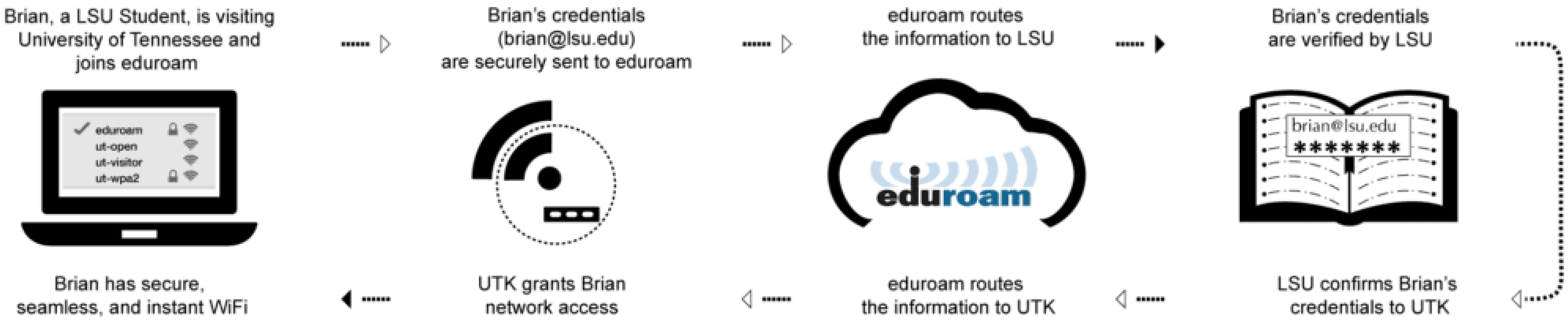


Organisation
DB
SP
IdP
User Directory
Service Provider
Hub with Central Login
SAML Assertion Flow
Connection to User Directory
SAML Metadata including all SPs
SAML Metadata including central IdP

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.).



Brian, a LSU Student, is visiting University of Tennessee and joins eduroam

Brian's credentials (brian@lsu.edu) are securely sent to eduroam

eduroam routes the information to LSU

Brian's credentials are verified by LSU

LSU confirms Brian's credentials to UTK

eduroam routes the information to UTK

UTK grants Brian network access

Brian has secure, seamless, and instant WiFi

Example: SIR - The RedIRIS Identity Federation

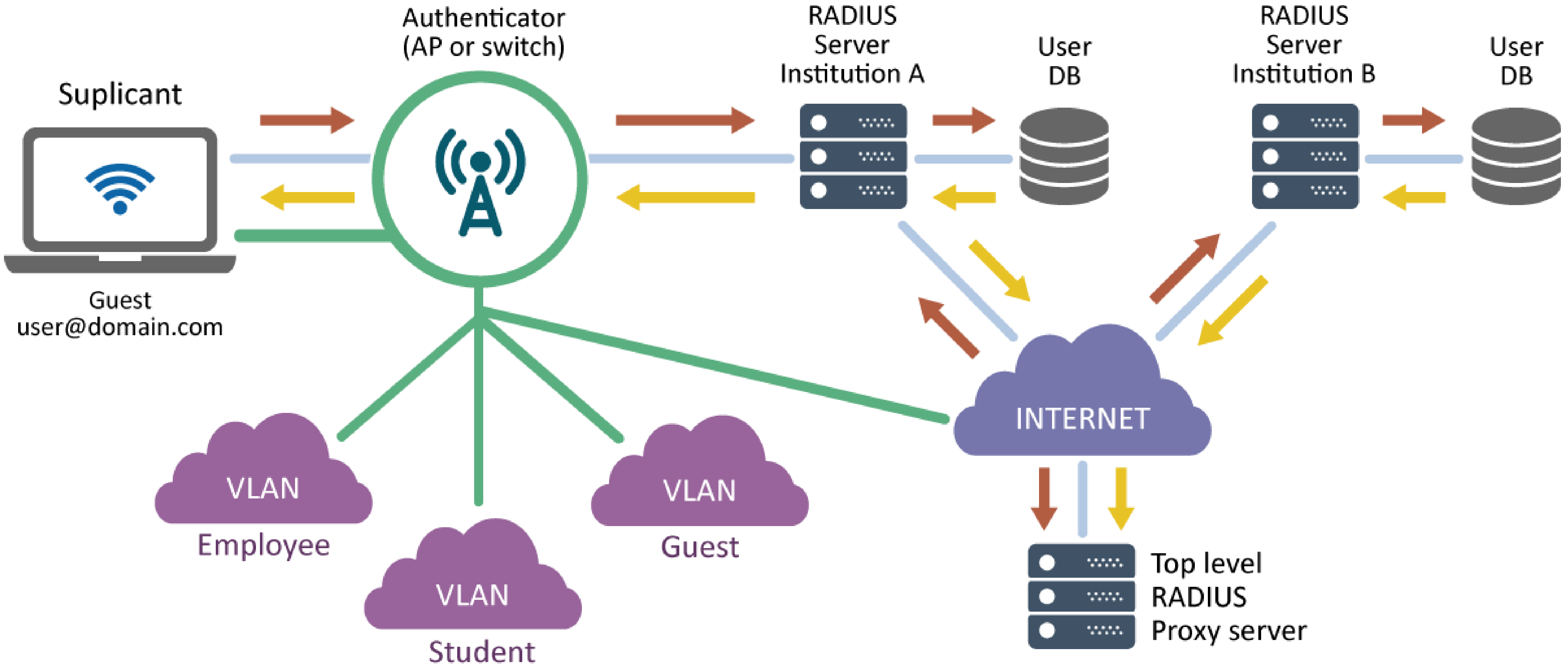
- Current version of SIR uses internally the **PAPI v.1 federation protocol** and is able to exchange data according to the following protocols:
- PAPI v.1
- SAML 1.1 / Shibboleth 1.3
- SAML 2 / Interoperable SAML2 Profile / Shibboleth 2
- eduGAIN, SAML 2.0 Int profile
- OpenID (version 1 and 2)
- Proprietary 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

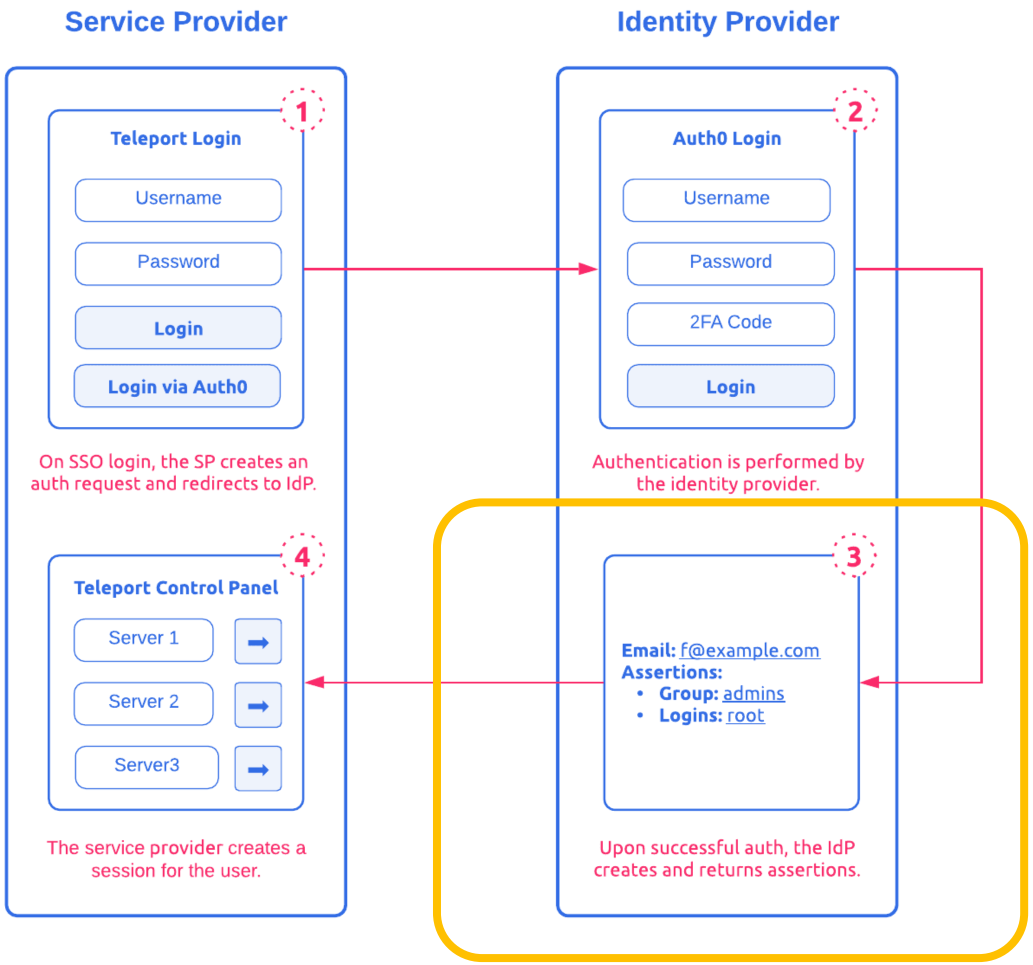
- Intra-federation, between IdP: SAML2Int
- Between SPs:
  - ▸ SAML2 & SAML1.1
  - ▸ PAPI
  - ▸ OpenID v1, v2 y OpenID Connect
  - ▸ OAuth2
  - ▸ CAS
  - Shibboleth

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

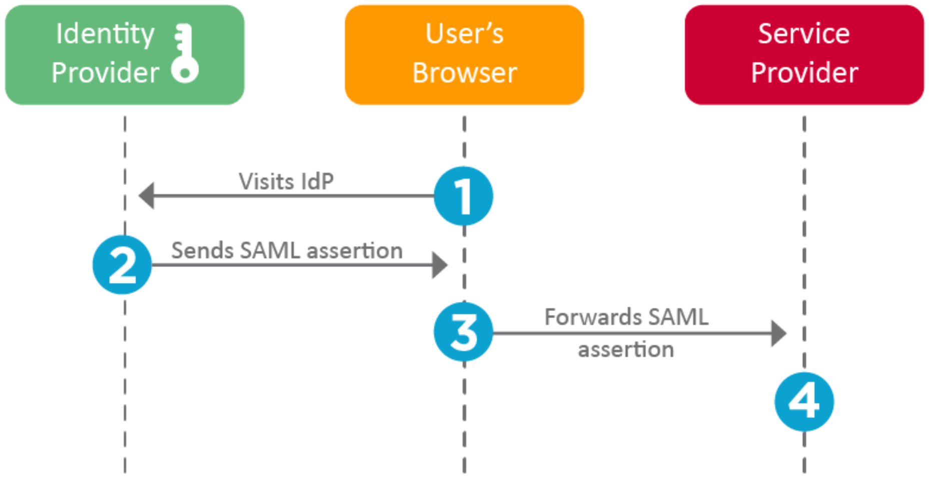

Service Provider
Identity Provider
1
Teleport Login
Username
Password
Login
Login via Auth0
On SSO login, the SP creates an auth request and redirects to IdP.
2
Auth0 Login
Username
Password
2FA Code
Login
Authentication is performed by the identity provider.
4
Teleport Control Panel
Server 1
Server 2
Server3
The service provider creates a session for the user.
3
Email: f@example.com
Assertions:
• Group: admins
• Logins: root
Upon successful auth, the IdP creates and returns assertions.

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



Identity Provider

User's Browser

Service Provider

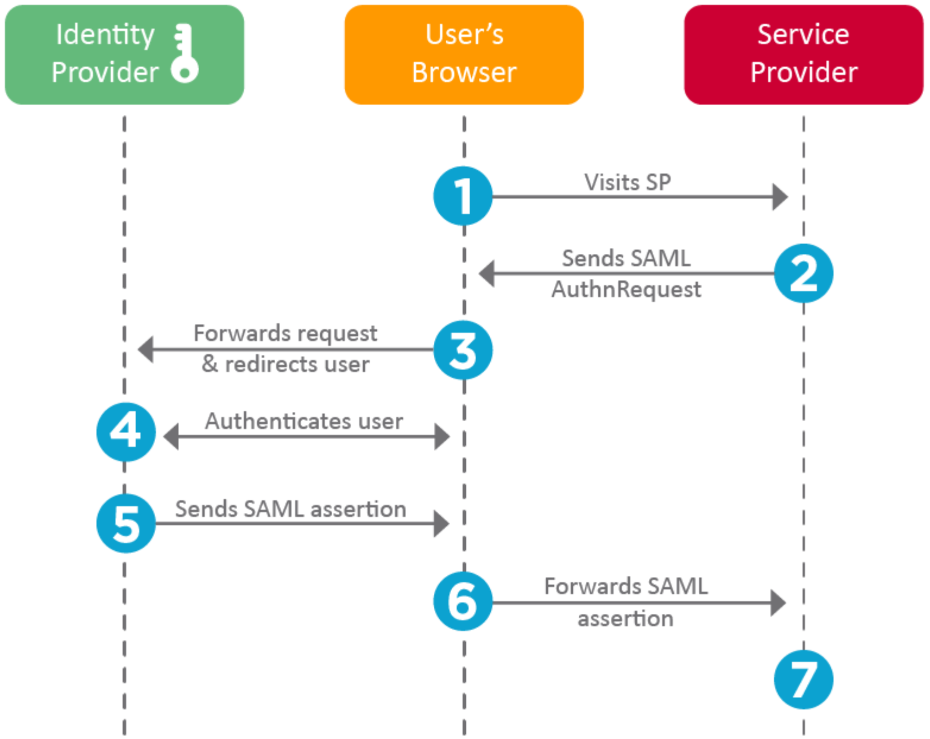
1 Visits IdP

2 Sends SAML assertion

3 Forwards SAML assertion

4

SP-initiated workflow



Identity Provider

User's Browser

Service Provider

1 Visits SP

2 Sends SAML AuthnRequest

3 Forwards request & redirects user

4 Authenticates user

5 Sends SAML assertion

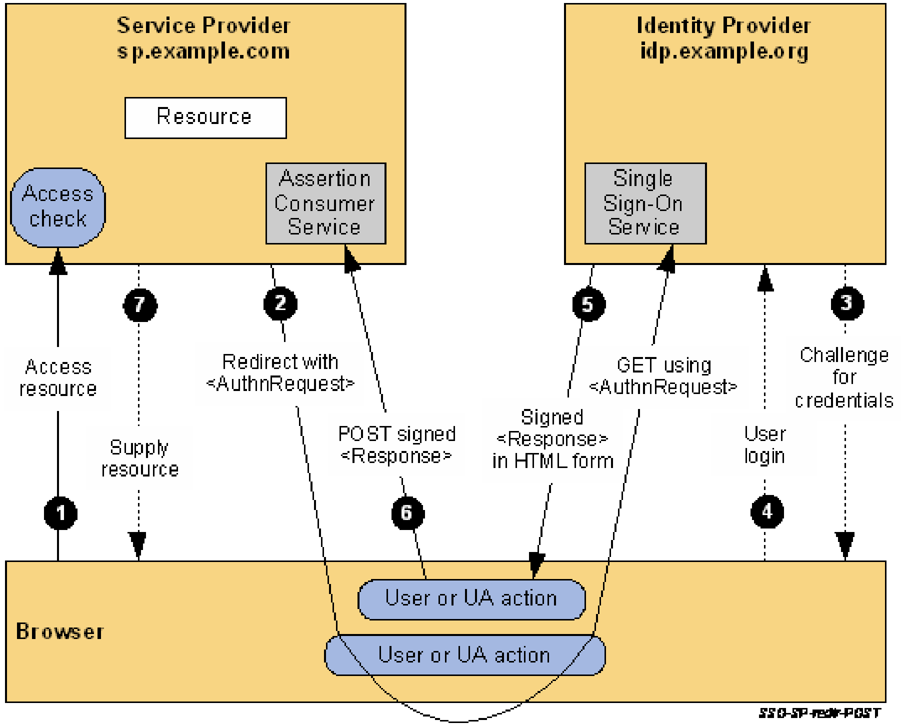
6 Forwards SAML assertion

7

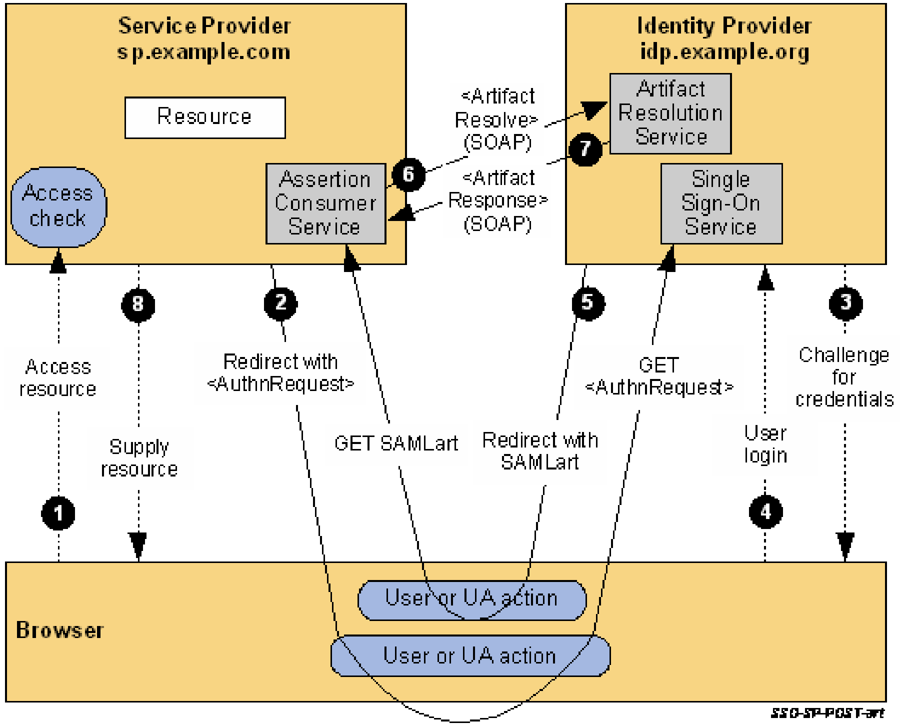
Source: https://developer.fourth.com/

Artifact Binding

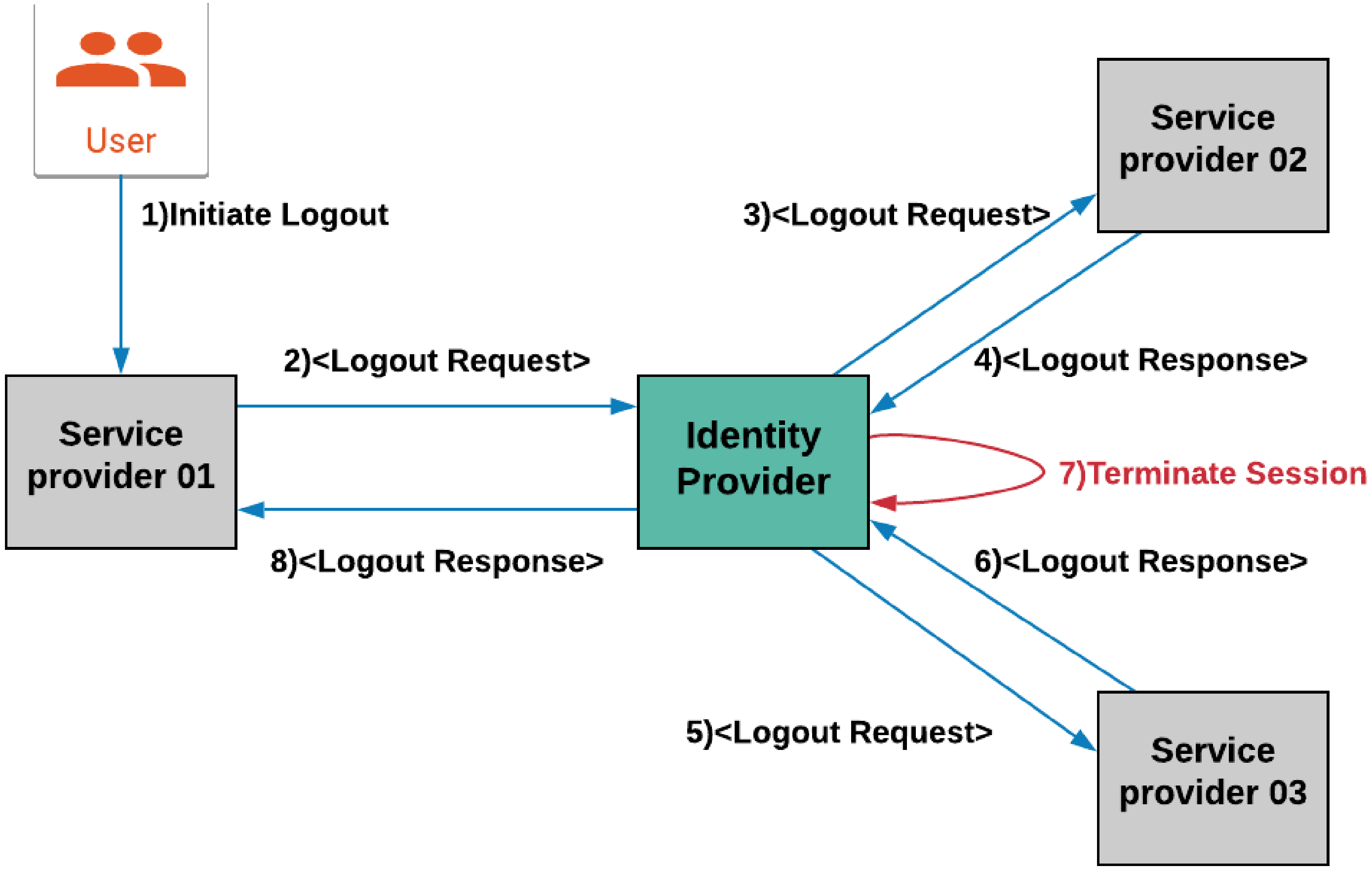
without



with



SAML2 Single Logout (SLO)



SAML attacks

- **Replay attack**
  - Valid SAML messages are intercepted and reused by an attacker to gain unauthorised access
  - Countermeasure: use tokens with a limited lifespan; assertions must be invalidated as soon as they are used
- **Assertion manipulation**
  - The absence of a digital signature means that the assertion’s integrity and authenticity cannot be verified
  - Allowing an attacker to modify the assertion’s attributes, such as roles or privileges
  - Countermeasure: all SAML assertions are digitally signed by the IdP; SPs must systematically check the signature of each assertion to ensure that it has not been altered in transit.

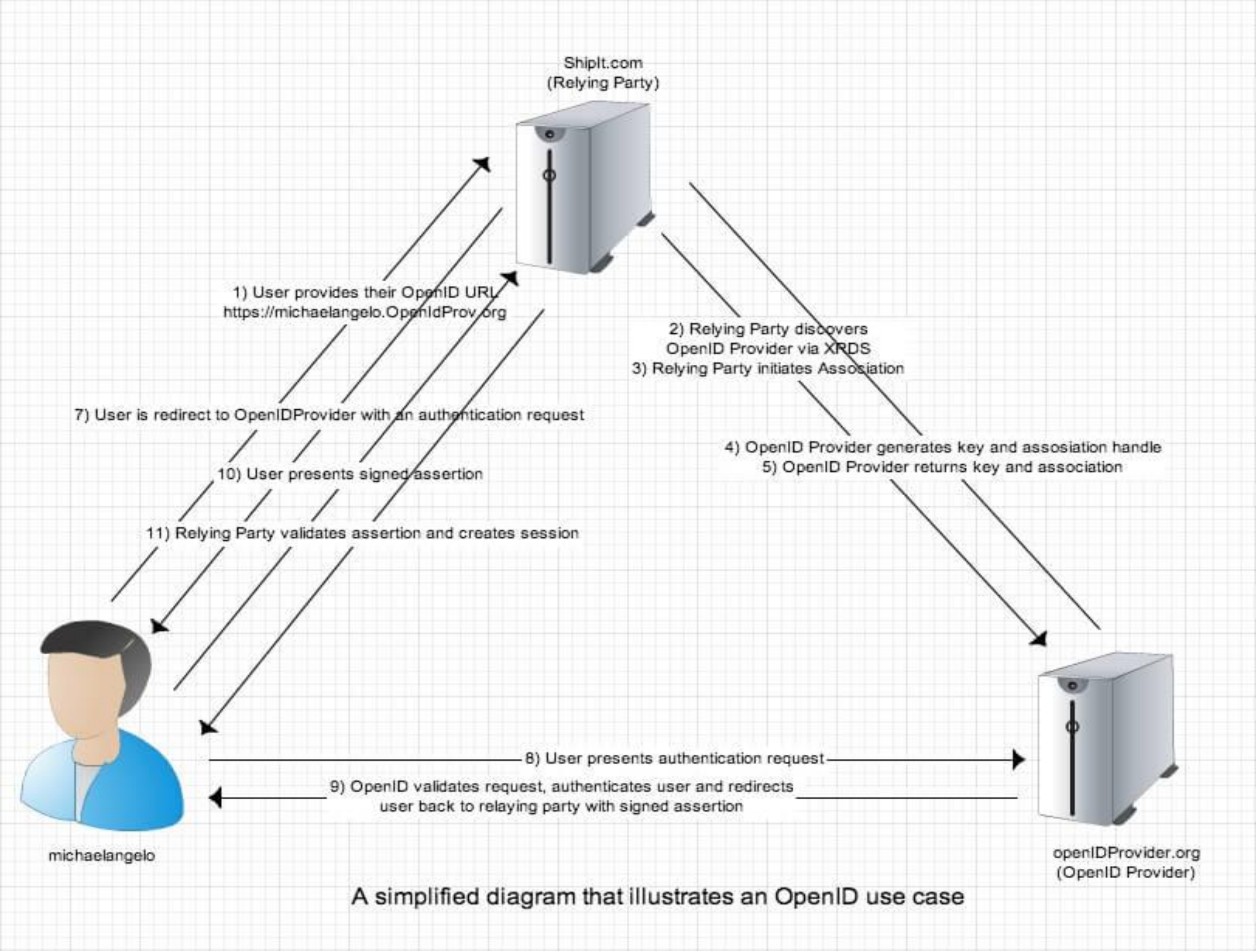
SAML attacks

- **XXE (XML External Entity)**
  - Based on exploitation of vulnerabilities in the processing of XML documents by misconfigured parsers
  - Read sensitive files on the server, make network requests from the server and execute remote commands on the remote server
  - Countermeasure: avoid custom parser configurations (e.g., disallowing the Doctype declaration completely)
- **Email forwarding attack**
  - Exploits attribute validation flaws in SAML assertions
  - If the system does not check that the email in the SAML assertion actually belongs to the tenant’s domain, an attacker can gain unauthorised access by using a valid email from another tenant.
  - Countermeasure: Crucial to test the possibility of stealing an account from another tenant.

OpenID

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

https://www.youtube.com/watch?v=A7GVeqFvqFM



1) User provides their OpenID URL
https://michaelangelo.OpenIdProv.org

2) Relying Party discovers OpenID Provider via XRDS
3) Relying Party initiates Assosiation

4) OpenID Provider generates key and assosiation handle
5) OpenID Provider returns key and association

7) User is redirect to OpenIDProvider with an authentication request

8) User presents authentication request

9) OpenID validates request, authenticates user and redirects user back to relaying party with signed assertion

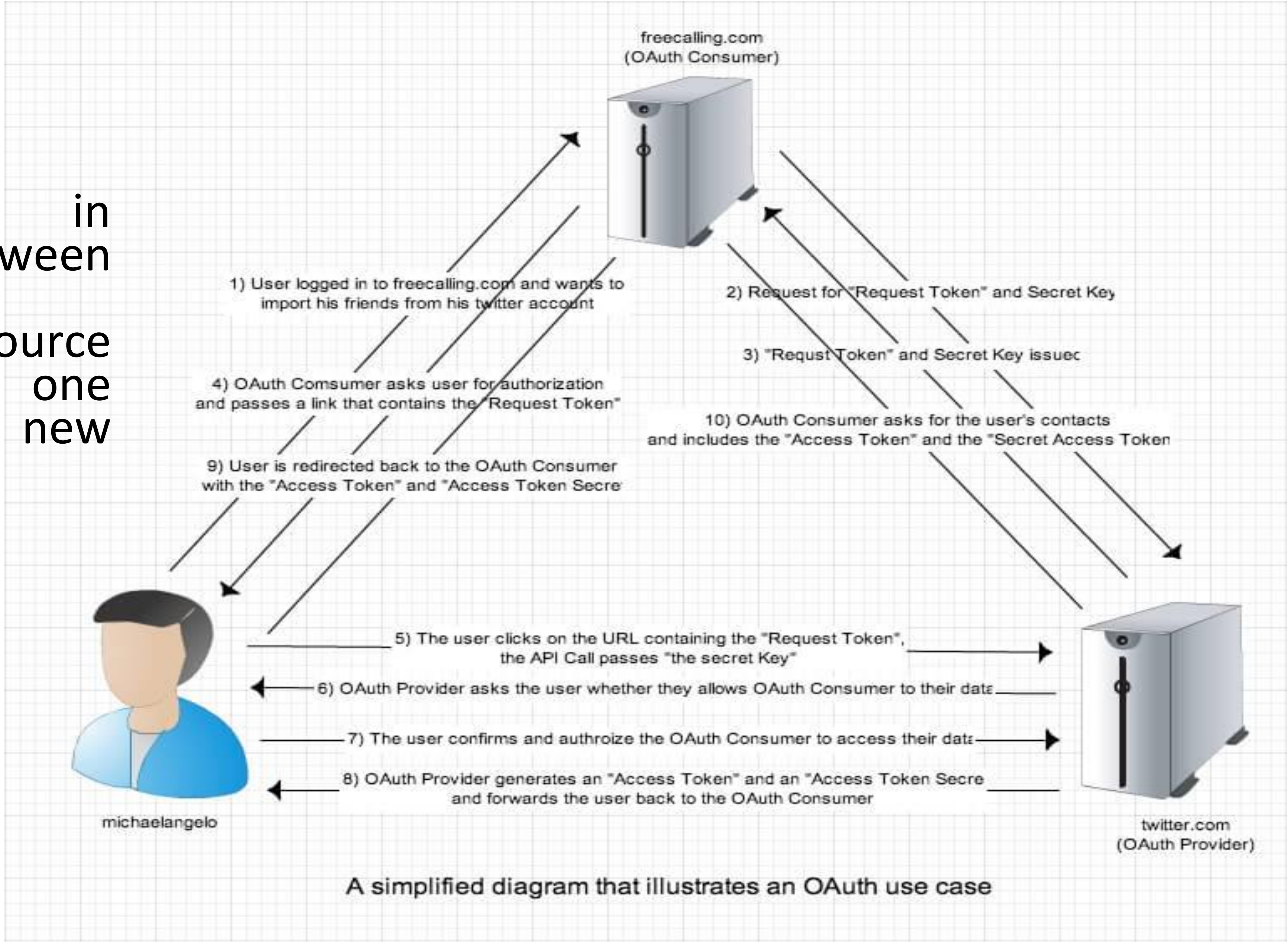
10) User presents signed assertion

11) Relying Party validates assertion and creates session

A simplified diagram that illustrates an OpenID use case

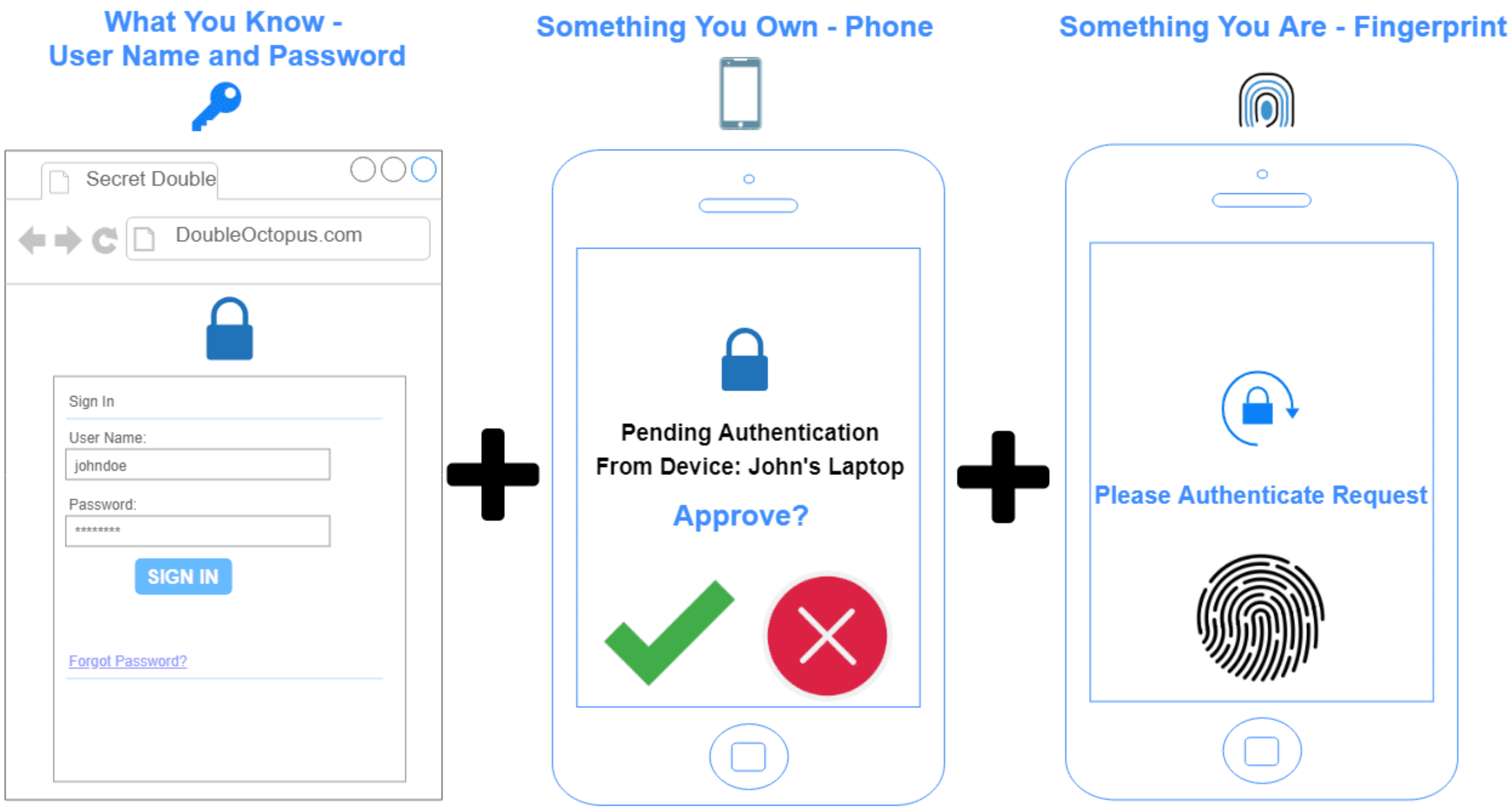
OAuth

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


freecalling.com
(OAuth Consumer)
1) User logged in to freecalling.com and wants to import his friends from his twitter account
2) Request for "Request Token" and Secret Key
3) "Requst Token" and Secret Key issued
4) OAuth Comsumer asks user for authorization and passes a link that contains the "Request Token"
5) The user clicks on the URL containing the "Request Token", the API Call passes "the secret Key"
6) OAuth Provider asks the user whether they allows OAuth Consumer to their data
7) The user confirms and authroize the OAuth Consumer to access their data
8) OAuth Provider generates an "Access Token" and an "Access Token Secret and forwards the user back to the OAuth Consumer
9) User is redirected back to the OAuth Consumer with the "Access Token" and "Access Token Secret
10) OAuth Consumer asks for the user's contacts and includes the "Access Token" and the "Secret Access Token
michaelangelo
twitter.com
(OAuth Provider)

A simplified diagram that illustrates an OAuth use case

Multi-Factor Authentication (MFA)



What You Know -
User Name and Password

Secret Double

DoubleOctopus.com

Sign In

User Name: johndoe

Password: ********

SIGN IN

Forgot Password?

+

Something You Own - Phone

Pending Authentication
From Device: John's Laptop

Approve?

+

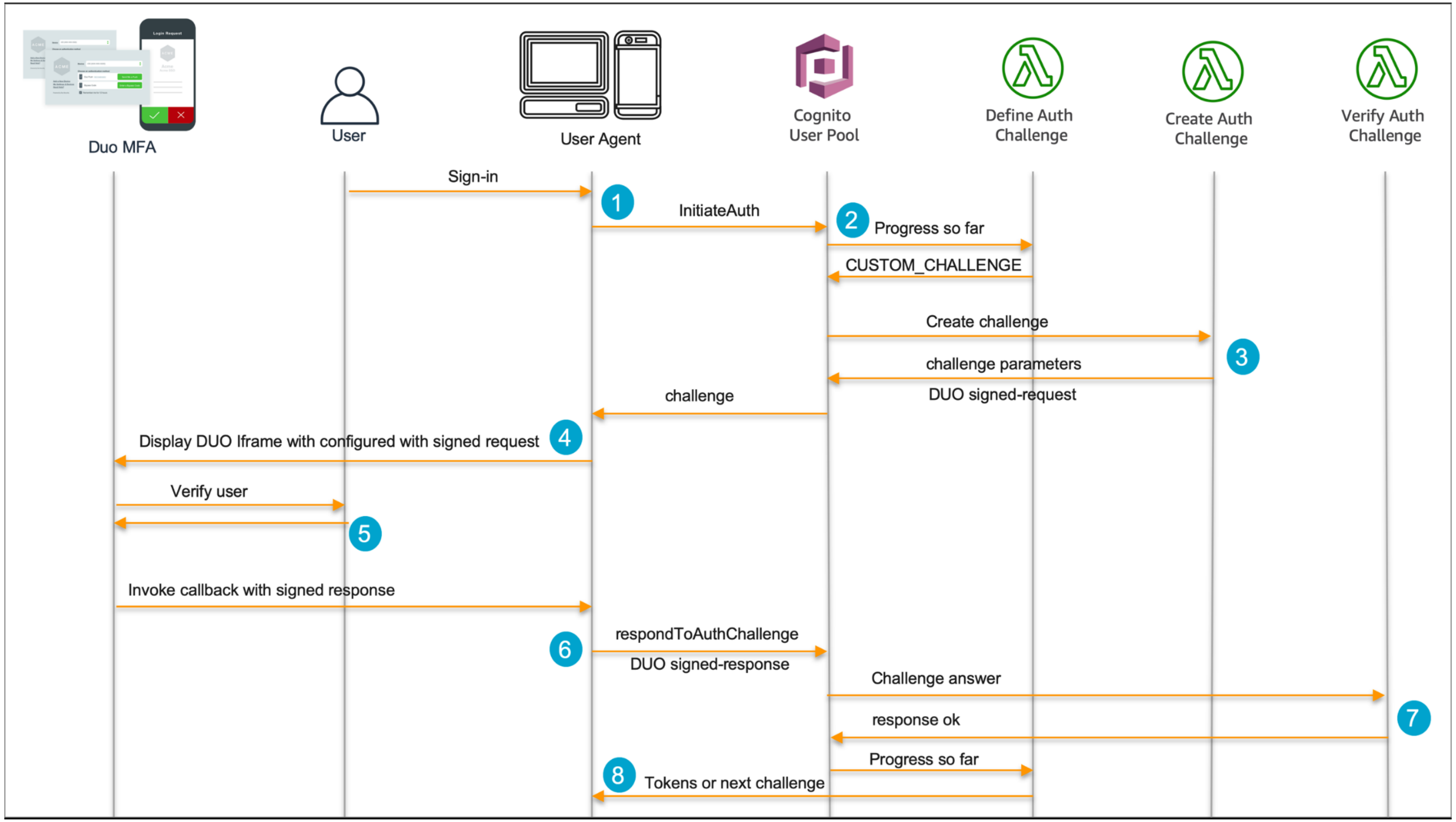
Something You Are - Fingerprint

Please Authenticate Request

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

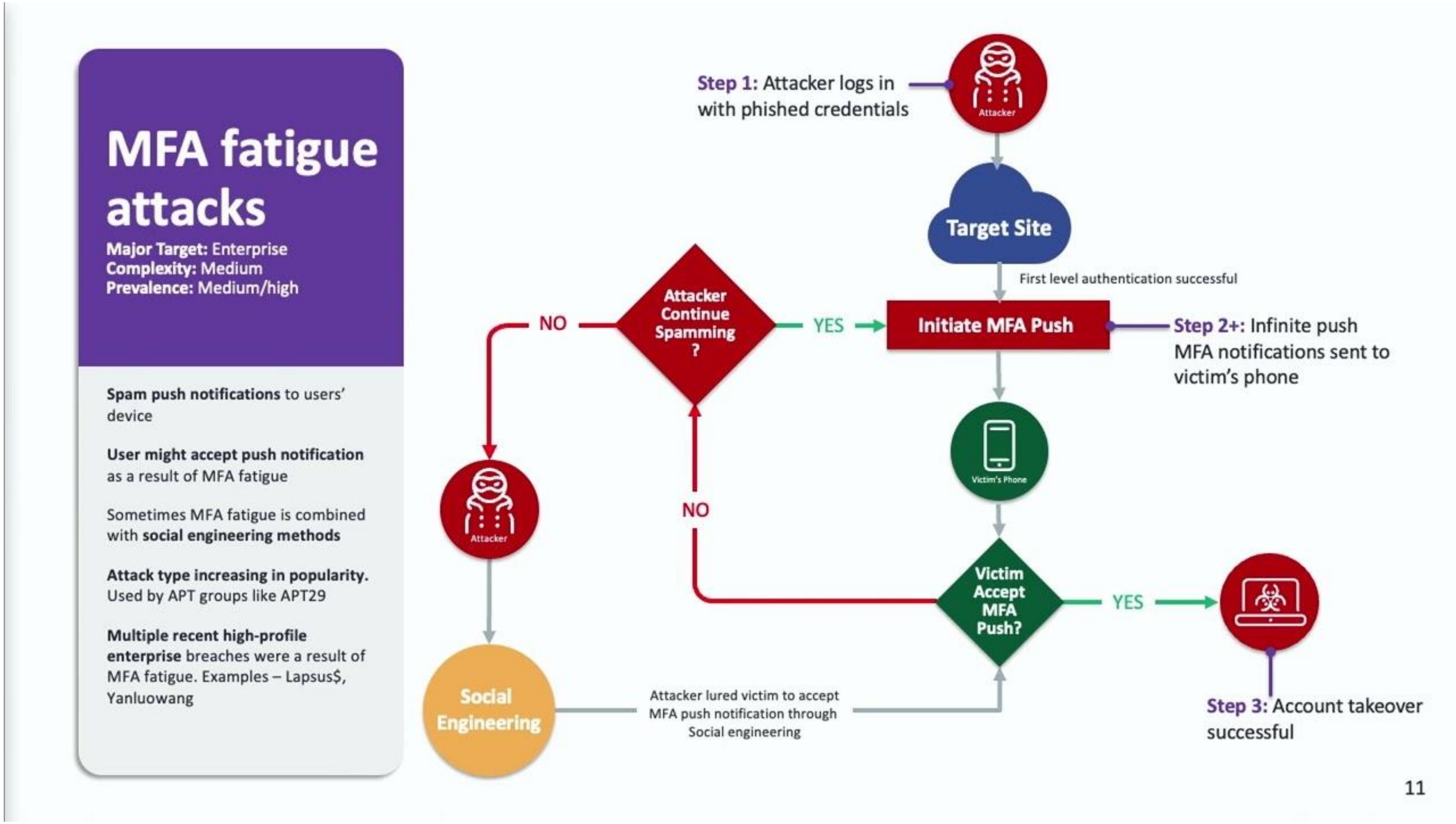
SECRET
DOUBLE
OCTOPUS

Multi-Factor Authentication (MFA)



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

MFA fatigue attacks (aka MFA bombing)



MFA fatigue attacks

Major Target: Enterprise
Complexity: Medium
Prevalence: Medium/high

Spam push notifications to users' device

User might accept push notification as a result of MFA fatigue

Sometimes MFA fatigue is combined with **social engineering methods**

Attack type increasing in popularity. Used by APT groups like APT29

Multiple recent high-profile enterprise breaches were a result of MFA fatigue. Examples – Lapsus$, Yanluowang

Step 1: Attacker logs in with phished credentials

First level authentication successful

Step 2+: Infinite push MFA notifications sent to victim's phone

Attacker lured victim to accept MFA push notification through Social engineering

Step 3: Account takeover successful

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.

Additional References

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Document	Title	URL
SP 800-63-3	Digital Identity Guidelines	https://doi.org/10.6028/NIST.SP.800-63-3
SP 800-63A	Enrollment and Identity Proofing	https://doi.org/10.6028/NIST.SP.800-63a
SP 800-63B	Authentication and Lifecycle Management	https://doi.org/10.6028/NIST.SP.800-63b
SP 800-63C	Federation and Assertions	https://doi.org/10.6028/NIST.SP.800-63c

- 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
T5- Identity Management

marc.ruiz-ramirez@upc.edu