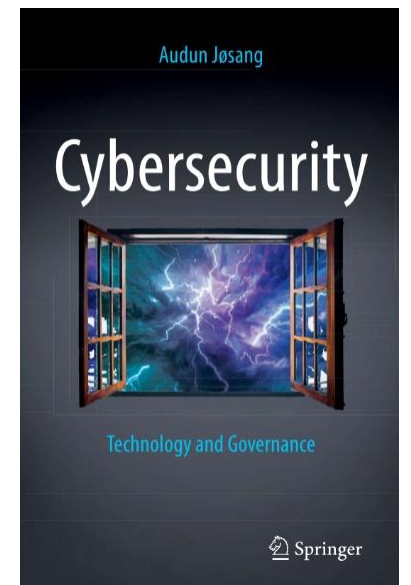


Chapter 9: Identity and Access Management

Cybersecurity: Technology and Governance

Audun Jøsang,

1st Edition, Springer Nature, 2024.



Overview

- What is IAM (Identity and Access Management)
- What is identity
- The identity management silo model
- Federated identity management model
 - User authentication as a service
- Access control

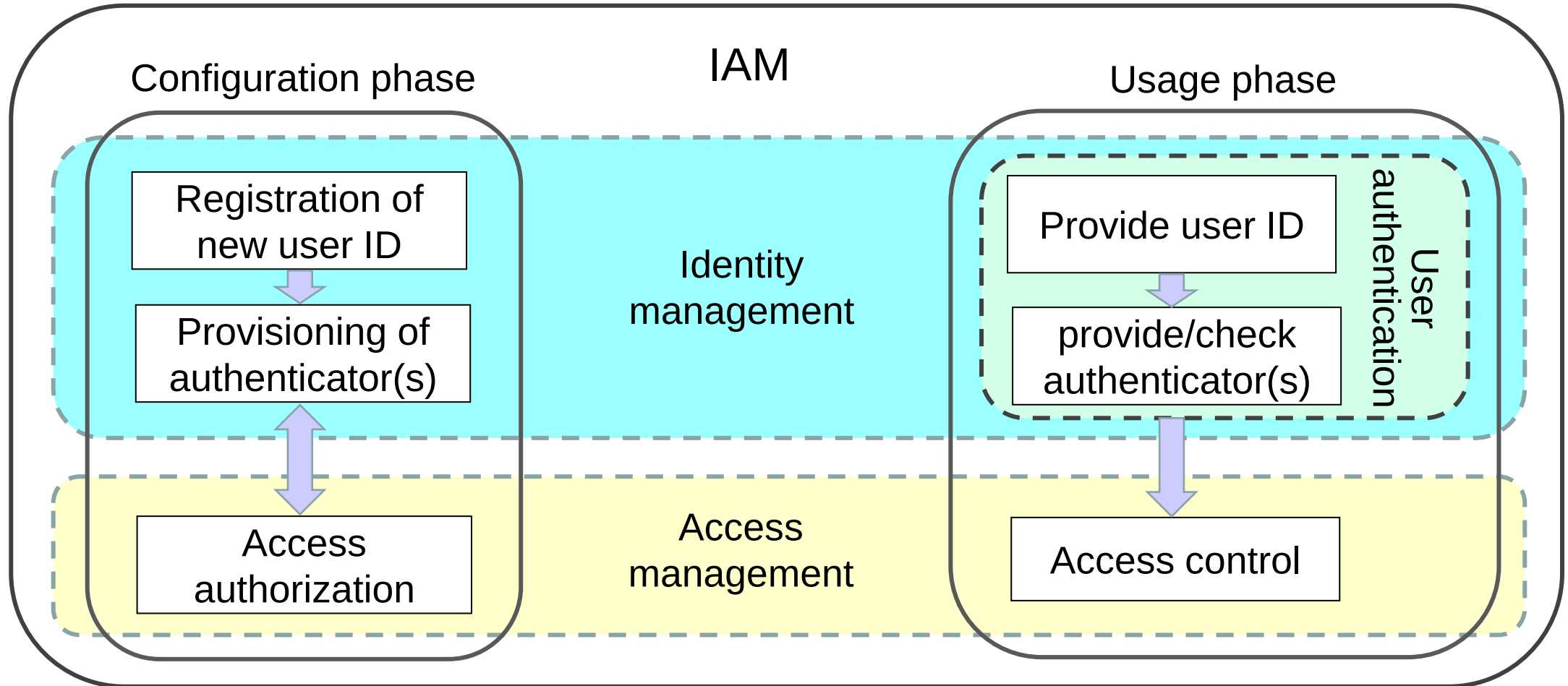
IAM - definition

- Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.

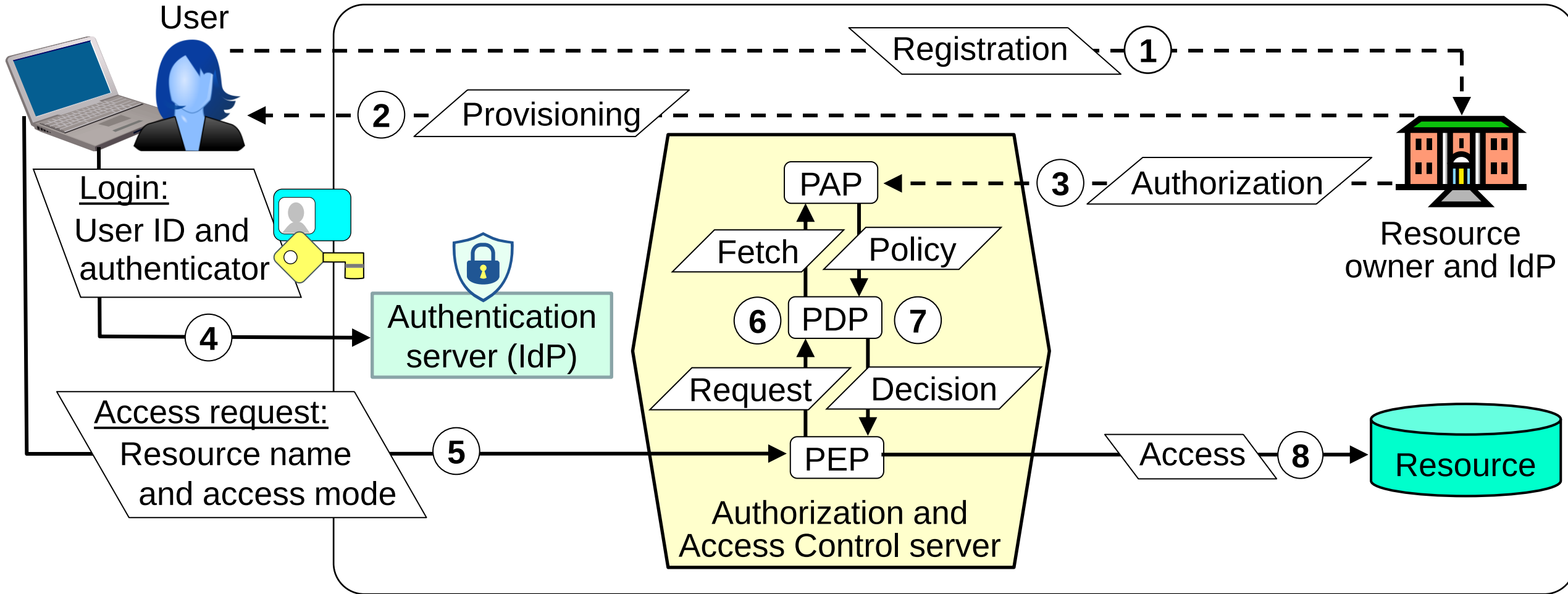
Gartner, security glossary

<https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam>

Identity and Access Management



IAM scenario

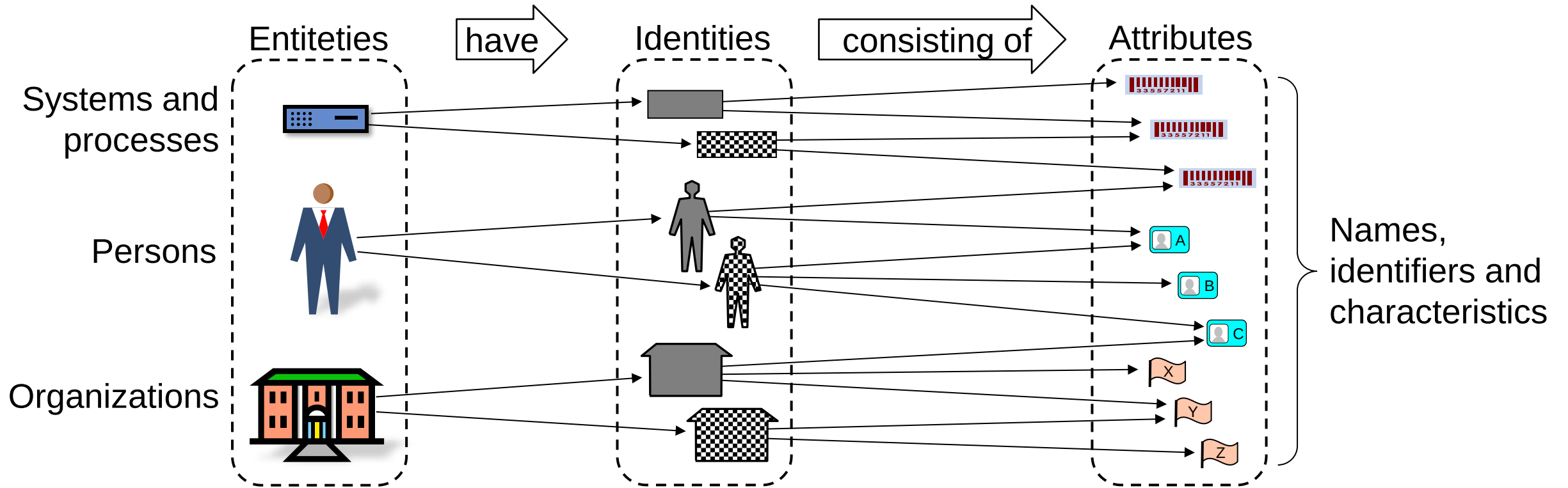


PAP: Policy Administration Point
PDP: Policy Decision Point

PEP: Policy Enforcement Point
IdP: Identity Provider

--> Configuration phase
--> Usage phase

Identity as a concept



Concepts related to identity

- Entity
 - A person, organization, agent, system, session, process, etc.
- Identity
 - A set of names/attributes for the entity in a specific domain
 - An entity can have identities in multiple domains
 - An entity can have multiple identities in the same domain
- Digital identity
 - Digital representation of names/attributes in a way that is suitable for digital processing
- The names and attributes of entities can be
 - Unambiguous or ambiguous within a domain
 - short-term or permanent;
 - self-defined or defined by authority,
 - processed by humans and/or computers
 - and so forth.
- An identifier is a name that is unique within a namespace

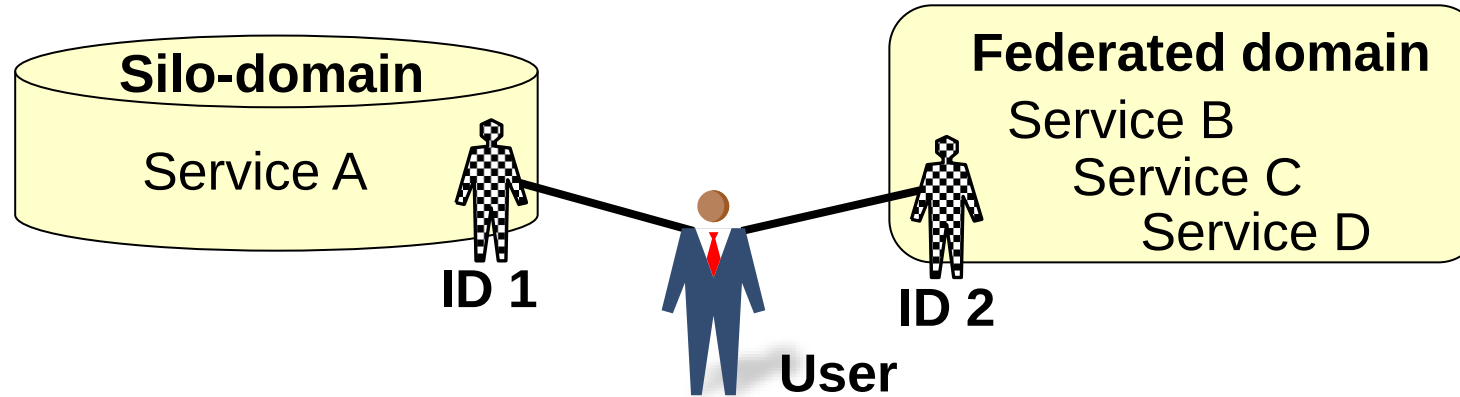
Identity – creation – registration



- Etymology (original meaning of words)
 - "Identity" = "the same one as last time".
- Authentication requires that an identity has been registered
- An entity cannot be authenticated without identity
 - because there is no "last time"
 - because the identity must first be created and registered
- Registration can take place in two ways:
 - Identity verification, new digital identity based on previous identity such as passport
 - creation of a new digital entity, e.g. a newborn baby, with an associated new identity

Identity domains

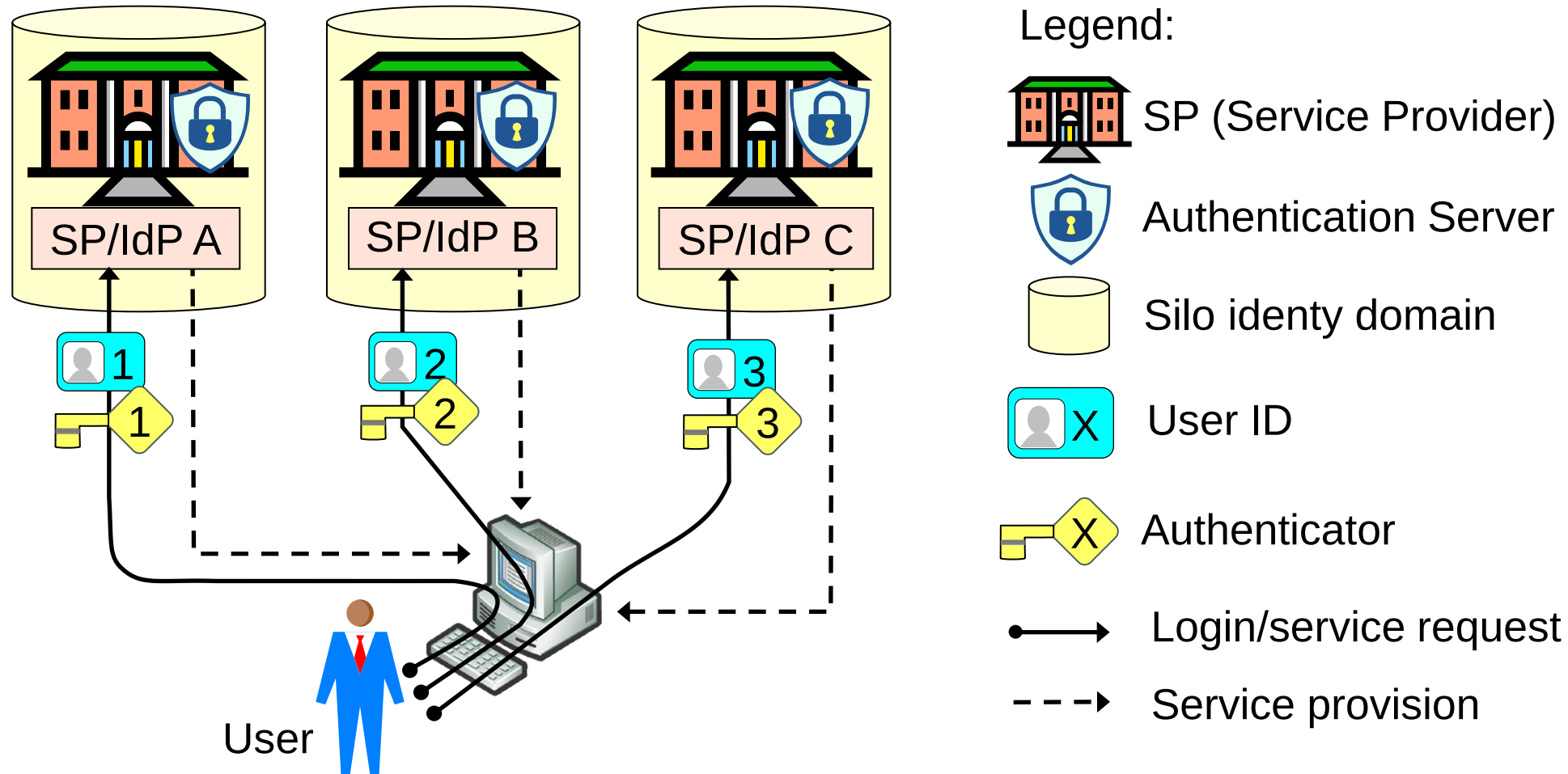
- An identity domain has a namespace with unique names
 - The same user can have separate identities in different domains
 - The same user normally has only one identity in a domain, but it is quite possible that the same user can have multiple identities in a domain.



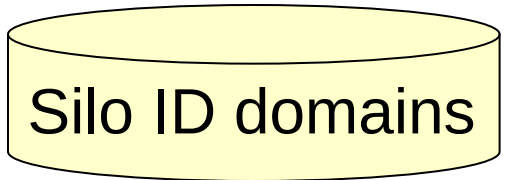
- Siloed domain with one authority, e.g. corporate network
- Federated identity domains
 - The identity domain can be used by many different service providers
 - Requires collaboration on identity policy between service providers

Silo identity management

Silo ID domains



Silo identity management



Silo ID domains

- SP (Service Provider) = IdP (Authentication Server):
 - SP controls the namespace and performs authentication
- Unique identifiers assigned to each user
- Advantages:
 - Easy to set up, low initial costs
 - Potentially a good basis for strong privacy
- Disadvantages:
 - Identity overload for users, poor usability, poor integration of services between providers
 - Low acceptance of new services with separate ID and authenticator
 - Users must provide the same information to many service providers
 - For Service Providers: Barrier to User Data Collection

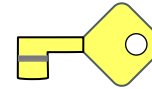
Roles in federated identity management

- User

- Has user ID and authenticator(s)
- Want to use the services of different SPs.



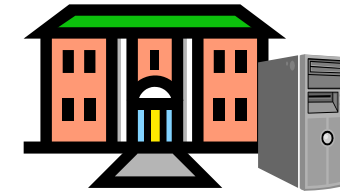
User ID



Authenticator

- Service Provider (SP), also called Relying Party

- Has a register of user IDs
- Have an agreement with one or more User Authentication IdPs



- Authentication server (IdP: Identity Provider)

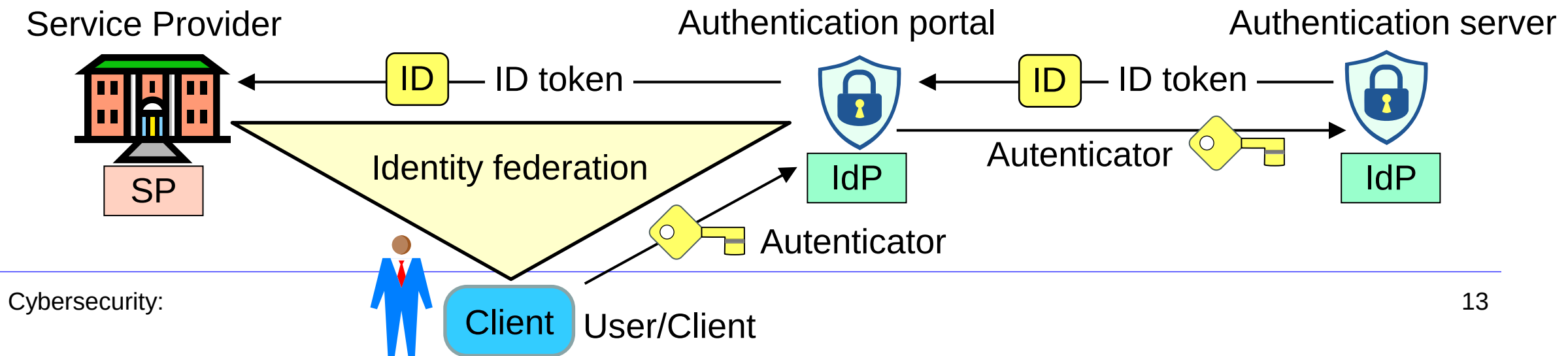
- Authentication portal

- Has an agreement with SPs
- Provides/sells user authentication as a service to SPs



Protocols/Standards for ID Federation

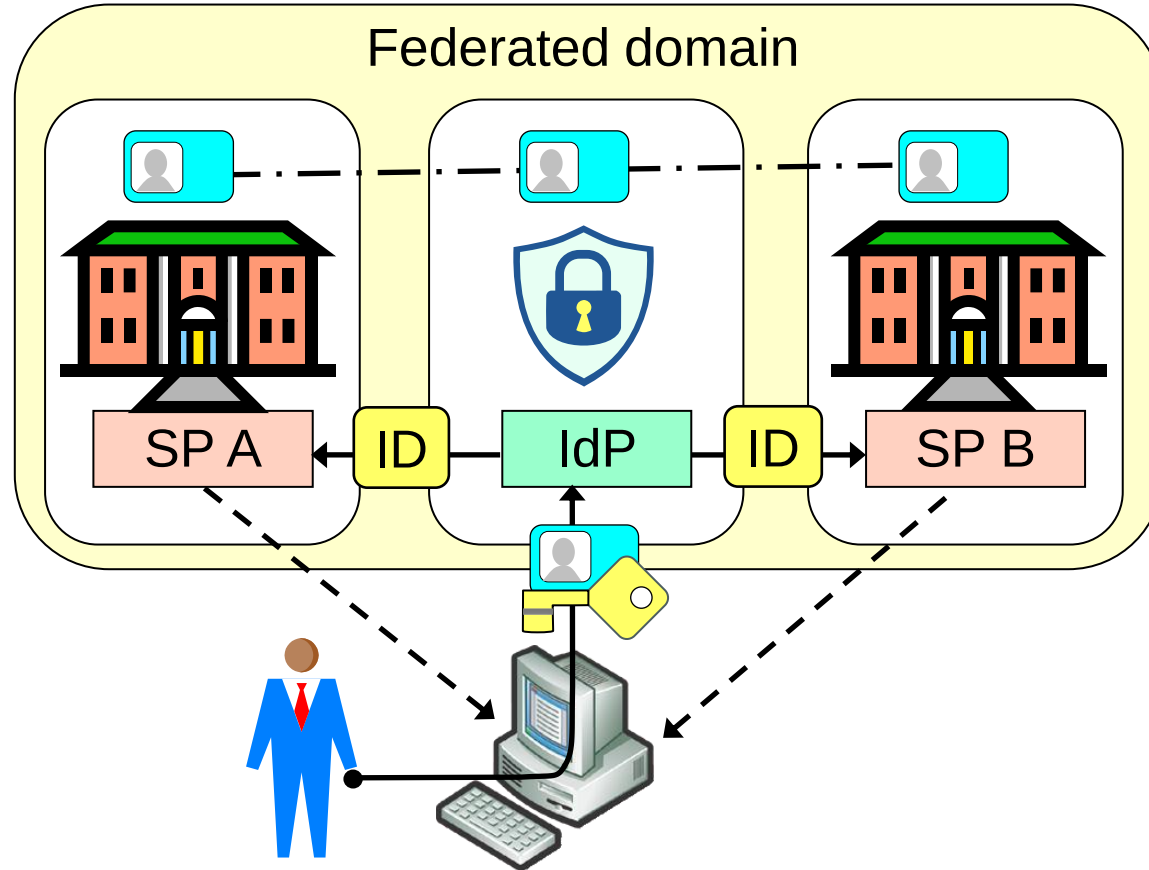
- Involving multiple entities
 - User/browser, IdP, SP, and sometimes a broker/authentication portal (e.g. ID-porten)
- The IdP authenticates the user, and sends digitally signed ID tokens to the SP.
- SP receives the ID token as proof that the user is authenticated.
- Standards:
 - OAuth (Open Authorization)
 - OIDC (OpenID Connect), which is based on OAuth
 - SAML (Security Assertions Markup Language),
 - SAML was previously a widespread standard for ID federation, but IdPs and SPs are switching to OIDC.



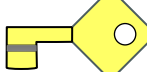
ID federation – advantages and disadvantages

- Advantages
 - Better usability
 - Allows SPs to focus on services, eliminating the need to deal with authenticators
 - Allows IdPs to gather usage pattern information for users
 - Scales well within a sector, provides good quality authentication
- Disadvantages
 - Technical and legal complexity
 - Trust requirements between actors
 - Each actor can potentially compromise security
 - Privacy issues,
 - Massive collection/exchange of data between SP and IdP is a threat to privacy
 - Limited scalability between different sectors/domains,
 - Constrained by political and economic constraints
 - A federated domain can become a new form of silo in relation to other domains

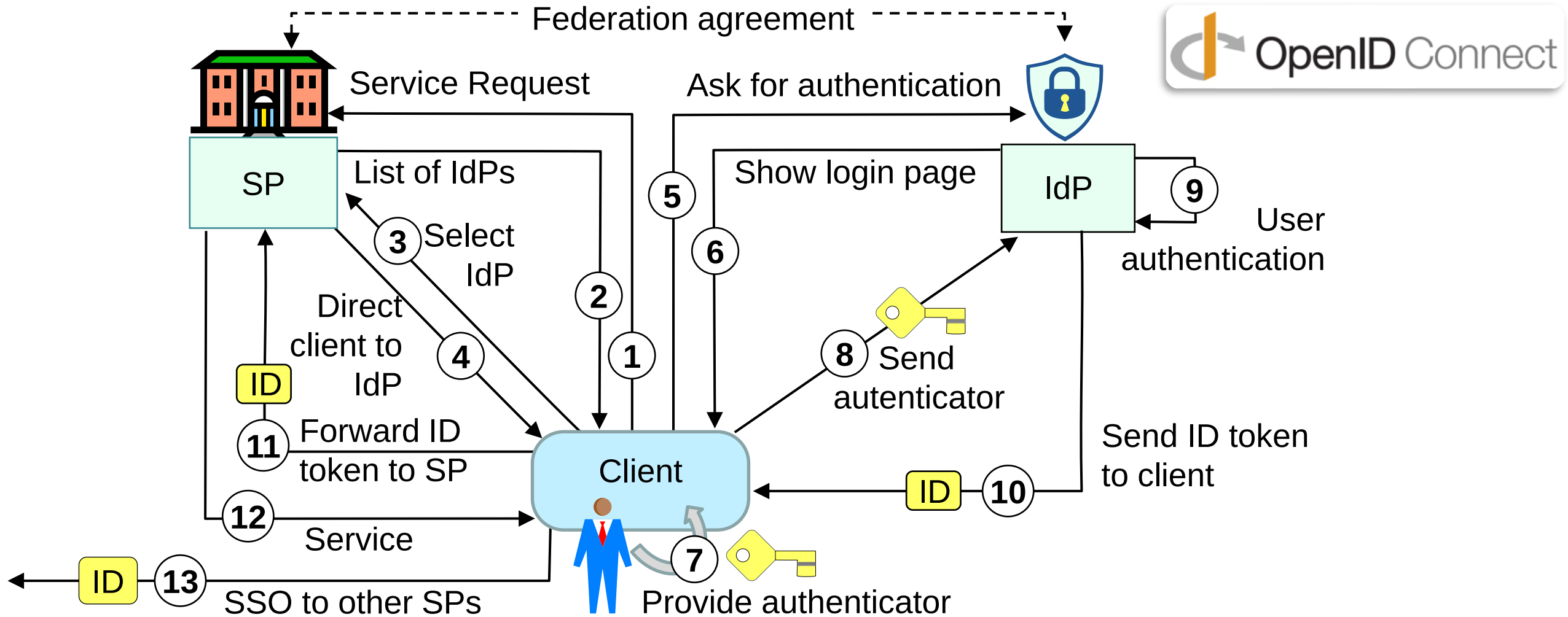
ID federation use-case



Legend:

-  SP (Service Provider)
-  IdP (Authentication Server)
-  Identity domain
-  User ID
-  Authenticator
-  ID token/security token
-  Login
-  Service
-  Federated ID

OIDC federated authentication



OAuth (Open Authorization)



- OIDC is based on the OAuth 2.0 specification
 - SPs establish federation agreements with IdPs through OAuth
 - e.g. Airbnb (SP) with facebook (IdP)

- OIDC (OpenID Connect) is used in  e-Pramaan
-  Nigerian eID



Australia's
Digital ID
System

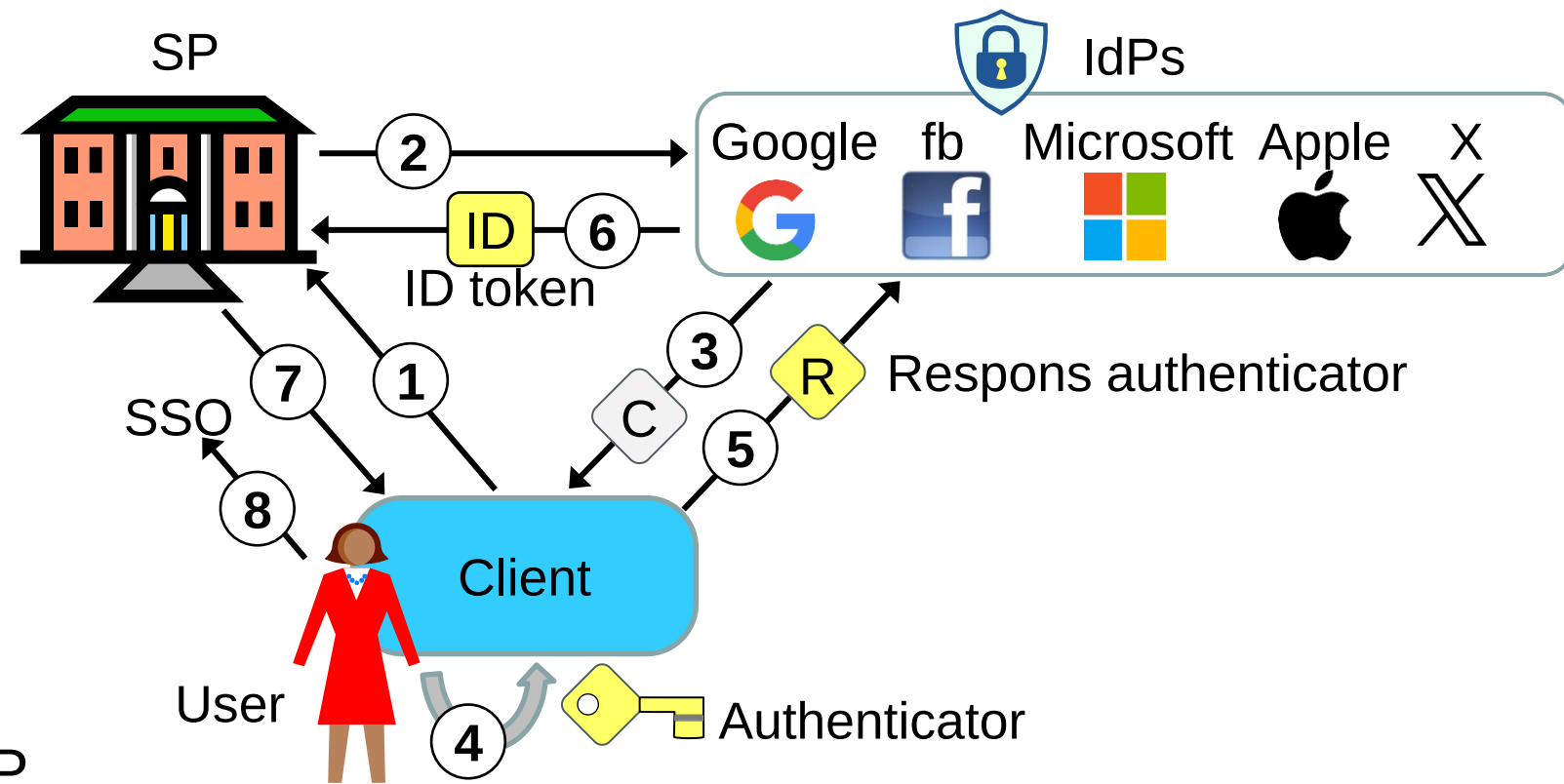


- For example, IAM for the Indian e-Government services is based on OIDC
 - Every citizen has an Aadhaar number
 - The Aadhaar number is used to access various services

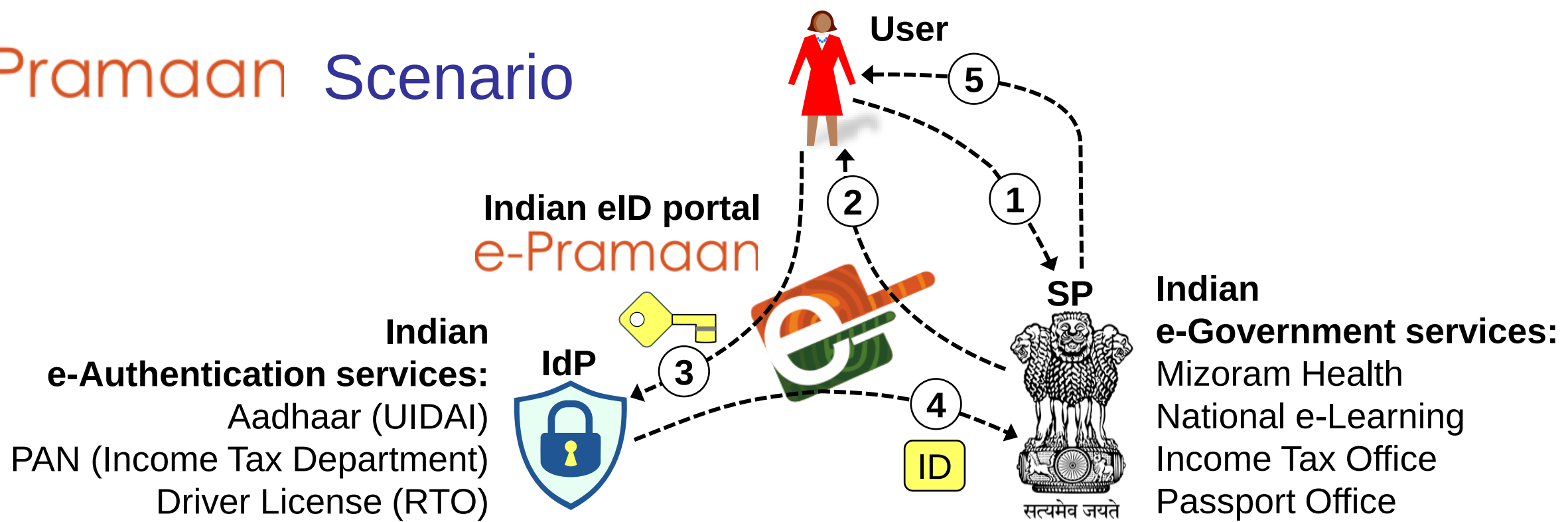
Identity federation and Single-Sign-On (SSO) with google, facebook, microsoft, apple, and X

Simplified OIDC scenario

1. User requests service
2. Redirect browser to IdP
3. Present login page from IdP
4. User provides ID and authenticator(s)
5. The user ID and authenticator are sent to the IdP who authenticates the user
6. The ID token is sent to SP (actually via browser)
7. SP provides service to user
8. The client has SSO (do not need to authenticate) to all SPs that use the same IdP



e-Pramaan Scenario



Simplified e-Pramaan scenario

1. The user requests access to a service
2. The SP asks the user to select the IdP for authentication.

3. The user provides name/identifier and authenticator(s) in the login window from the IdP.
4. The IdP authenticates the user, and sends ID tokens and user attributes to SP.
5. The SP checks security ticket and user attributes, and provides services in accordance with policy.

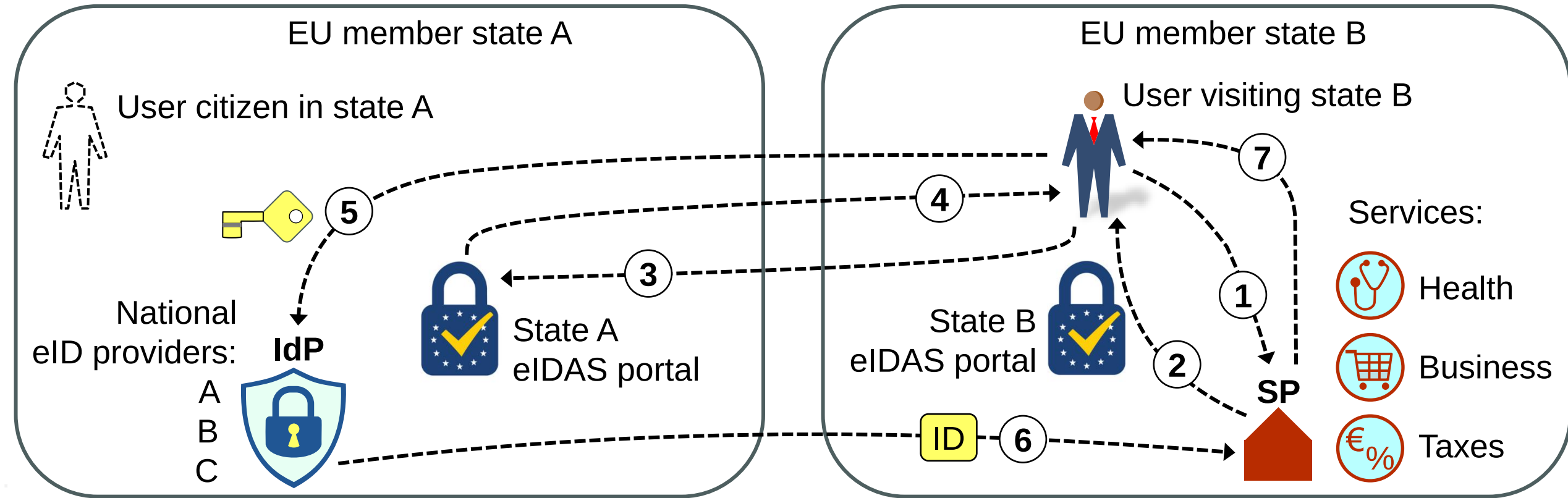
Identity federation – categories

Federation category	Centralized identity namespace	Distributed identity namespace
Centralized authentication	German eID Nigerian eID   Singapore singpass 	Norwegian education  
Distributed authentication	Indian e-Pramaan Norwegian ID portal  	Google fb Microsoft Apple X      European eIDAS Australia's Digital ID System  

Federated identity management - Examples

- German eID is centralized
 - BSI both manages the namespace and performs authentication
- Aadhaar (India) is centralized
 - Aadhaar both manages the namespace and performs authentication
- Eduroam has distributed namespaces, but centralized authentication
 - Different actors each manage their own namespaces
 - A single user can only be authenticated by the home institution, which is thus centralized
- Big-Tech Id providers for authentication and access control
 - ID federations on the internet have distributed namespaces and distributed authentication
 - Users' identities (which are common email addresses) are managed distributed
 - user can select different IdPs for authentication, which are thus deployed
- Secure European e-Identity
 - The EU ID federation is still work-in-progress. Will have distributed namespaces and distributed authentication.

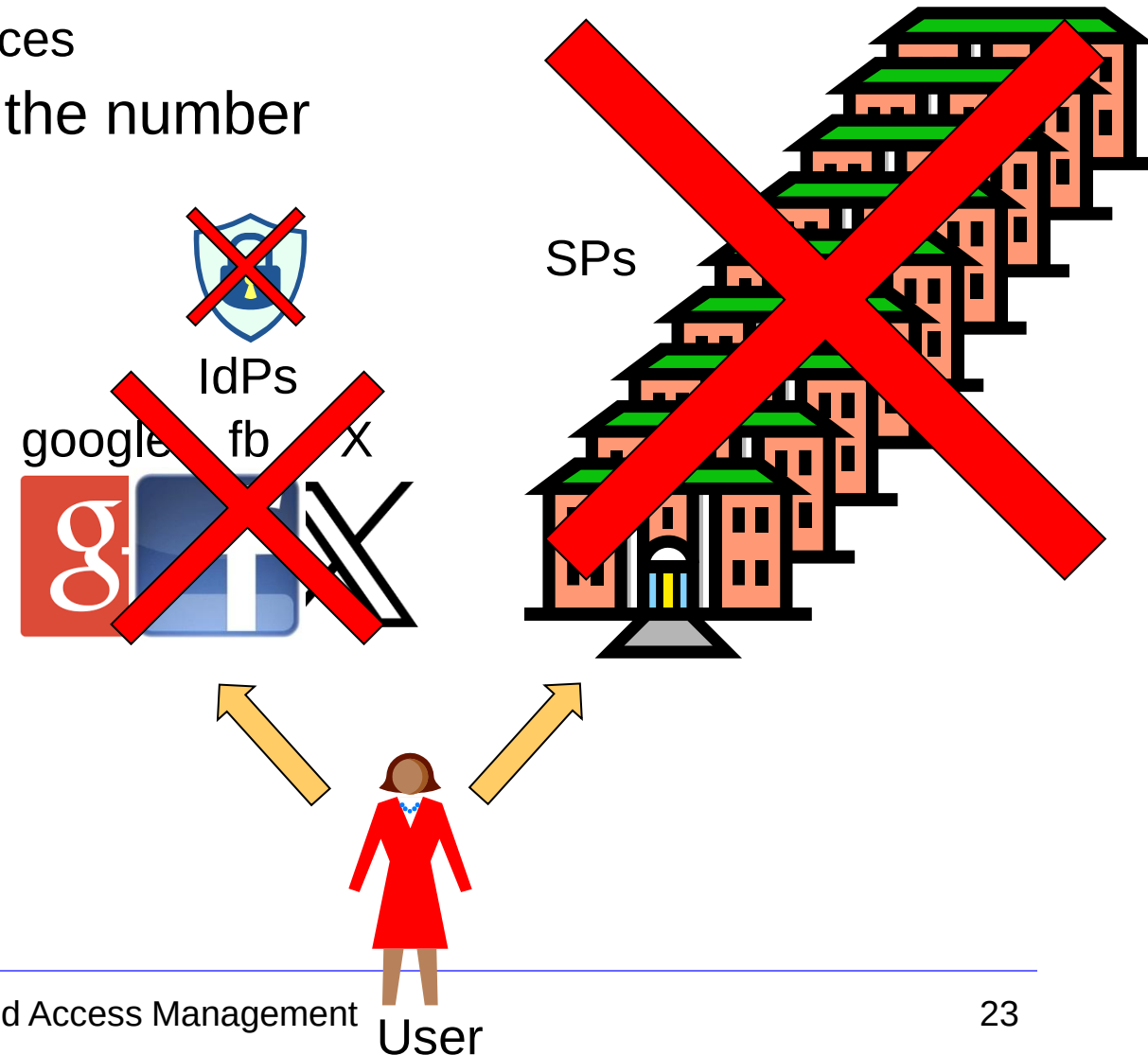
Scenario for European eID



- The EU requires eID providers (IdP for eGovernment) to be state-owned/controlle

IdP dependency

- Facebook fell out for 6 hours on October 4, 2021
 - Millions of users could not log in to online services
- The number of IdPs is very low relative to the number of SPs
- IdP dependency is a problem
- Need for alternative login



Access Control

Models and methods



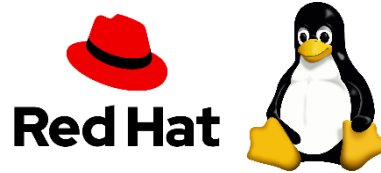
Access control models

- Purpose
 - *How should one define which subjects (users) should have access to which objects (resources) with which access mode (read, write, execute)?*
- Three classic models
 - Discretionary Access Control (DAC)
 - Name-based access control
 - Mandatory Access Control (MAC)
 - Label-based access control
 - Role-Based Access Control (RBAC)
- Modern and general model of access control:
 - Attribute-Based Access Control (ABAC)
 - Generalization of DAC, MAC, and RBAC

DAC – Discretionary Access Control

(Name-based access control)

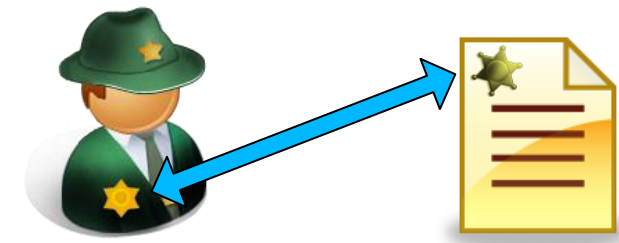
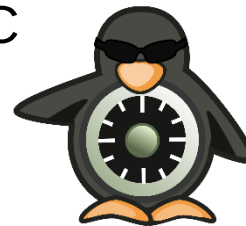
- Access authorization is specified and enforced based on the users' (subject) name and the resource's (object) name.
- Implemented with ACLs (Access Control Lists) that specify which subjects are authorized to access which objects with which access modes
- Metadata for ACL can be stored in Subject Profile or Object Profile
- DAC is "discretionary" in the sense that the owner of the resource can, at their discretion, determine who is authorized for access, by specifying names in an ACL.
- DAC is a classic model that is used by, among others:
- Windows, Mac OS and Linux



		Object name	
		HR	Sales
Subject name	John	r , w	
	Mary		r , w

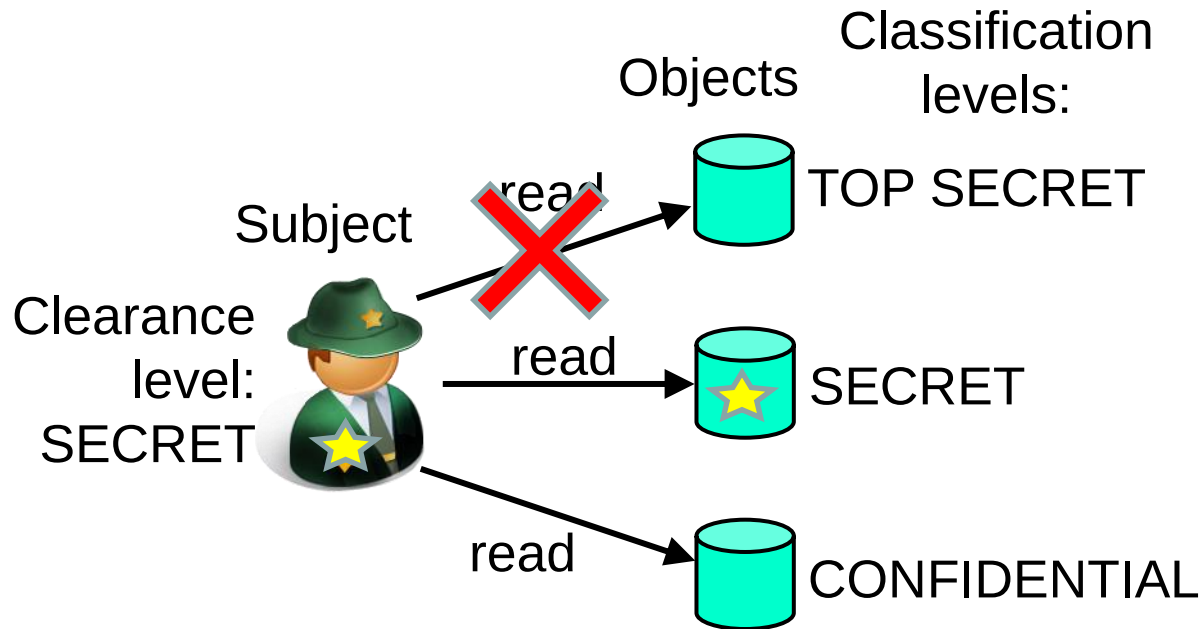
MAC – Mandatory Access Control (Label-based access control)

- Security labelling of subjects and objects
 - Security clearance for users (subjects)
 - Classification level of resources (objects)
- Access control is done by comparing labels on the user and the resource
- Users have a max clearance level, but can choose a lower level for each session.
- MAC is "mandatory" in the sense that access authorization to resources is determined by a "mandatory" (mandatory) security labeling policy, and is not determined by the user themselves
- Where is MAC used?
 - SE (Security Enhanced) Linux supports MAC
 - Some military systems use MAC

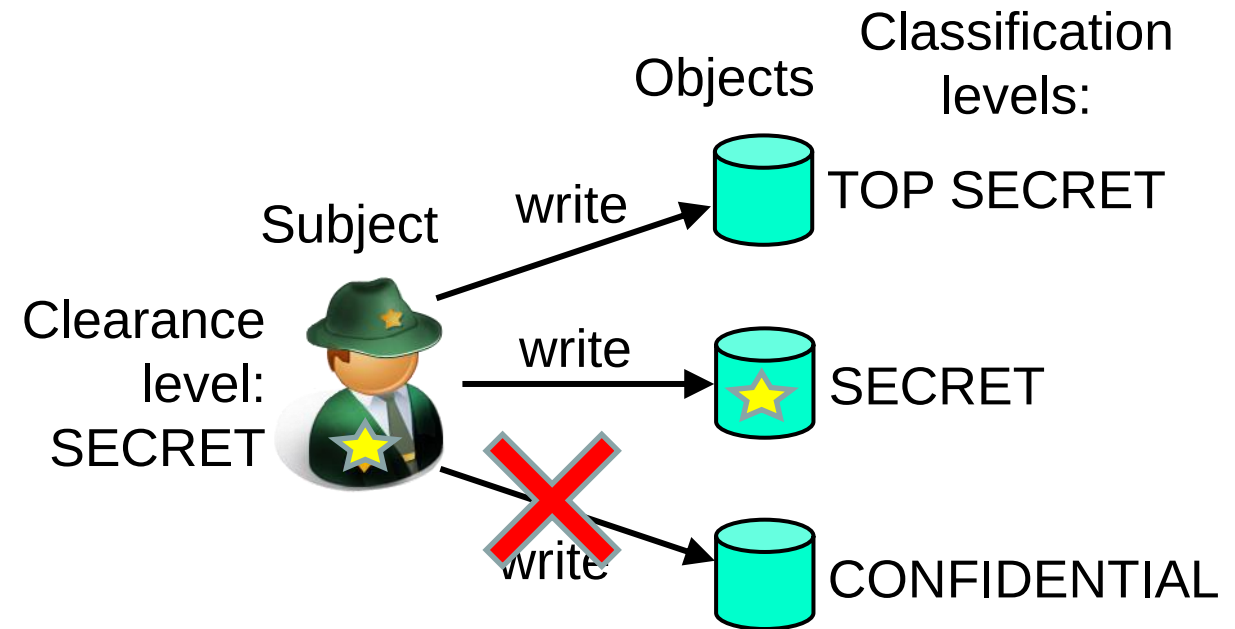


Bell-LaPadula (MAC model): No-Read-Up and No-Write-Down

No-Read-Up

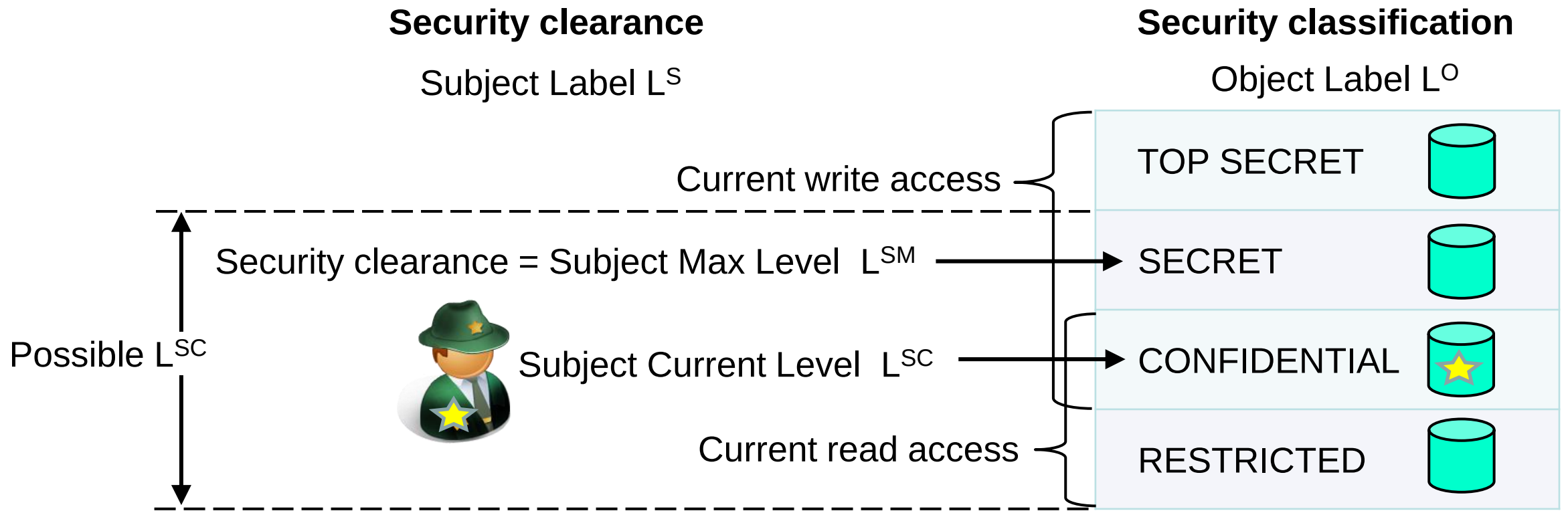


No-Write-Down



Bell-LaPadula (MAC Model) - Clearance level for a session

- To conveniently edit documents, a user (subject) can select an appropriate trust level for a specific session at the same or lower level than their actual trust level. The user can always edit documents with the same graduation as their current clearance level.

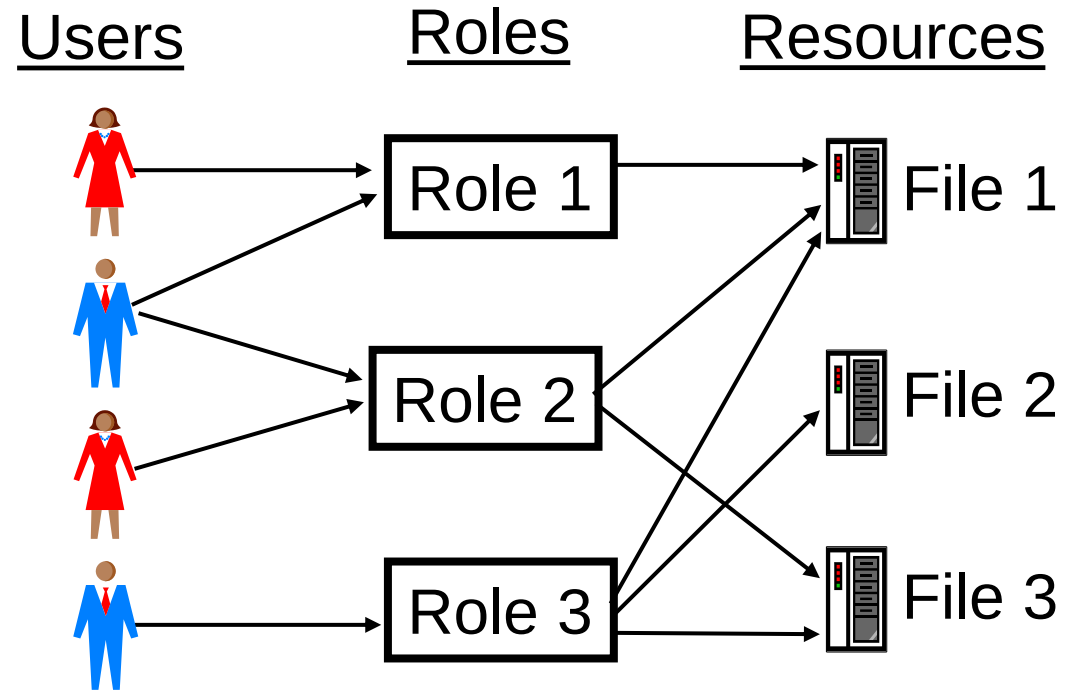


RBAC: Role Based Access Control

- A user has access to resources based on the user's work role.
- Roles are defined based on job functions.
- A user can be authorized to select different roles.
- Users usually only have one role at a time.
- The purpose of RBAC is to simplify the granting of authorisations.
- The problem with RBAC is role explosion, i.e. that very many different roles are defined.

RBAC – Role Based Access Control

Employees come and go frequently.
Roles are (perhaps) more stable.



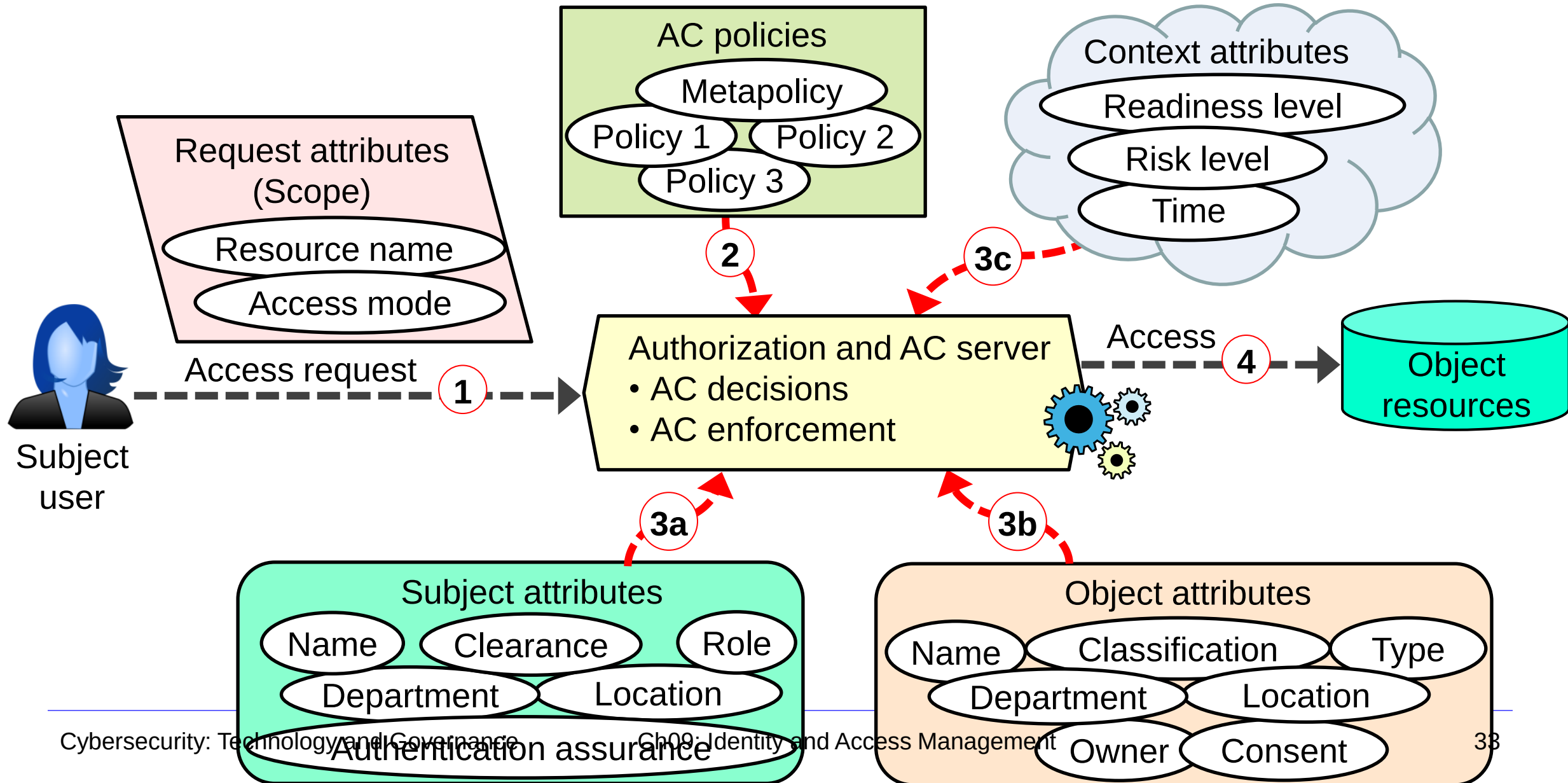
- RBAC can be configured as DAC or MAC

ABAC, XACML and JSON

ABAC = Attribute Based Access Control

- ABAC specifies access authorizations and enforces access through policies combined with attributes. Policies can use any type of attribute (user attribute, resource attribute, context attribute, etc.).
- ABAC attributes and policies can be expressed in different ways
 - JSON (JavaScript Object Notation) Schema brukes i implementeringer basert på OAUTH og OIDC.
 - XACML er XML-basert (Extensible Markup Language) og brukes i implementeringer basert på SAML (Security Assertion Markup Language).
- Both languages can be used to define how the system should make access decisions according to the rules defined in policies.

ABAC – Attribute-Based Access Control



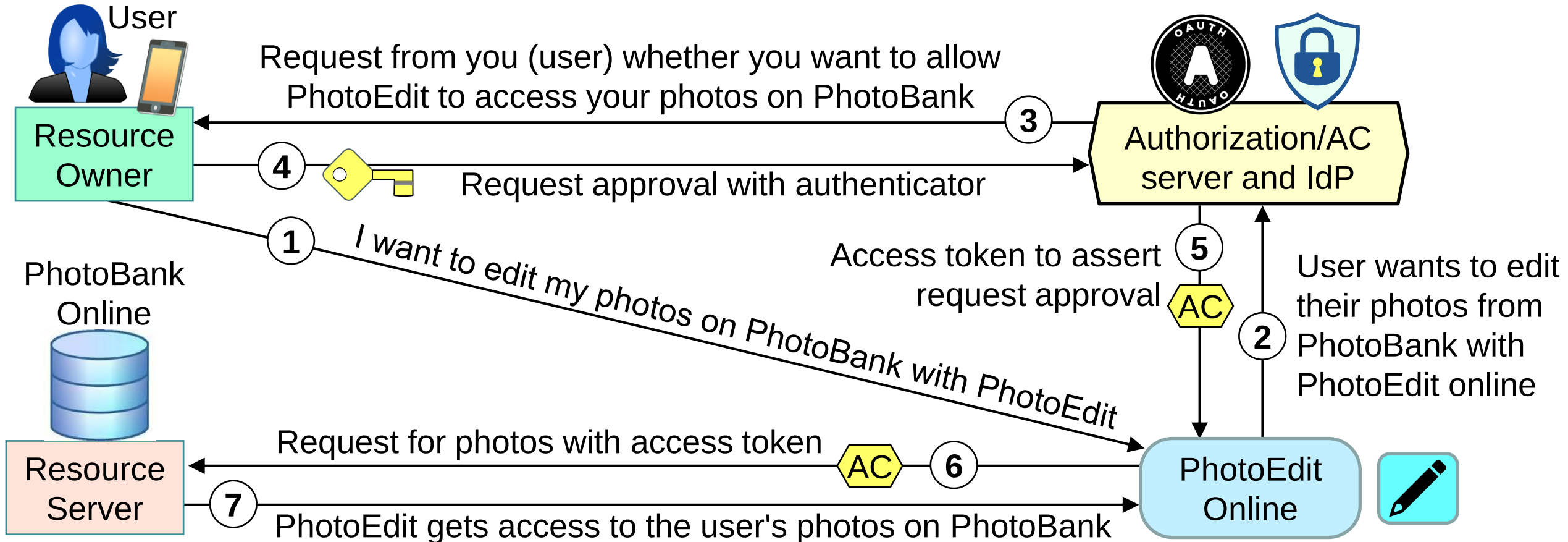
Distributed access control with OAuth



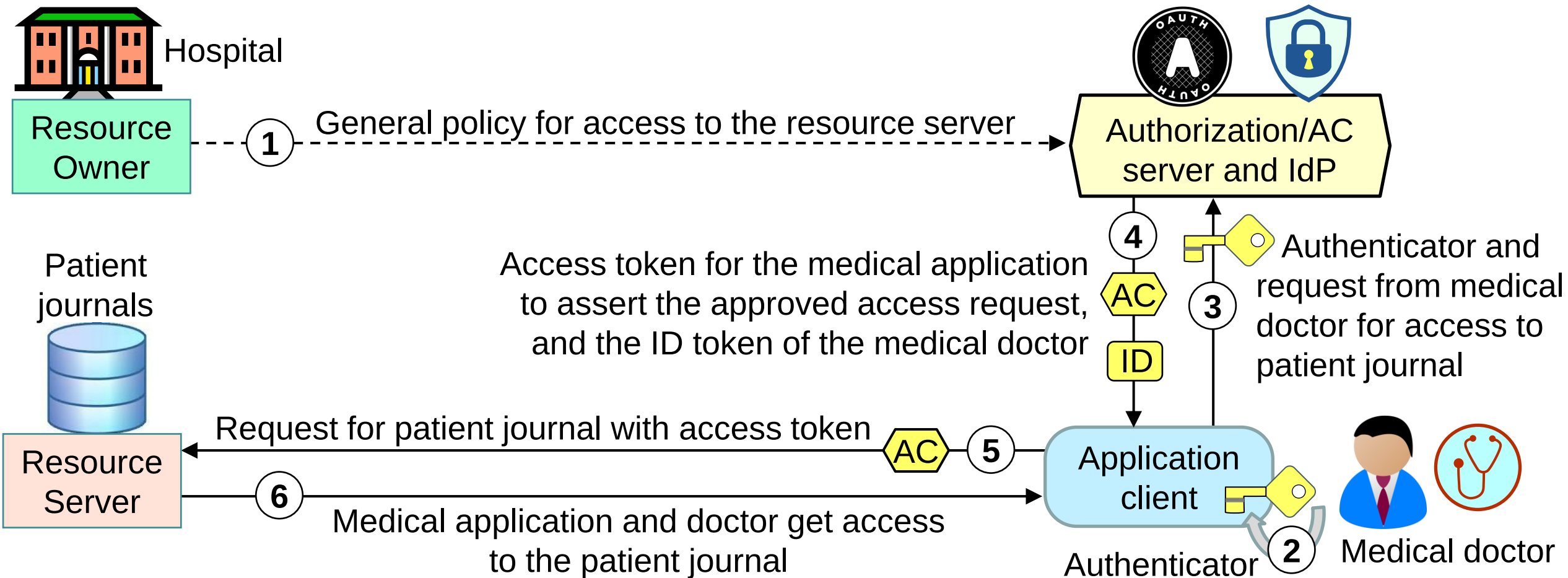
- In modern applications, the resource owner and resource server are often separate physical, logical, and legal entities.
- It is often desirable that access control (access decision) is done by different entities, depending on the architecture.
- OAuth (Open Authorization) is a standard for defining various architectures for access authorization and access control.
- OAuth includes, and is used in conjunction with, Open ID Connect (OIDC).



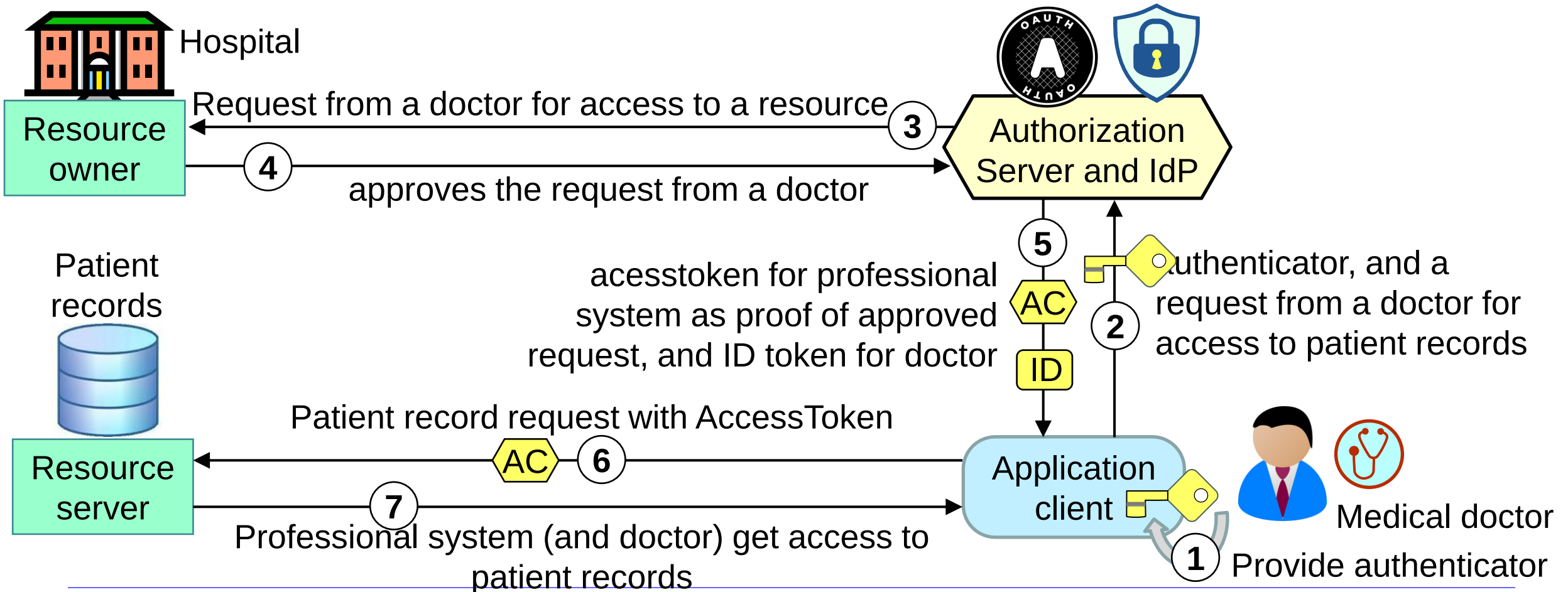
OAuth for Distributed Access Control on the Internet



Access management for collaboration in the public health sector with general access policy



Access management for collaboration in the public health sector with specific access policy



End of presentation

