Access Control and Authorisation (2)

Budi Arief

b.arief@kent.ac.uk

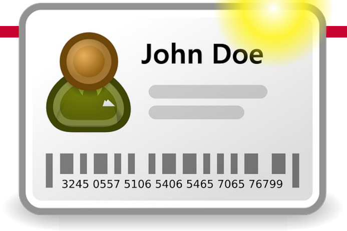
Based on slides by Shujun Li

Outline

- Identity Management
- Summary

Week 17

Authentication: Entity vs Identity

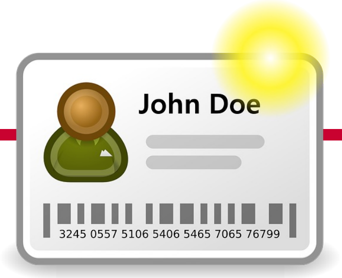


- Entity vs Identity: a many-to-many relationship
  - One entity can have multiple identities.
  - One identity can be allocated/claimed/used by multiple entities.
  - An **identity management system** or an **identity provider** (IdP/IDP) is often used to create, maintain and manage identities, including mappings to entities.
- Identity vs Identifier (ID)
  - Identities are normally identified via a **unique identifier** to avoid ambiguity in the authentication process.
- Real vs Virtual
  - Example: a person’s real name vs a person’s pen name
- Physical vs Electronic
  - Example: a person’s real name vs a person’s email address

Identity management (IdM / IDM)

- The definitions
  - NIST: “Identity management systems are responsible for the creation, use, and termination of electronic identities …”
  - ISO/IEC 24760-1:2019: “processes and policies involved in managing the lifecycle and value, type and optional **metadata** of **attributes** in identities known in a particular domain”
  - ITU-T X.1250 (2009): “A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, **authentication** and **assertions**) used for:
    - assurance of identity information (e.g., identifiers, **credentials**, **attributes**);
    - assurance of the identity of an entity (e.g., users/subscribers, groups, user devices,
    - organizations, network and service providers, network elements and objects, and virtual objects); and
    - supporting business and security applications”

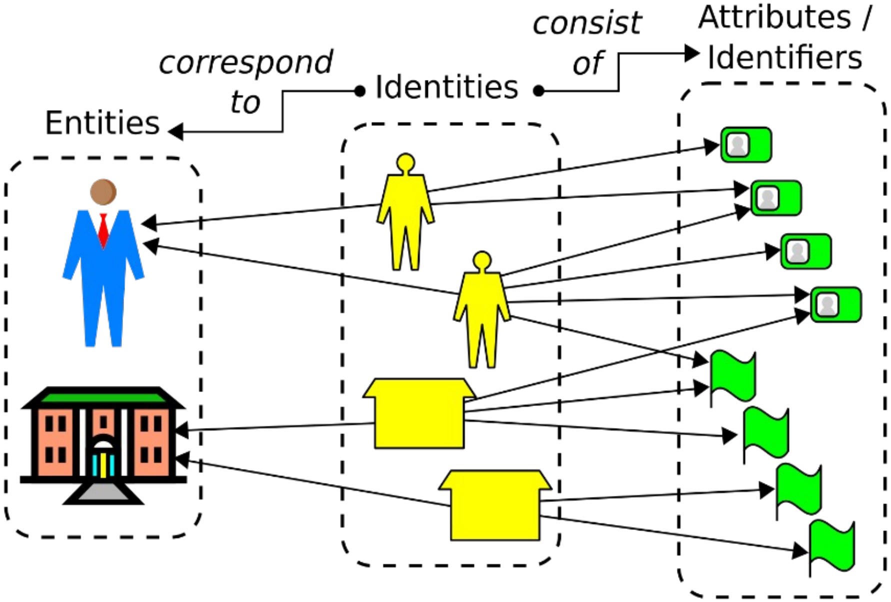
Attributes and credentials



- Attributes
  - ITU-T X.1250 (2009): "Information bound to an entity that specifies a characteristic of the entity."
  - Identifier is a special attribute of an entity.
  - An attribute may be self-claimed by an entity, but may also be assigned by **attribute authorities (AAs)**.
  - IdM is about verifying **attribute assertions**: An entity claims to hold one or more specific attributes (identifier and others).
- Credentials
  - ITU-T X.1250 (2009): "… used to support the authentication of entities – either one or both parties to an information exchange or transaction."
    - Examples: digital certificates, government-issued credentials, SIM cards, automatic teller machine (ATM) cards, …

“In-class” exercise

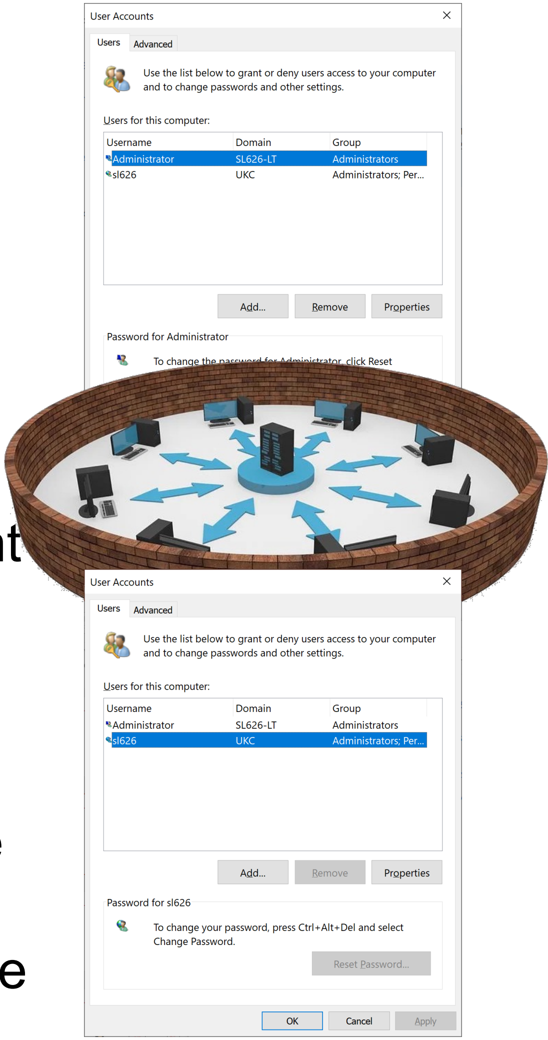
- List some attributes and credentials of entities that are used for real-world service providers you’ve ever seen.
  - Think about why these attributes are needed and if they are self-claimed or are issued / assigned by an AA.
  - What AAs are involved?
  - What attributes are included in each of the credentials?
  - How are such attributes verified?



Author: Audun Jøsang

Local and remote identity management (IdM)

- IdM systems on **local** computing devices
  - Examples: user management system on a local computer (e.g., a Windows PC running a local domain), user management system in a local video game, …
- IdM systems on **remote** servers
  - Examples: Active Directory Domain Services (Windows domain controllers), user management system on remote servers / email servers / websites / any other online services, …
- No clear cut between the two
  - Your local system may actually be based on one or more remote IdM systems (e.g., a cached / synchronised version or just a local user interface of the latter)



User Accounts

Use the list below to grant or deny users access to your computer and to change passwords and other settings.

Users for this computer:

Username	Domain	Group
Administrator	SL626-LT	Administrators
sl626	UKC	Administrators; Per...

Password for Administrator

To change the password for Administrator, click Reset

User Accounts

Use the list below to grant or deny users access to your computer and to change passwords and other settings.

Users for this computer:

Username	Domain	Group
Administrator	SL626-LT	Administrators
sl626	UKC	Administrators; Per...

Password for sl626

To change your password, press Ctrl+Alt+Del and select Change Password.

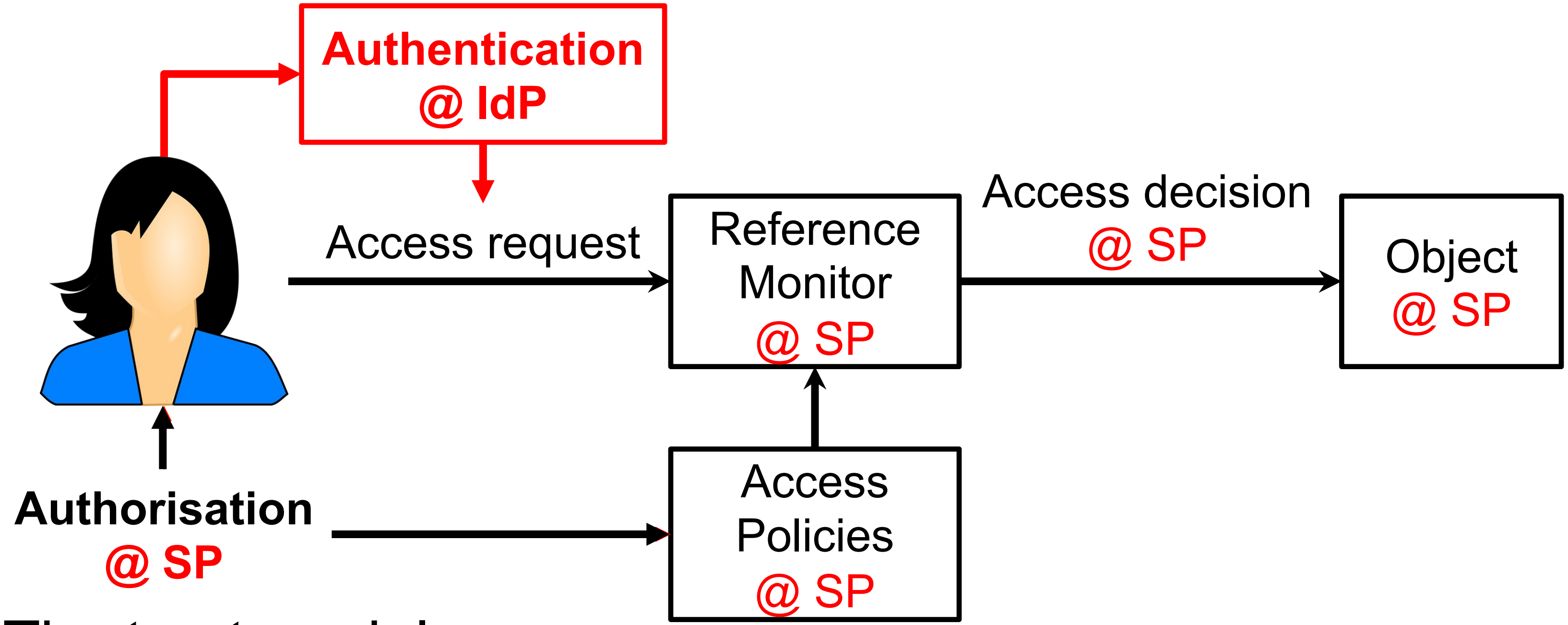
Federated identity management (FIM)

- The problem
  - We are living in a highly connected world.
  - ⇒ We use many different computing systems at the same time.
  - ⇒ It is a pain to register with and log into all systems separately.
- The need
  - **Attribute authentication** (not user authentication):
    Many service providers only need to authenticate one or more relevant attribute(s) of you (e.g., if you have a specific degree).

- A solution
  - Use a **federation** to allow a user to access many security domains
    - ITU-T X.1250 (2009): "An association of users, service providers and identity providers"
  - ⇒ Single sign-on (SSO): A user can access resources at many different service providers by logging in just once.

FIM: The general idea

- Separation of authentication and authorisation
  - Authentication: between users and identity providers (IdPs)
  - Authorisation: between users and service providers (SPs)



Authentication @ IdP

Access request

Reference Monitor @ SP

Access decision @ SP

Object @ SP

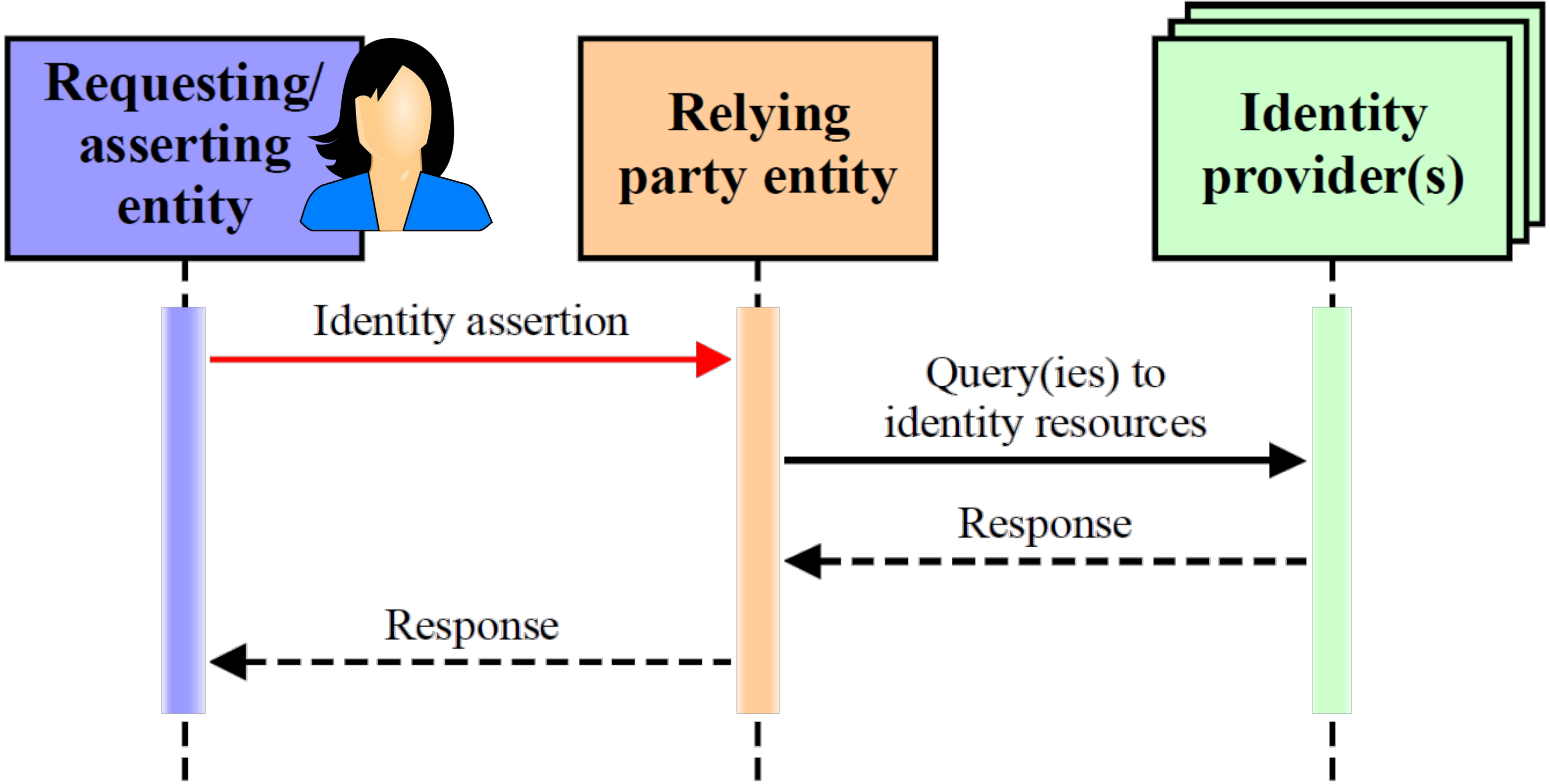
Authorisation @ SP

Access Policies @ SP

- The trust model
  - Users trust IdPs + SPs trust IdPs + Users do not trust SPs (on handling identity information at IdPs)

FIM: A typical three-party protocol (1)

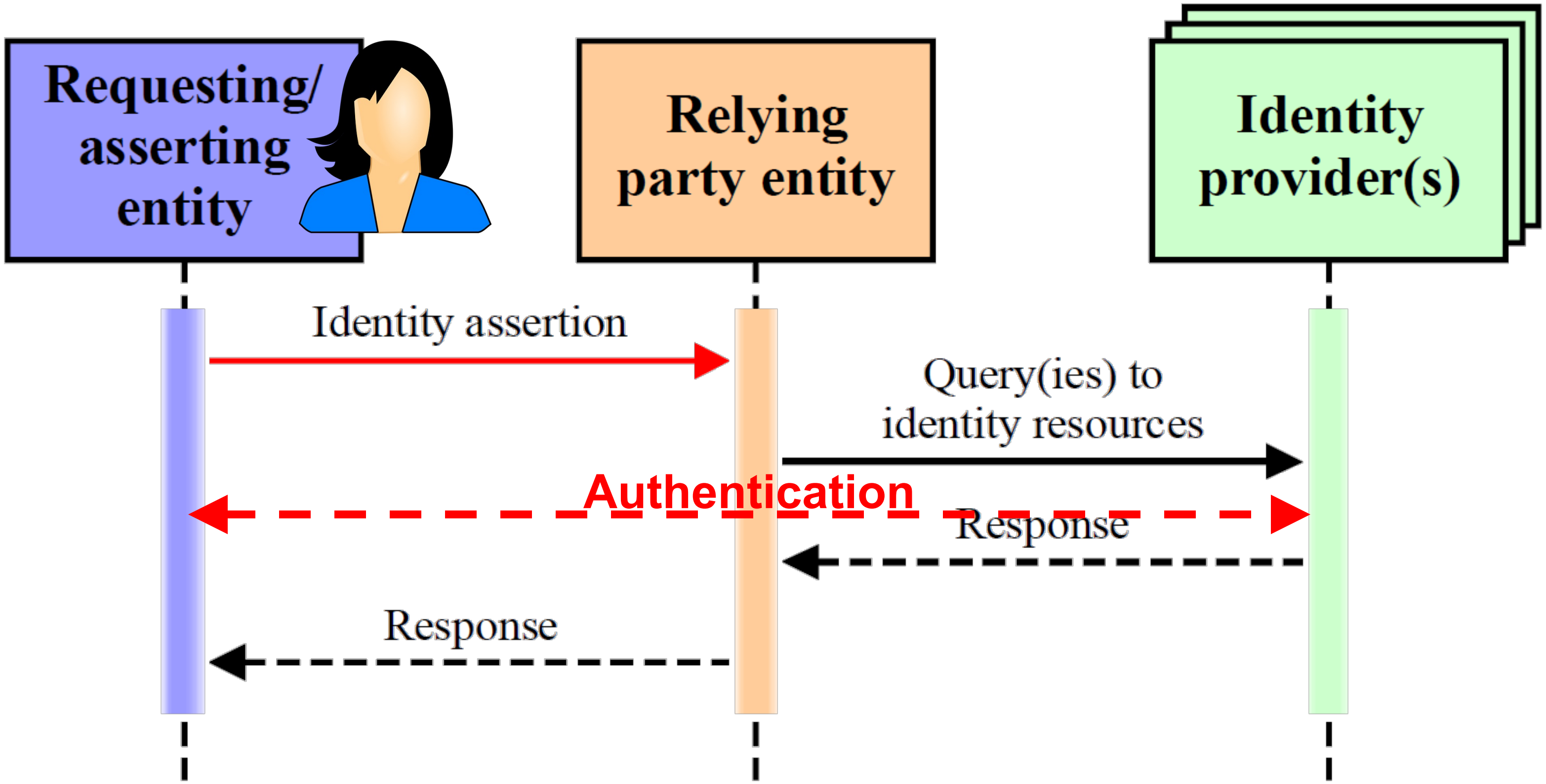
- ITU-T X.1250 (2009) Figure 2a
  - Requesting / asserting entity: subject / principal (e.g., a user)
  - Relying party entity = SP



X.1250(09)_F02a

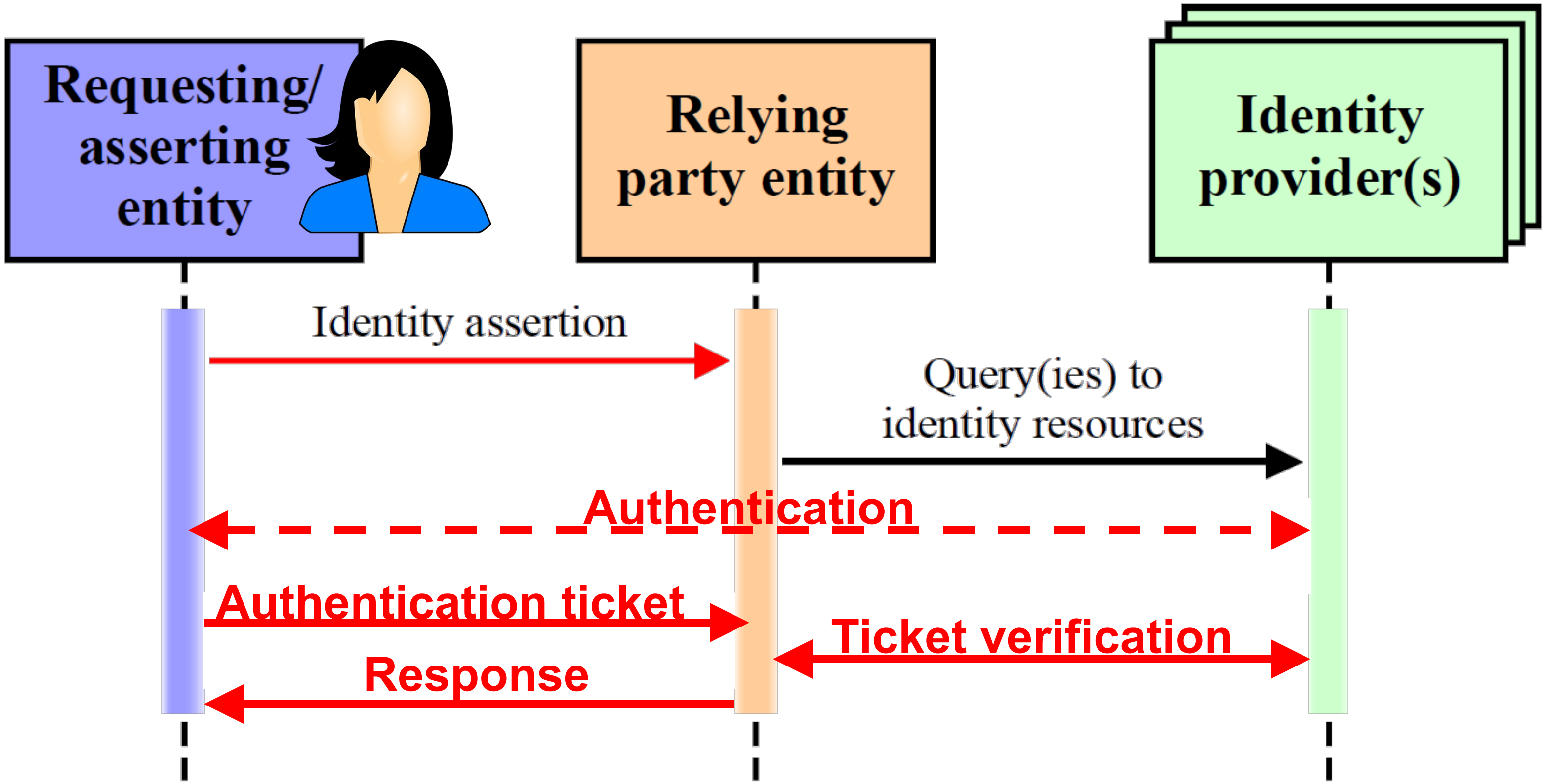
FIM: A typical three-party protocol (2)

- Difference from Figure 2a of ITU-T X.1250 (2009)
  - (If not already done) The user (or the user agent) communicates with the IdP for authentication.



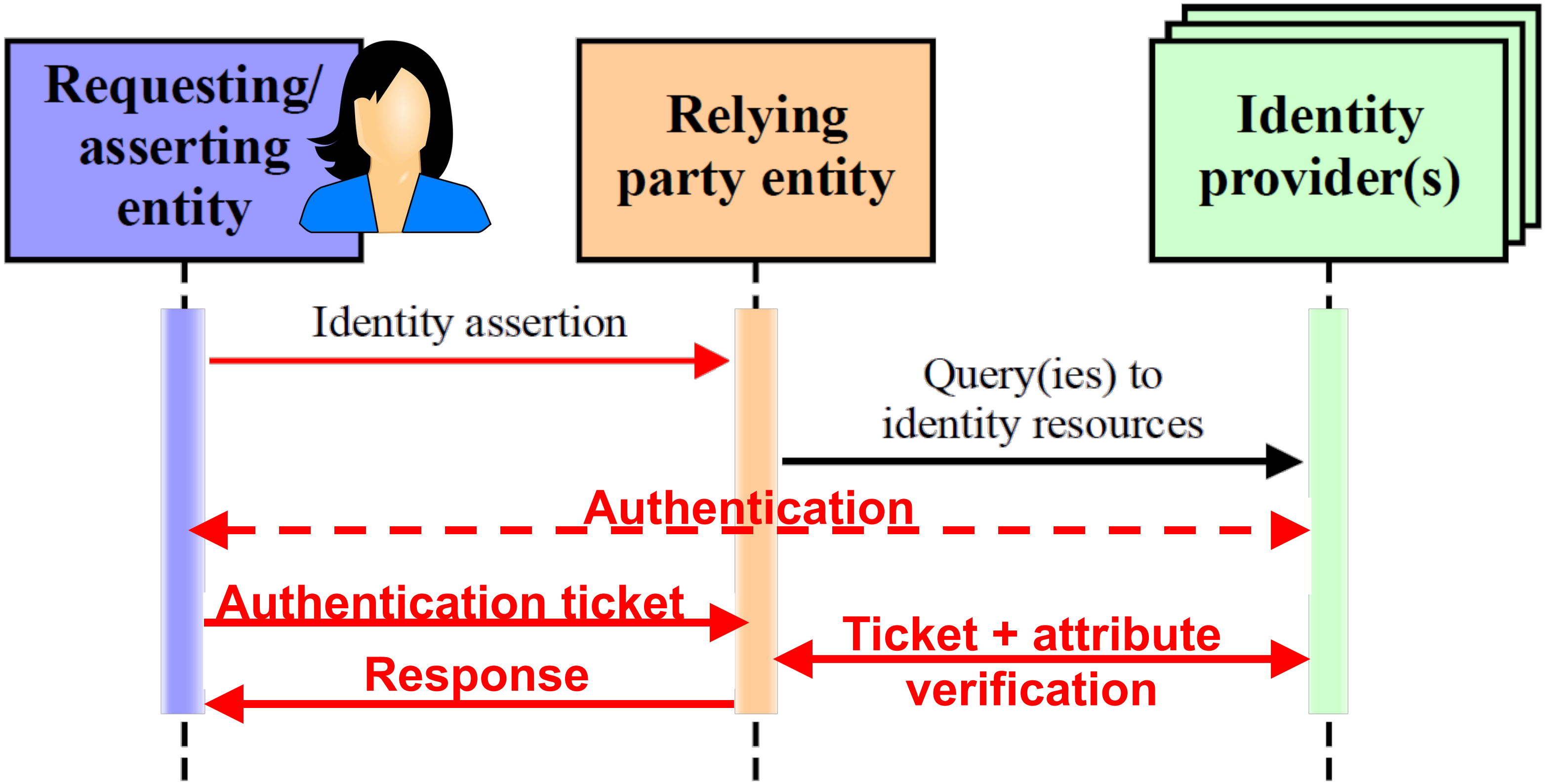
FIM: A typical three-party protocol (3)

- Differences from the one on the previous slide
  - The user (or its agent) returns an authentication ticket to the SP, and the SP verifies it with the IdP.



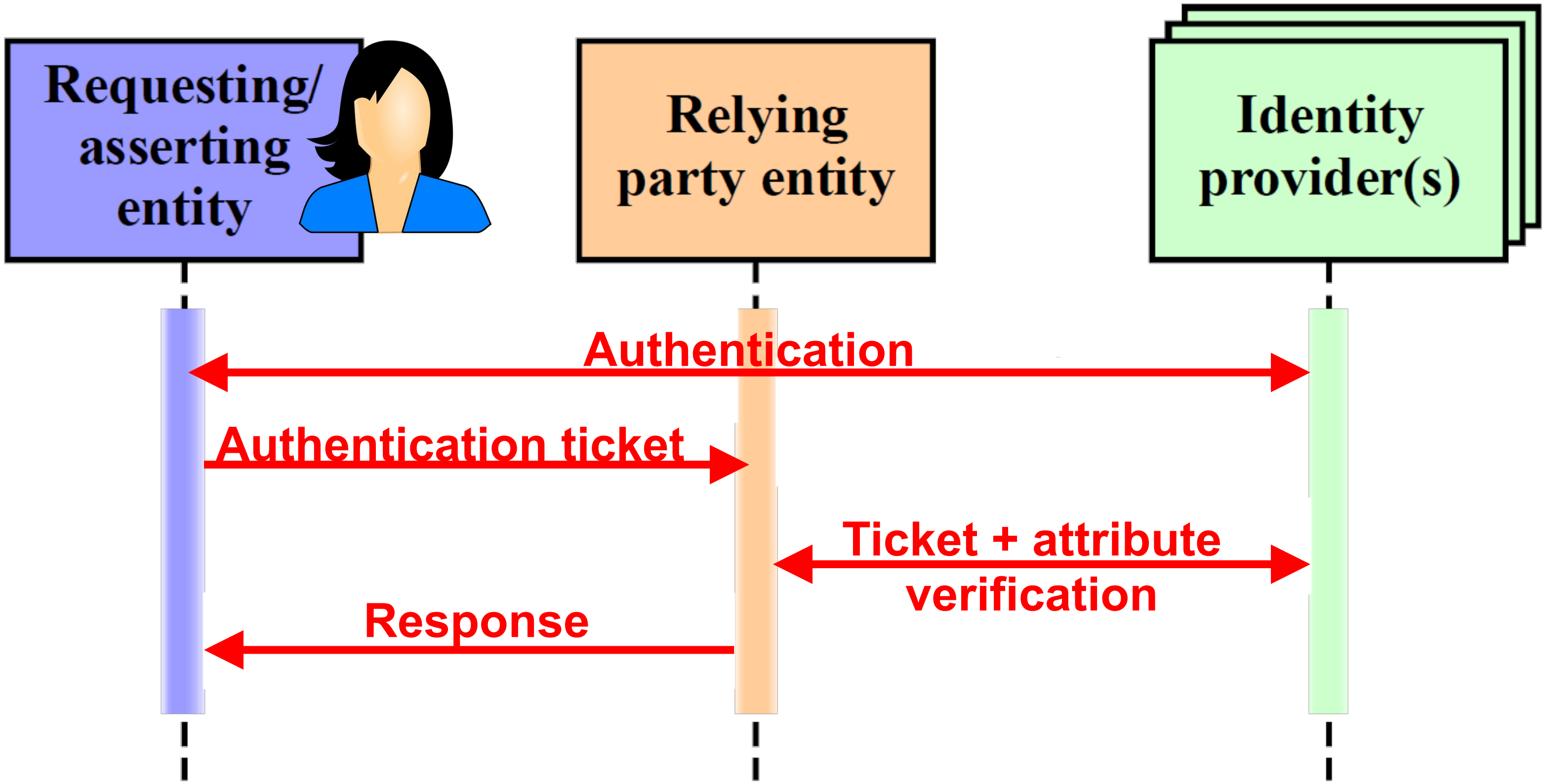
FIM: A typical three-party protocol (4)

- Differences from the one on the previous slide
  - The SP may want to verify some relevant attribute(s) of the requesting entity after authentication is verified.



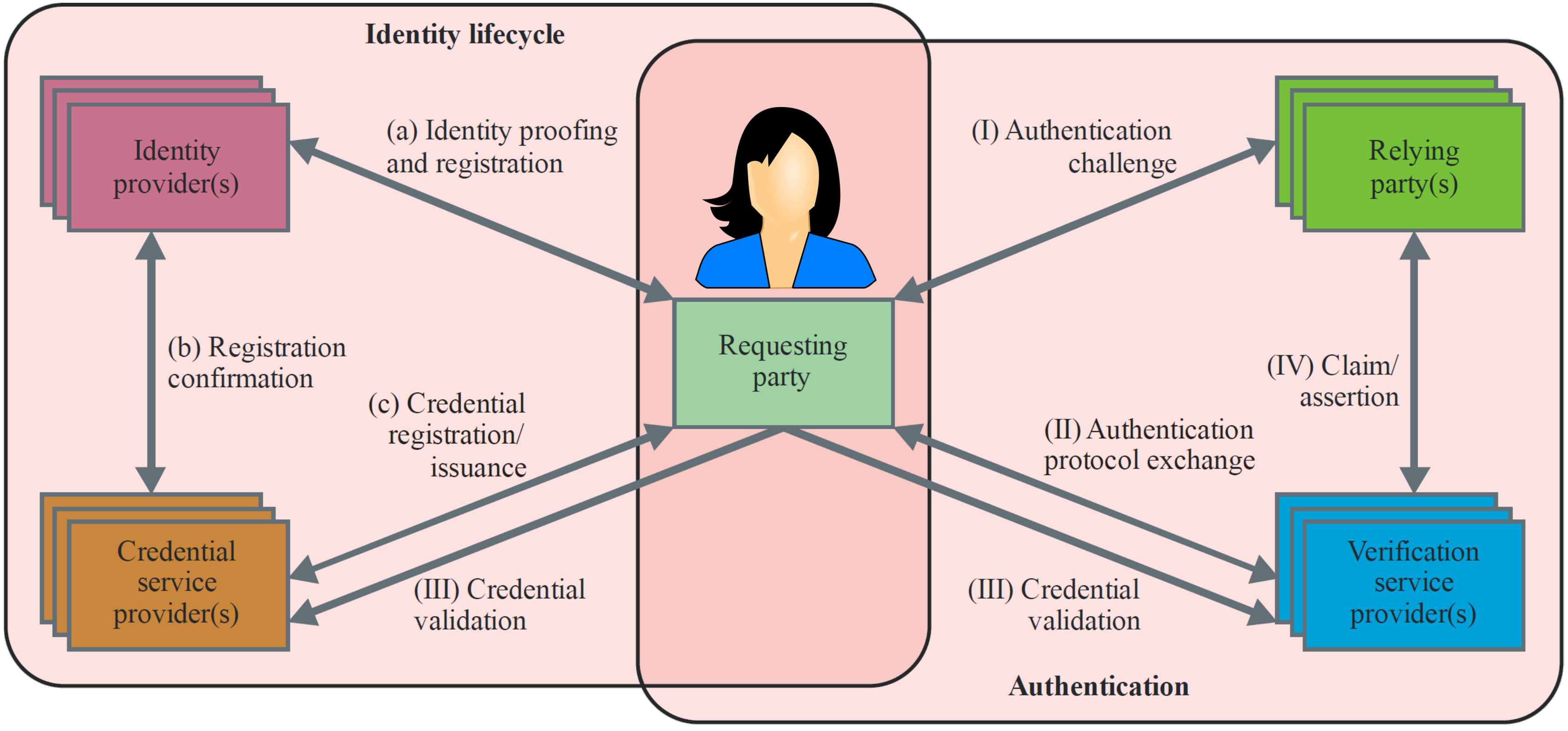
FIM: A typical three-party protocol (5)

- Differences from the one on the previous slide
    - The SP may want to verify some relevant attribute(s) of the requesting entity after authentication is verified.



FIM: A more complicated system

- ITU-T X.1250 (2009) Figure 2b
  - The IdP is split into three separate system entities: identity provider (narrow sense), credential SP, and verification SP



Identity lifecycle
Identity provider(s)
(a) Identity proofing and registration
(b) Registration confirmation
(c) Credential registration/ issuance
Credential service provider(s)
(III) Credential validation
Requesting party
(I) Authentication challenge
Relying party(s)
(IV) Claim/ assertion
(II) Authentication protocol exchange
(III) Credential validation
Verification service provider(s)
Authentication

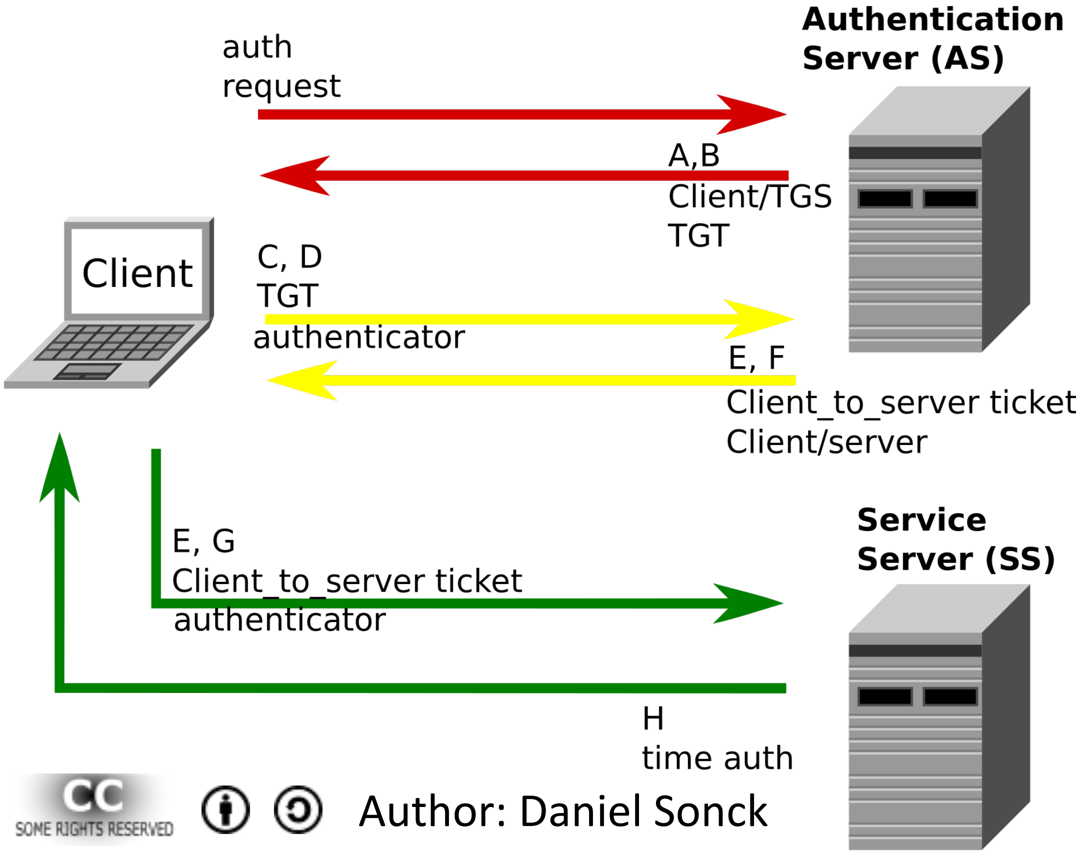
X.1250(09)_F02b

“In-class” exercise

- Find real-world examples of FIMs you’ve ever used or seen.
  - If possible, find out how each FIM system works technically.
  - Depending on the application context, a FIM can involve a single IdP or multiple IdPs.
  - Try to understand **SSO does not mean a single IdP**, not even for a single user (which is why some people prefer using the term RSO – reduced sign-on instead).
- Hint: Pay attention to the trust model and the business model behind those examples.

Selected FIM technique: Kerberos

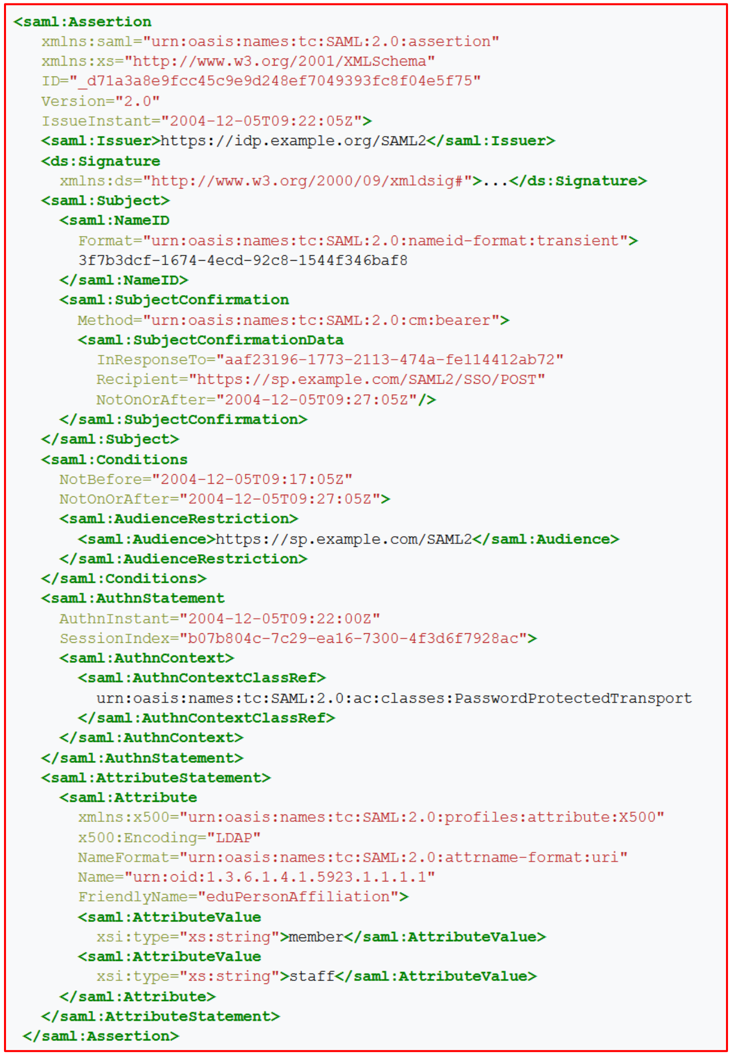
- An **authentication** server (AS) is used as the IdP, and a ticket-granting server (TGS) issues ticket-granting tickets (TGTs) after authentication.
- The TGS **authorises** service requests from clients and issues client-to-server tickets for clients to access service servers (SSs = SPs).



Author: Daniel Sonck

Selected FIM technique: SAML

- SAML = Security Assertion Markup Language
    - Current version 2.0 (2005)
    - A standard of OASIS (Organization for the Advancement of Structured Information Standards)
- Two types of system entities
    - SAML identity providers: authentication authorities and attribute authorities
    - SAML service providers
- An example SAML 2.0 assertion (→)
    - The assertion ("b07b804c-7c29-ea16-7300-4f3d6f7928ac") was issued at time "2004-12-05T09:22:05Z" by identity provider (https://idp.example.org/SAML2) regarding subject (3f7b3dcf-1674-4ecd-92c8-1544f346baf8) exclusively for service provider (https://sp.example.com/SAML2).



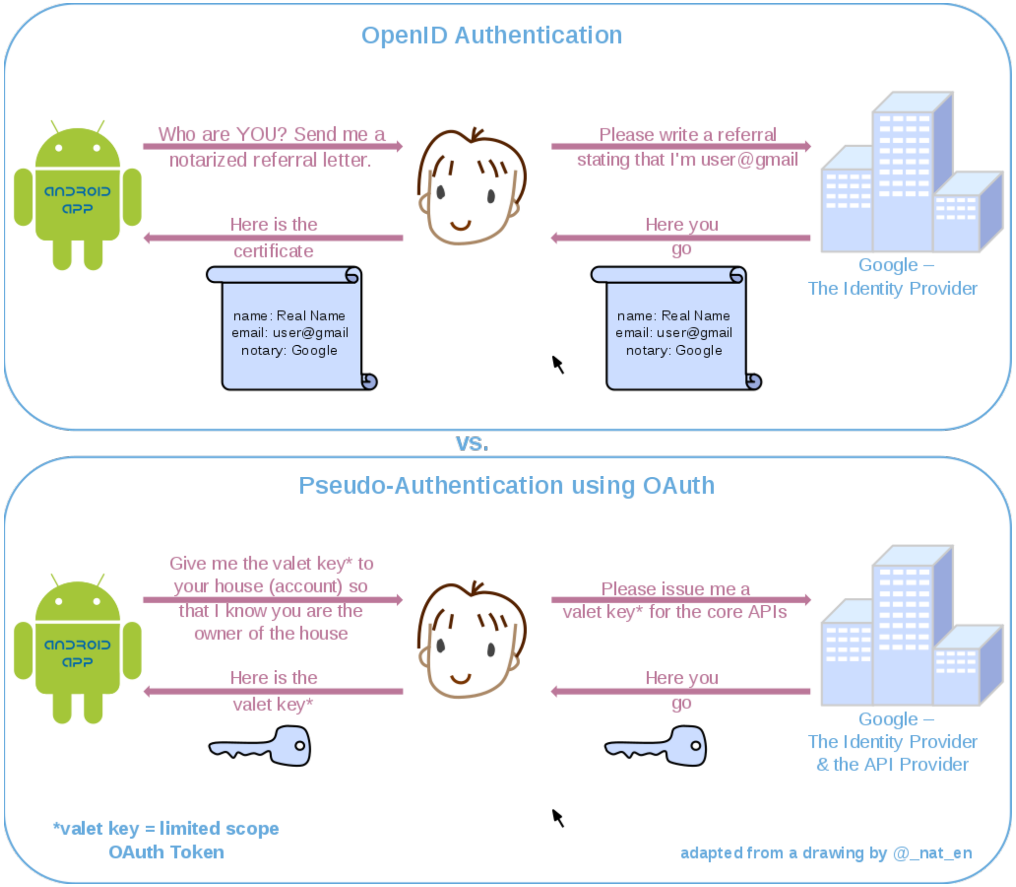
```xml
<saml:Assertion
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   ID="_d71a3a8e9fcc45c9e9d248ef7049393fc8f04e5f75"
   Version="2.0"
   IssueInstant="2004-12-05T09:22:05Z">
   <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
   <ds:Signature
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
   <saml:Subject>
     <saml:NameID
       Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
       3f7b3dcf-1674-4ecd-92c8-1544f346baf8
     </saml:NameID>
     <saml:SubjectConfirmation
       Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
       <saml:SubjectConfirmationData
         InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
         Recipient="https://sp.example.com/SAML2/SSO/POST"
         NotOnOrAfter="2004-12-05T09:27:05Z"/>
     </saml:SubjectConfirmation>
   </saml:Subject>
   <saml:Conditions
     NotBefore="2004-12-05T09:17:05Z"
     NotOnOrAfter="2004-12-05T09:27:05Z">
     <saml:AudienceRestriction>
       <saml:Audience>https://sp.example.com/SAML2</saml:Audience>
     </saml:AudienceRestriction>
   </saml:Conditions>
   <saml:AuthnStatement
     AuthnInstant="2004-12-05T09:22:00Z"
     SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
     <saml:AuthnContext>
       <saml:AuthnContextClassRef>
         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
       </saml:AuthnContextClassRef>
     </saml:AuthnContext>
   </saml:AuthnStatement>
   <saml:AttributeStatement>
     <saml:Attribute
       xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
       x500:Encoding="LDAP"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
       FriendlyName="eduPersonAffiliation">
       <saml:AttributeValue
         xsi:type="xs:string">member</saml:AttributeValue>
       <saml:AttributeValue
         xsi:type="xs:string">staff</saml:AttributeValue>
     </saml:Attribute>
   </saml:AttributeStatement>
 </saml:Assertion>
```

Selected FIM technique: OpenID

- An open standard for (decentralised) authentication protocol on the Web
  - Current version 2.0 (2007)
  - Promoted by [OpenID Foundation]
- For users to access multiple websites (SPs) by using an OpenID IdP.
  - SPs are called OpenID acceptors (who accept authentication assertions from OpenID IdPs).
- [OpenID Attribute Exchange] facilitates attribute assertions.

Selected FIM technique:
OAuth 2.0 + OpenID Connect (OIDC)

- OAuth 2.0 (IETF RFC 6749, 2012)
  - A **user-centric** **authorisation** framework for users to grant access of their information on some websites to other websites or applications.
- OIDC
  - OpenID **authentication** layer on top of OAuth 2.0
  - Current version 1.0 (2014)
- An example (↗)

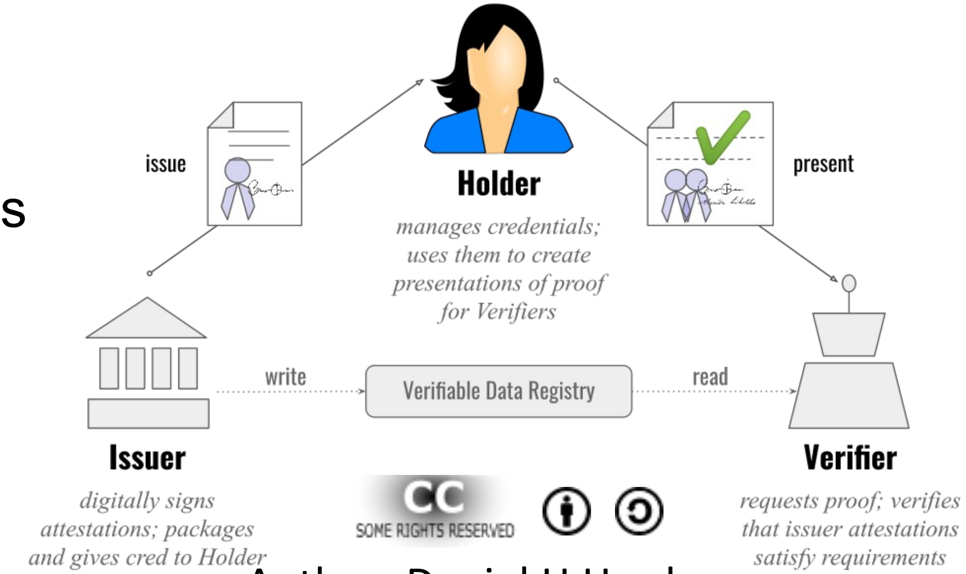

OpenID Authentication
ANDROID APP
Who are YOU? Send me a notarized referral letter.
Please write a referral stating that I'm user@gmail
Here is the certificate
Here you go
name: Real Name
email: user@gmail
notary: Google
name: Real Name
email: user@gmail
notary: Google
Google – The Identity Provider
vs.
Pseudo-Authentication using OAuth
ANDROID APP
Give me the valet key* to your house (account) so that I know you are the owner of the house
Please issue me a valet key* for the core APIs
Here is the valet key*
Here you go
Google – The Identity Provider & the API Provider
*valet key = limited scope OAuth Token
adapted from a drawing by @_nat_en

The future?
Self-sovereign identity (SSI)

- Self-sovereign = Giving control back to users!
  - **Claim-issuers** issue identities to users.
  - **Each user controls her/his own identities**.
  - A user presents (part of) her/his identity to a **verifier** so that the latter can verify the presented identity (i.e., relevant attribute(s)).
  - Such user-controlled identities can be represented in the form of **verifiable credentials** (more on the next slide).
  - European Self-Sovereign Identity Framework (ESSIF)
- Can be based on decentralised identifiers (DIDs) or more traditional (centralised) identities.
  - W3C DID working group is drafting a DID standard (as of 12/2020):
    - "DIDs are URIs that associate a DID subject with a DID document allowing trustable interactions associated with that subject."

The future?
Verifiable credentials (VCs)

- Verifiable credentials (VCs)
  - Electronic credentials that individual users can hold and get them verified by others when needed in the context of SSI.
  - W3C Verifiable Credentials Data Model 1.0 (2019)
- Use cases
  - Parking permits
  - COVID immunity passports
  - …


issue
Holder
manages credentials; uses them to create presentations of proof for Verifiers
present
write
Verifiable Data Registry
read
Issuer
digitally signs attestations; packages and gives cred to Holder
SOME RIGHTS RESERVED
Verifier
requests proof; verifies that issuer attestations satisfy requirements

Author: Daniel H Hardman

The future?
Verifiable credentials (VCs)

- If you are interested to learn more, you can have a look at the work of a former colleague: Professor David Chadwick, who is an expert in FIM and VC.
  - Reducing Identity Theft with Verifiable Credentials
    - https://www.youtube.com/watch?v=MgE5dI09A4M
  - Self Sovereign Identity (SSI) Covid-19 Application Demo
    - https://www.youtube.com/watch?v=Q-1X1FRSTss

Outline

- Identity Management
- Summary

Making it easier to manage your identity

- Identity Management
  - A way to alleviate the burden of remembering and managing too many passwords
- Some examples
  - Federated Identity Management (FIM)
  - Self-sovereign Identity (SSI)
  - Verifiable Credentials (VC)
- Final Lecture:
  - Accountability