

# Identity Management Systems

## Lecture „Secure Application Design“

Dr. Thomas Zefferer

*Summer Term 2025*

# Topics for Today's Lecture

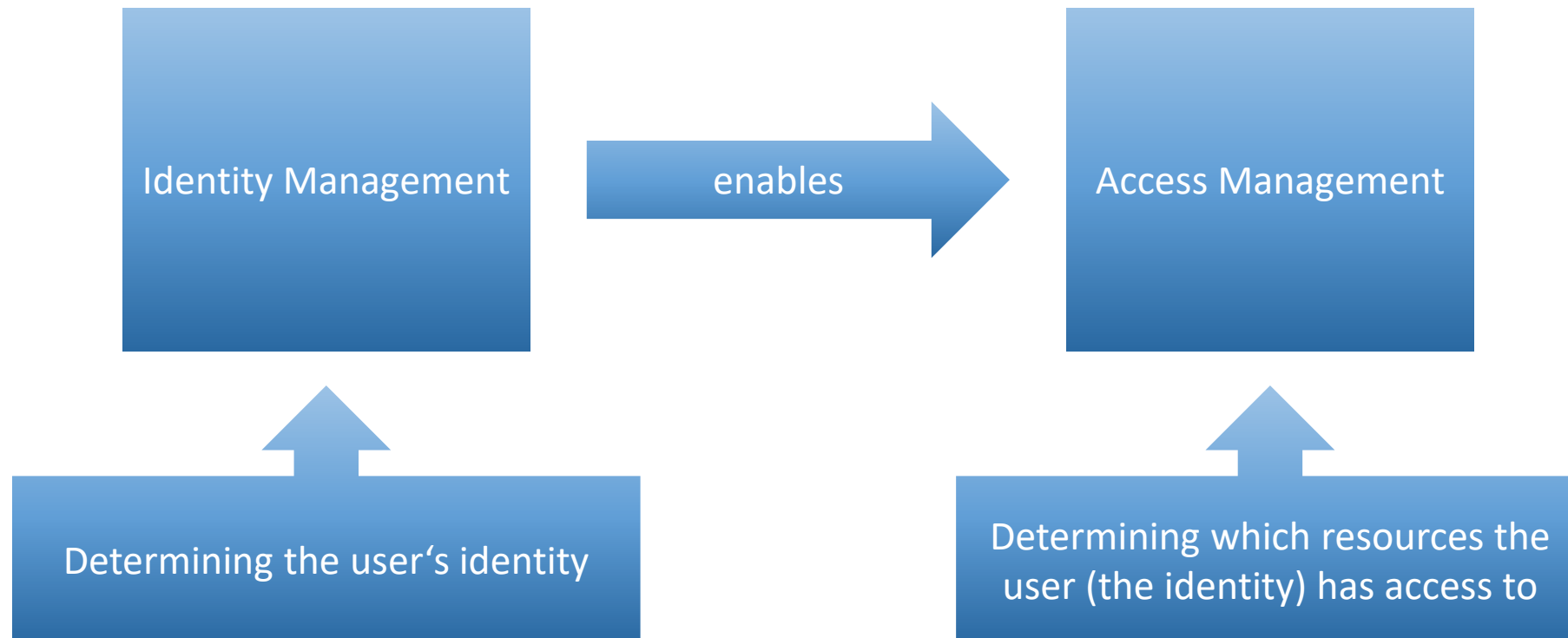
- The idea behind identity management
- “Identity” vs. “electronic identity”
- Identification vs. authentication vs. authorization
- Authentication as crucial aspect in identity management
- Overview of common identity-management models
- The special role of the identity provider
- A first glimpse at ID Austria

# Identity Management



Goal: An IT system („Service Provider“) needs to know the identity of the user, e.g., to decide whether the user is granted access to certain resources (service, data, etc.)

# Identity Management vs. Access Management



By the way... what do we mean with „identity of the user“?

# Identity: Some Definitions

“a person's name and other facts about who they are”  
(*Cambridge Dictionary*)

“the qualities, beliefs, etc., that make a particular person or group different from others”  
(*The Britannica Dictionary*)

“Identity is the qualities, beliefs, personality traits, appearance, and/or expressions that characterize a person or group”  
(*Wikipedia*)

“Identity refers to the distinguishing characteristics or traits that define an individual or entity and differentiate them from others. It encompasses various aspects such as personal attributes, cultural affiliations, social roles, and psychological perceptions that contribute to one's sense of self. Identity can be shaped by factors like ethnicity, nationality, gender, sexuality, religion, occupation, interests, and experiences. It influences how individuals perceive themselves and how they are perceived by others, playing a crucial role in shaping their relationships, behavior, beliefs, and worldview.”

(*ChatGPT 2024*)



# Identity

- Definition of the term „identity“ depends on the context
- Note that this context is not necessarily an IT-related or even technical one
- The good news: For identity management systems, the concept of “electronic identity (eID)” is of particular importance
  - The concept of electronic identities is narrower and hence easier to define/describe
  - Still, it’s good to have at least a rough idea about the term “identity” so that we can distinguish it from the concept “electronic identity”

# Electronic Identity (eID): Some Definitions

In a generic way, an “Electronic identity” is a means for people to prove electronically that they are who they say they are and thus gain access to services. The identity allows an entity (citizen, business, administration) to be distinguished from any other.

*([https://ec.europa.eu/information\\_society/activities/ict\\_psp/documents/eid\\_introduction.pdf](https://ec.europa.eu/information_society/activities/ict_psp/documents/eid_introduction.pdf))*

A digital identity is information used by computer systems to represent an external agent – a person, organization, application, or device.

*(Wikipedia)*

Electronic identity, or e-Identity, refers to the digital representation of an individual’s identity that is used for online transactions and interactions. It is a set of electronic data that can be used to authenticate and verify the identity of an individual in the digital realm.

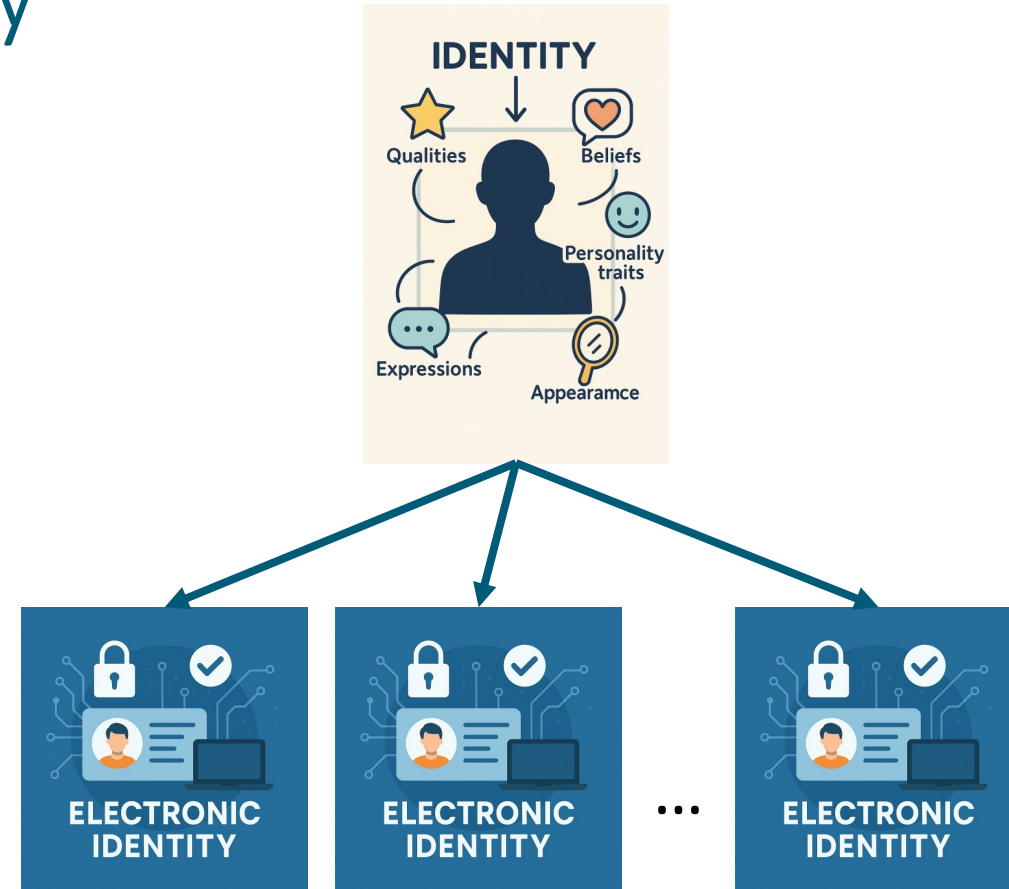
*(ChatGPT)*





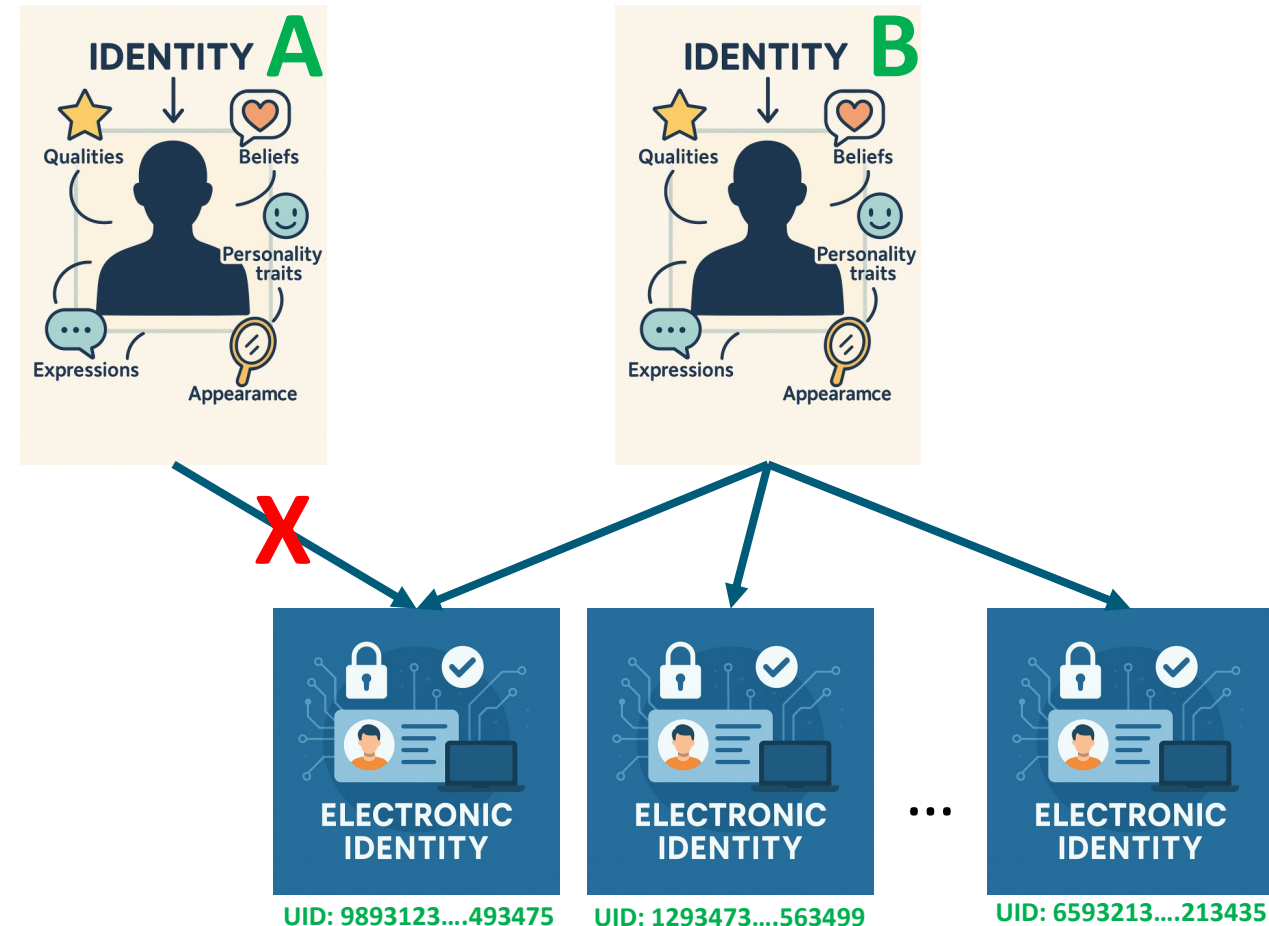
# Identity vs. Electronic Identity

- A natural person (typically) has one identity, but can have multiple electronic identities (eIDs), e.g.:
  - When booking a flight online, you act under your real name, which matches the data in your passport
  - In online discussion forums, you post messages under a pseudonym
  - You use an avatar to participate in online games
  - ...
- Depending on the electronic identity, its link to the person's identity can be more or less strong
  - E.g.: Use of real name vs. pseudonym



# Electronic Identity: Uniqueness

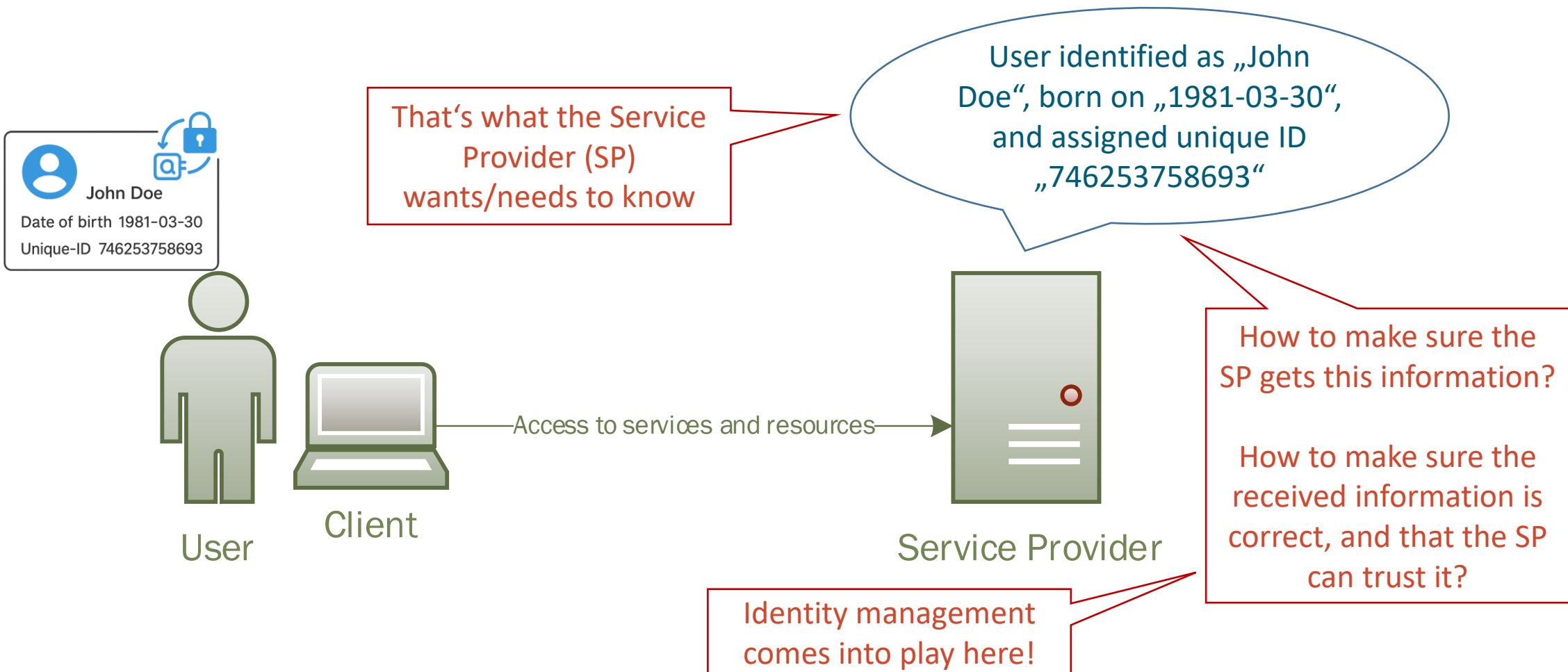
- An electronic identity should be unique, i.e., there must not be two persons with the same electronic identity
  - An electronic identity hence typically comes with a **unique identifier**
  - If electronic identities are not unique, service providers cannot reliably distinguish users



# Electronic Identity: Further Important Concepts

- **Persistence:** An electronic identity can be persistent (**does not change** over time) or non-persistent (**changes** over time)
  - Non-persistence can have privacy advantages
  - Non-persistence raises challenges for service providers (and users)
  
- An electronic identity can be revoked/deleted
  - That's typically not so easy for your real identity
  
- An electronic identity often comes with **additional identity attributes** (name, date of birth, etc.)

# Electronic Identity: Simple Example

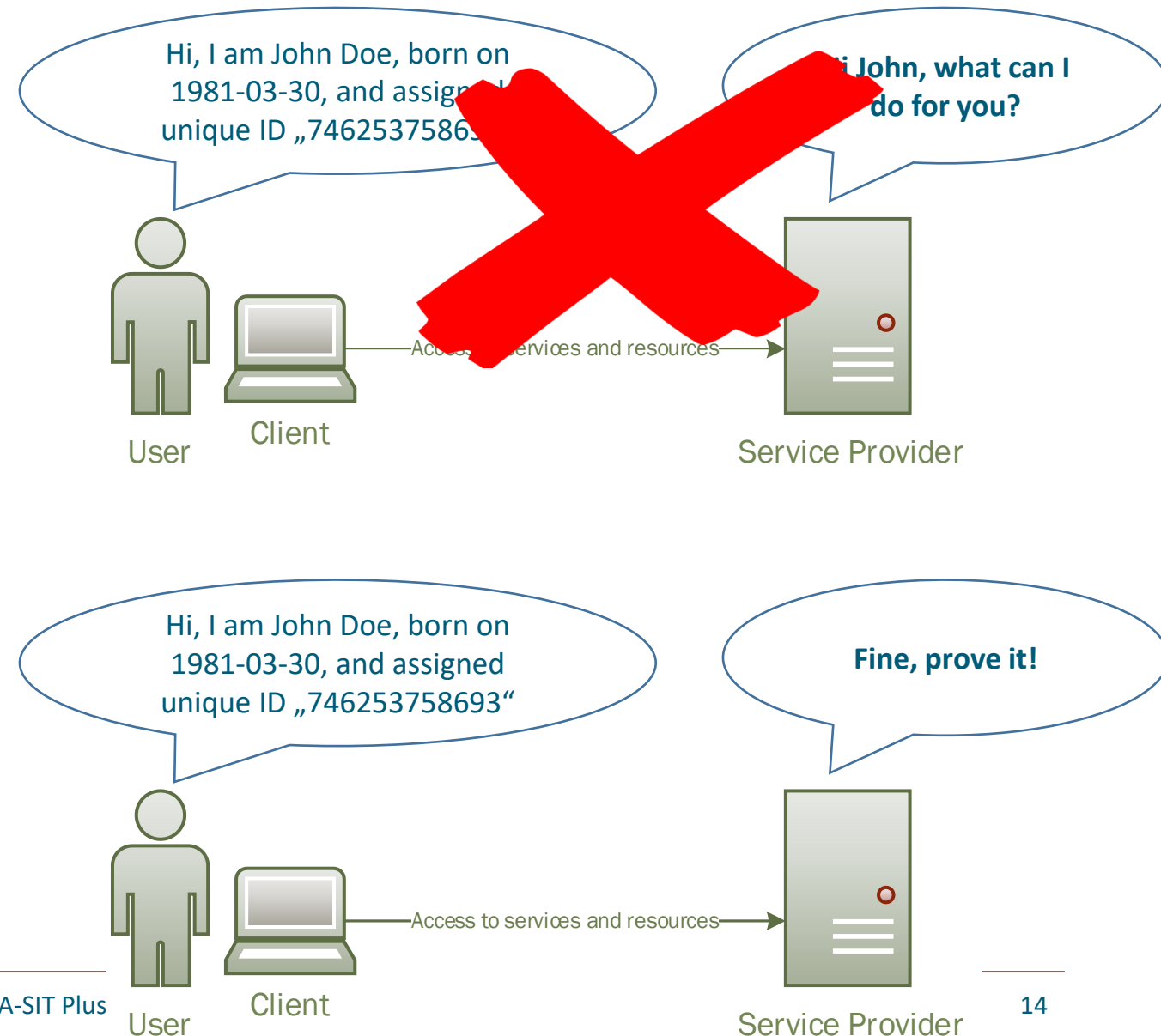


# Identity Management

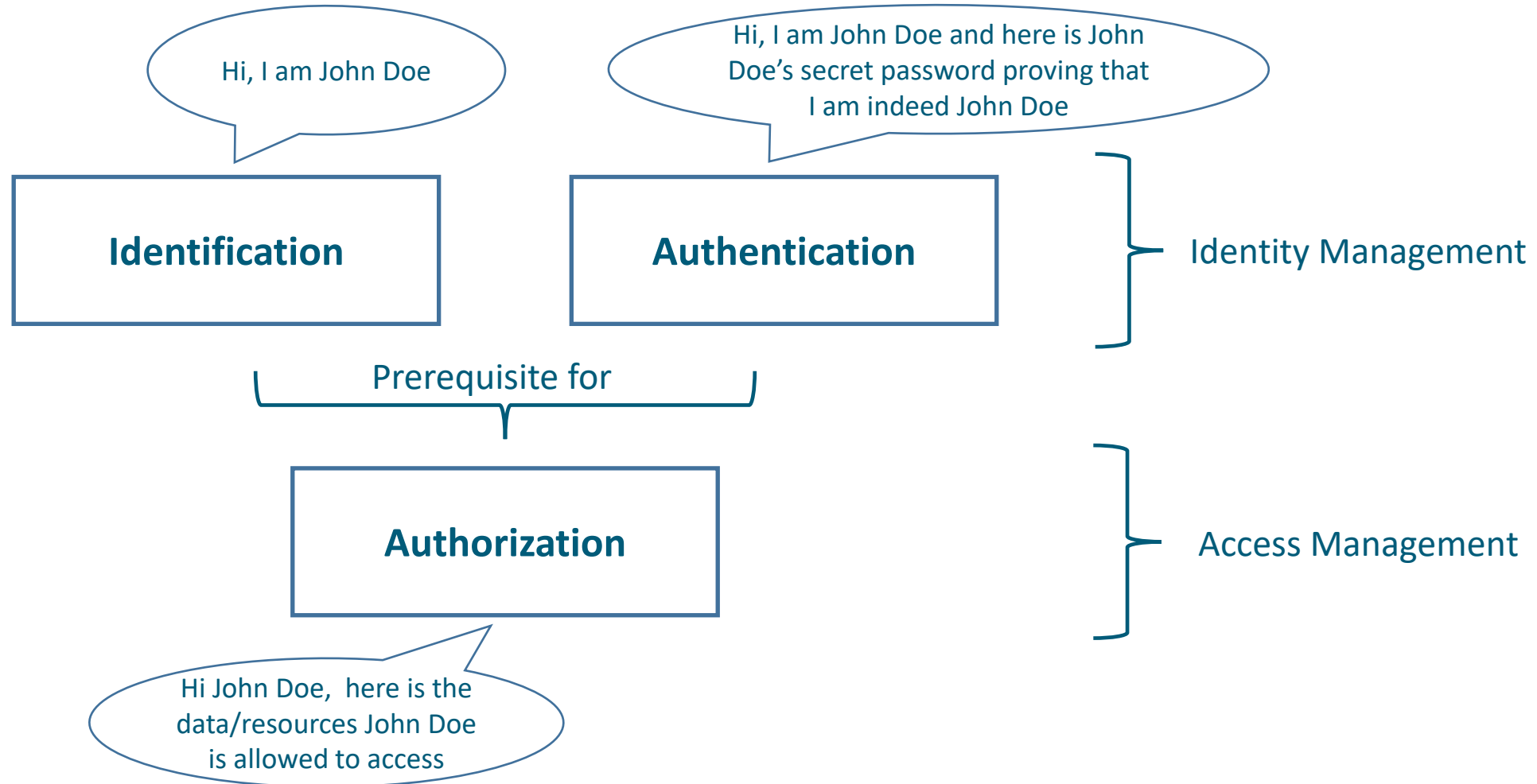
- Identity management: How to empower an IT system (Service Provider) to learn the electronic identity of a user
- Consider: How important is it for the Service Provider to have a link to the „real“ identity of the user?
  - Sufficient to know it is the same user as last week?
  - Need to know the user's correct data, i.e., real name, date of birth, etc.?
- In other words: How close must the electronic identity be related to the user's corresponding identity?
- We will get back to this question a bit later when talking about national identity management systems

# Challenges in IDM

- Claiming an (electronic) identity is not enough – (electronic) identities need to be proven
- Key question: How to accomplish that?



# Identification vs. Authentication vs. Authorization



# Authentication: How to Prove Your Identity

- Proving your identity is a non-trivial task
- Proving your identity in the real world:
  - Showing your passport
  - Showing your ID card
  - Showing some other document attesting your identity
- Proving your electronic identity (eID) in online scenarios:
  - Simply showing an ID card etc. obviously does not work
  - Instead, identity proofs rely on so-called **authentication factors**





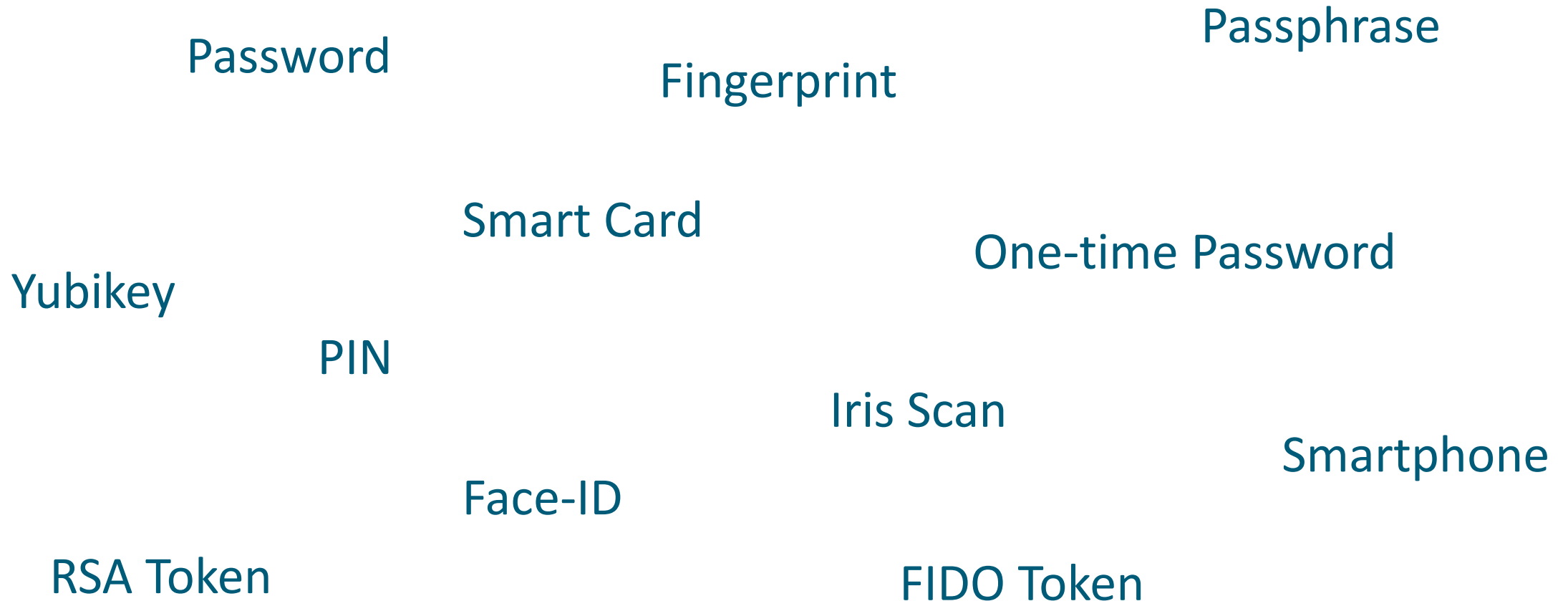
# Authentication Factors

- An authentication factor is a means to prove a claimed electronic identity
  
- Simple Example: Secret password
  - The password is associated with the electronic identity
  - The password is known only to the legitimate holder of that electronic identity
  - By proving knowledge of the password (i.e., by entering the password), the user proves to be the legitimate holder of the electronic identity
  - The verifier (i.e., the entity that wants to learn the user's eID) must have means to verify the entered password

# Authentication Factors – Requirements

- An authentication factor must be associated with the respective eID
- Only the legitimate holder of the eID can use the authentication factor
  - The authentication factor is kept secret (only known to the legitimate eID holder); and/or
  - The authentication factor is infeasible to copy/duplicate
- The authenticating entity must be able to verify the validity of the authentication factor

# Possible Forms of Authentication Factors



# Categories of Authentication Factors

## ■ Knowledge factors: „Something you know“

- Password
- PIN
- ...

+ Easy to use (for user and verifier)  
+ Well established and broadly used  
+ Easy to be changed when compromised

- Trade-off between security and usability (password complexity)  
- Shown to be a weak authentication factor in practice

## ■ Possession factors: „Something you have“

- FIDO Token
- Smart card
- Smartphone
- ...

+ Highly secure when done correctly (use of cryptography, use of tamper-proof hardware, etc.)

- More complex to implement and to use  
- More complex to revoke/replace when compromised  
- Special hardware requirements for users  
- Risk of loss and theft

## ■ Inherence factors: „Something you are“

- Fingerprint
- Iris scan
- Behavior (sometimes seen as separate category)
- ...

+ Easy and convenient to use for end-users  
+ No token needed/Nothing to remember

- Suitable scanning devices needed  
- More complex to implement and integrate  
- Nearly impossible to revoke/replace when compromised

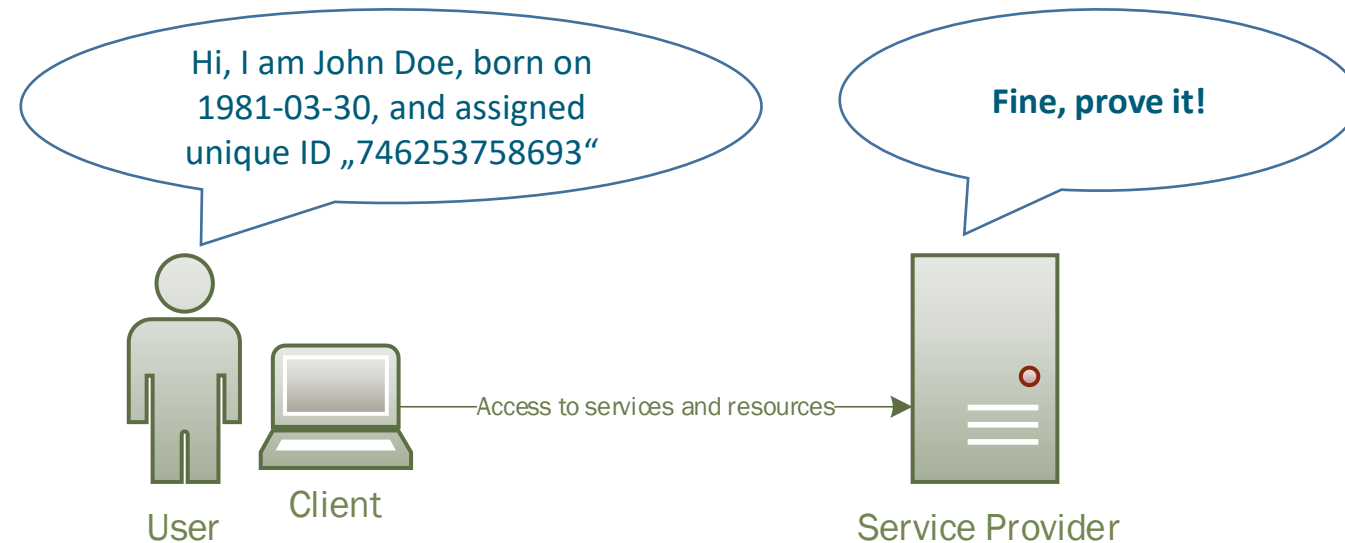
# Multi-Factor-Authentication

- All authentication factors (and categories of authentication factors) come with certain pros and cons
- Security-critical applications hence typically rely on 2-factor authentication or multi-factor authentication
  - Idea: Combine 2 or more authentication factors during an authentication process
    - ◆ Important: Combine factors of different types (e.g., knowledge + possession)
  - Examples:
    - ◆ At ATMs, you need to provide your bank card (factor “possession”) and your PIN (factor “knowledge”) to withdraw money
    - ◆ To log-in to your e-banking account, you need to provide a password (factor “knowledge”) and you need to authorize the log-in in your mobile app using your fingerprint (factors “possession” and “inherence”)
- 2FA/MFA makes user authentication more secure but also more complex for both users and service providers

More on authentication factors in one of your next lecture units!

# Authentication Factors: The Service Provider's Perspective

- To verify a claimed identity, the Service Provider (SP) needs to store reference values of authentication factors
  - Hash value of user password
  - Public key of user
  - Reference value of fingerprint/iris/etc.
  - ...



- SP needs to implement methods to acquire these reference values first („user registration“)
- SP needs to implement authentication method correctly
- In the worst case, user needs to have separate authentication factors for each SP
- **Conclusion: User authentication causes quite some burden for Service Providers and users**

Back to identity management...



# Identity Management

- Identity management: How to empower an IT system (Service Provider) to learn the electronic identity of a user
- We now know: Learning the electronic identity of a user (i.e., authenticating the user) in a secure and reliable way is a challenge, cumbersome, and causes quite some effort

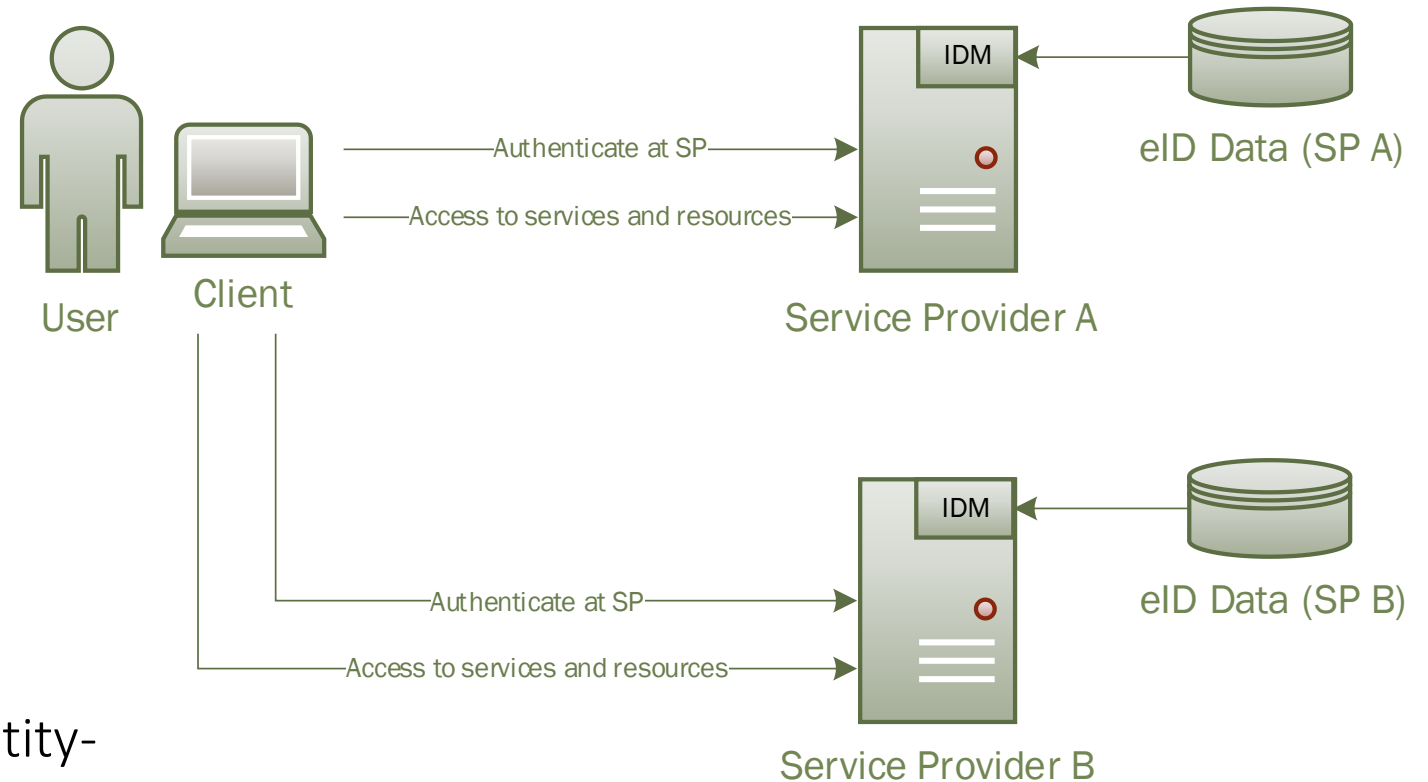
# Identity Management Models

- Different approaches/models to cope with this challenge<sup>1</sup>
  - Isolated model
  - Central model
  - User-centric model
  - Federated model
  - ...
  
- Let's have a more detailed look at some of these models..

[1] Bernd Zwattendorfer, Thomas Zefferer, Klaus Stranacher - "An Overview of Cloud Identity Management-Models", 10th International Conference on Web Information Systems and Technologies (WEBIST), 2014, pp. 82-92 <http://www.webist.org/?y=2014>

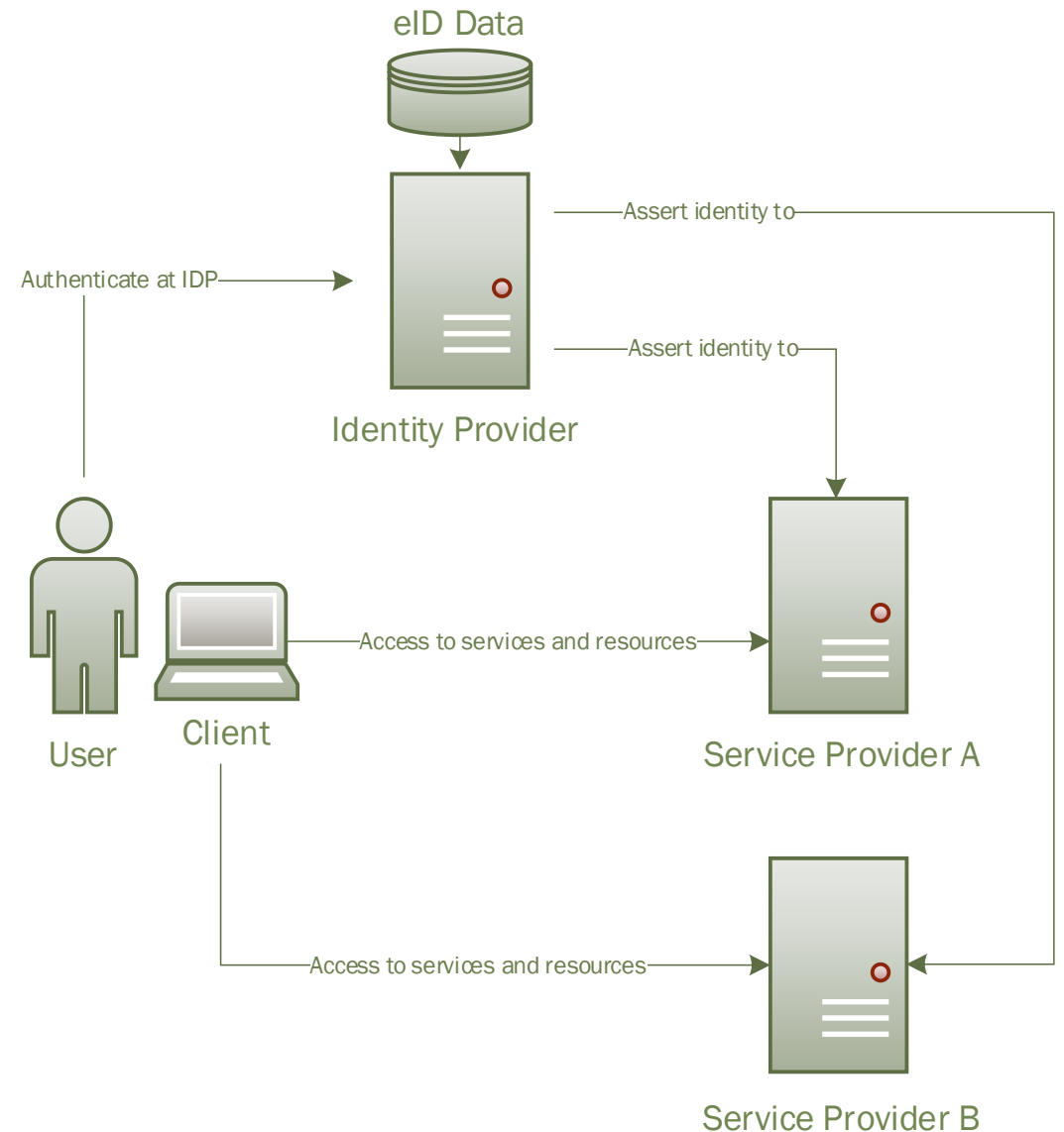
# Isolated Model

- Each SP implements its own user authentication
- Each SP has its own database containing user data
- Pros
  - No external dependencies
- Cons
  - Each SP needs to implement identity-management features on its own
  - User requires separate authentication factors (e.g., passwords) for each SP



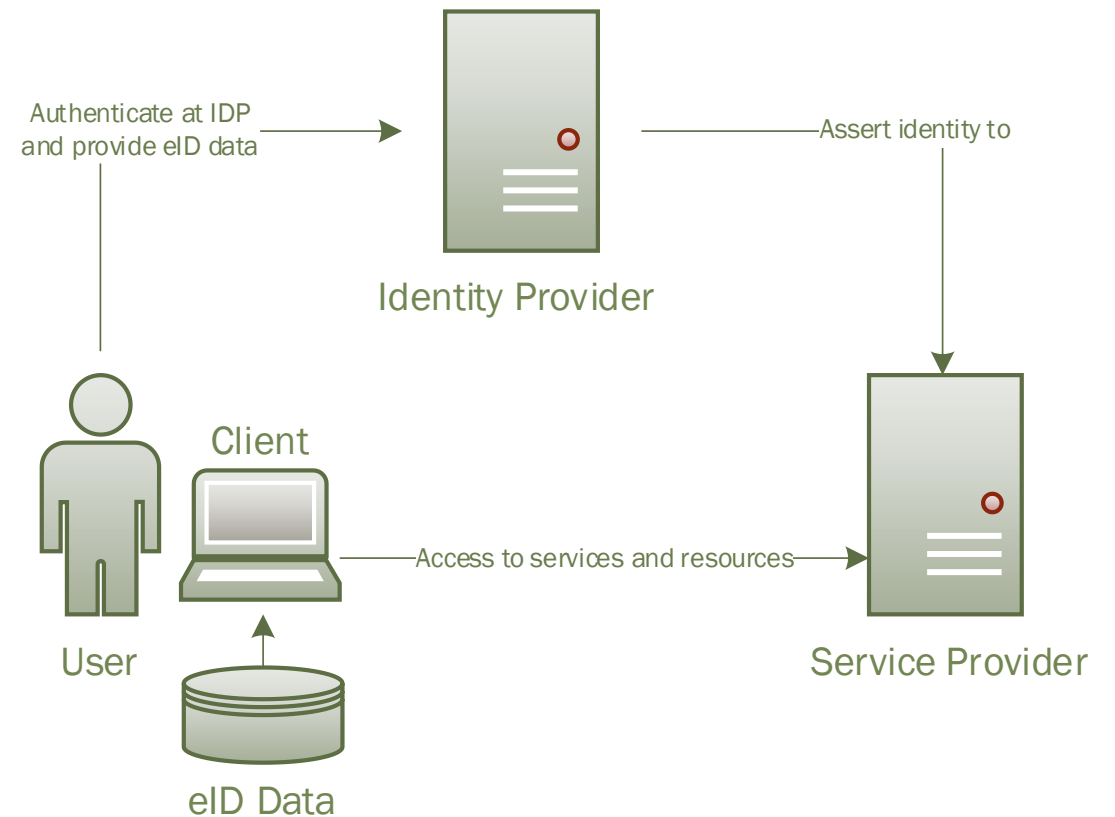
# Central Model

- User authentication is outsourced by the SPs to a central Identity Provider (IDP)
- IDP asserts user's identity by means of a signed assertion/ID token
- One IDP can serve multiple SPs
- Pros:
  - SP does not need to implement user authentication itself
  - User does not need to remember SP-specific authentication factors
  - Widely adopted (SAML2, OIDC, etc.)
- Cons:
  - Single point of failure (IDP)
  - Architecture enables tracking of users



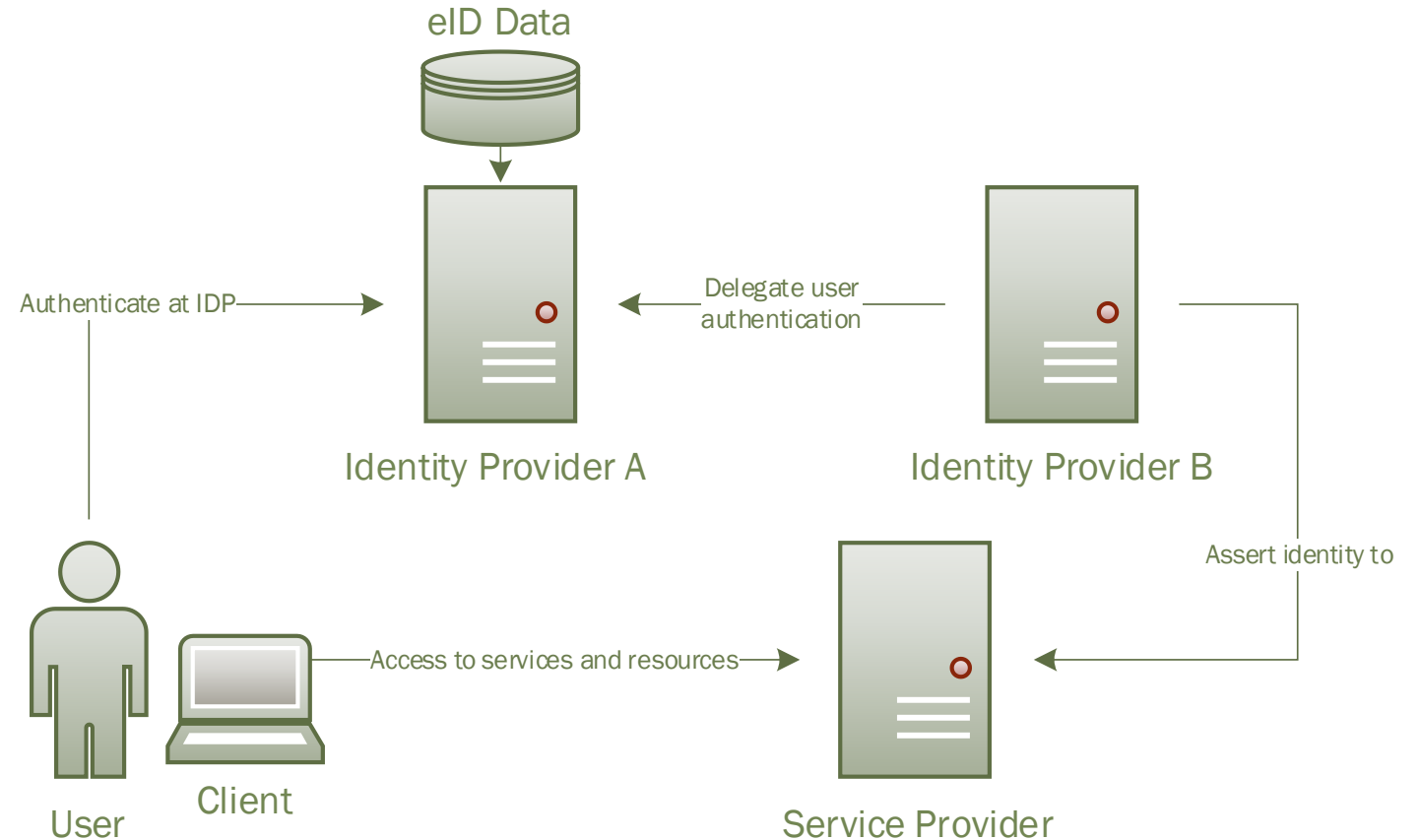
# User-centric Model

- Distinguishing feature compared to central model: eID data is stored in user domain
  - Smart cards
  - Tokens
- Pros:
  - User remains in full (physical) control of eID data
- Cons:
  - Technically more complex
  - Potentially weaker usability



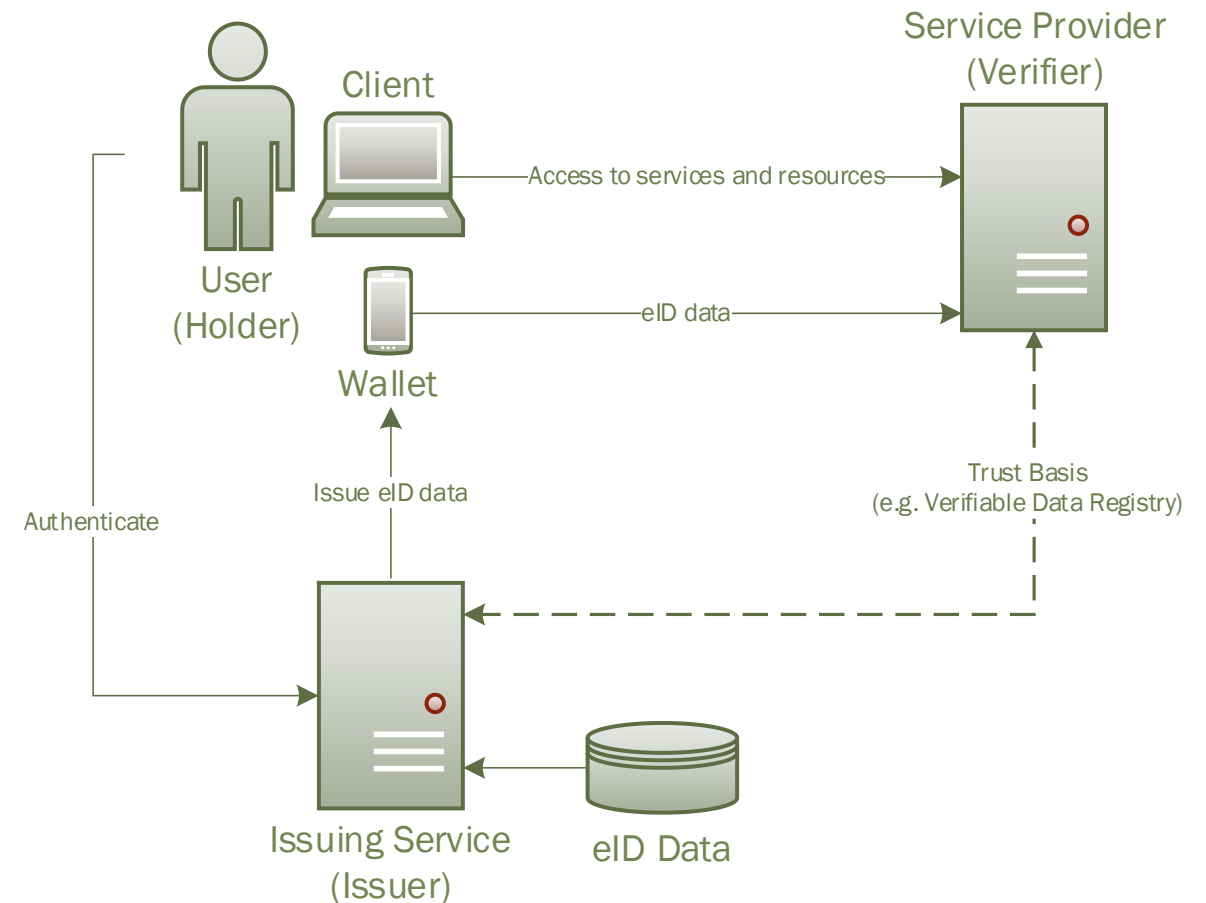
# Federated Model

- Multiple IDPs in place, which can delegate user authentication among each other
- Trust between IDPs is crucial
- Pros:
  - Allows for large cross-domain use cases
- Cons:
  - Trust management between IDPs needed



# Decentralized Models

- No IDP involved during user authentication
- eID data is stored to wallet (issuing) and can be used repeatedly for authentication (presentation)
- Pros
  - Tracking of user behavior can be prevented
  - Support for offline use-cases
- Cons
  - More complex verification of provided eID data
  - Copies of eID data stored in wallet
    - ◆ Data still up-to-date when needed?
    - ◆ How to revoke outdated data?



# The Crucial Role of the Identity Provider

- Identity management: How to empower an IT system (Service Provider) to learn the electronic identity of a user
- Several approaches/models exist to realize identity management in practice
- Irrespective of the underlying model, the **Identity Provider plays a crucial role**, as it verifies (by means of user authentication) the user's identity and attests the user's identity to the Service Provider
  - Note: In decentralized models, the IDP and its functionality is conceptually covered by the Issuing Service
- Both users and service providers need to trust the identity provider



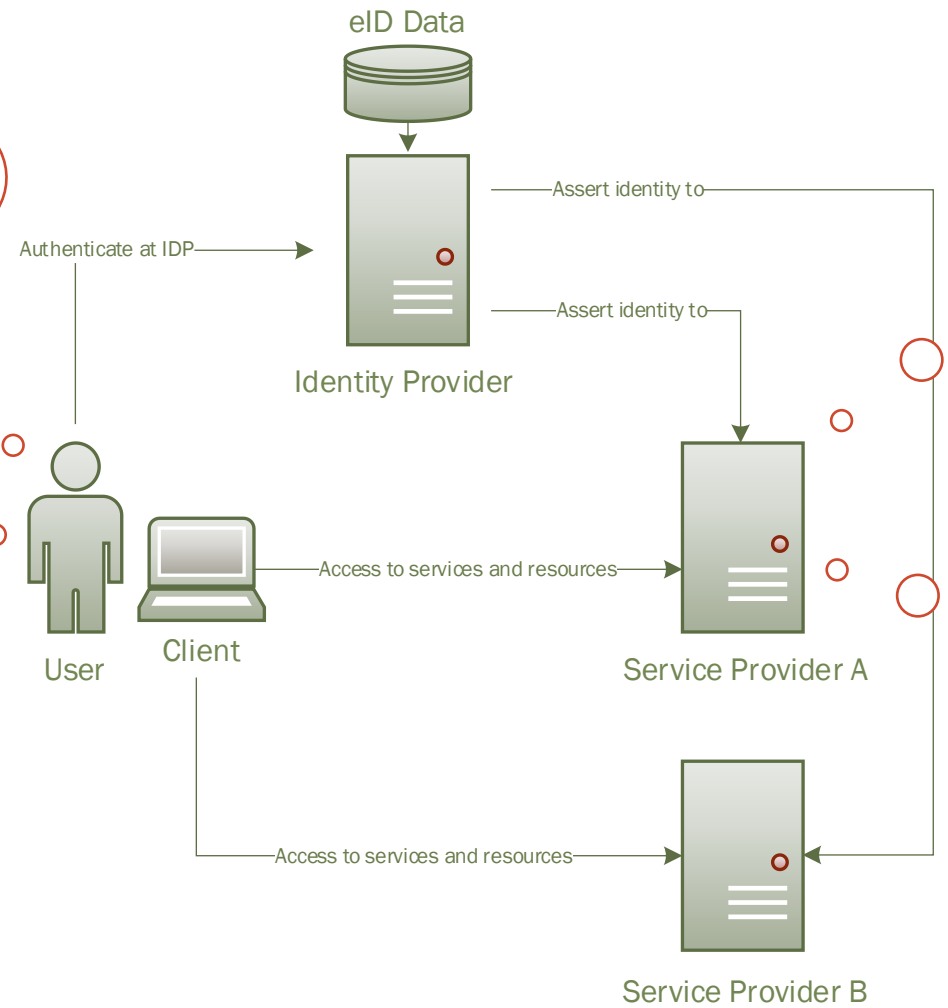
# Trust in the Identity Provider

Can I be sure that the IDP handles my data with care and forwards correct data to the Service Provider?

Can I be sure the asserted identities and associated eID data from users are correct?

Can I be sure the IDP does not misuse the information it learns during authentication processes?

Can I be sure the IDP does not misuse the information it learns during authentication processes?



# Trust in the Identity Provider – Key Questions

- Who operates the IDP?
  - In-house (e.g., a company operates a central IDP for all its own service providers)
  - A third private-sector company (Google, Apple, etc.)
  - A public-sector government body (EU Member State, etc.)
  - ...
  
- Why and how can we trust the IDP?
  - To which extent can we trust profit-oriented private-sector companies?
  - When does it make sense to rely on state-operated IDPs?
  - As a company, is it always the best idea to operate our own IDP in-house?
  - ...
  
- Consider what you've heard about trust in one of the previous lecture units

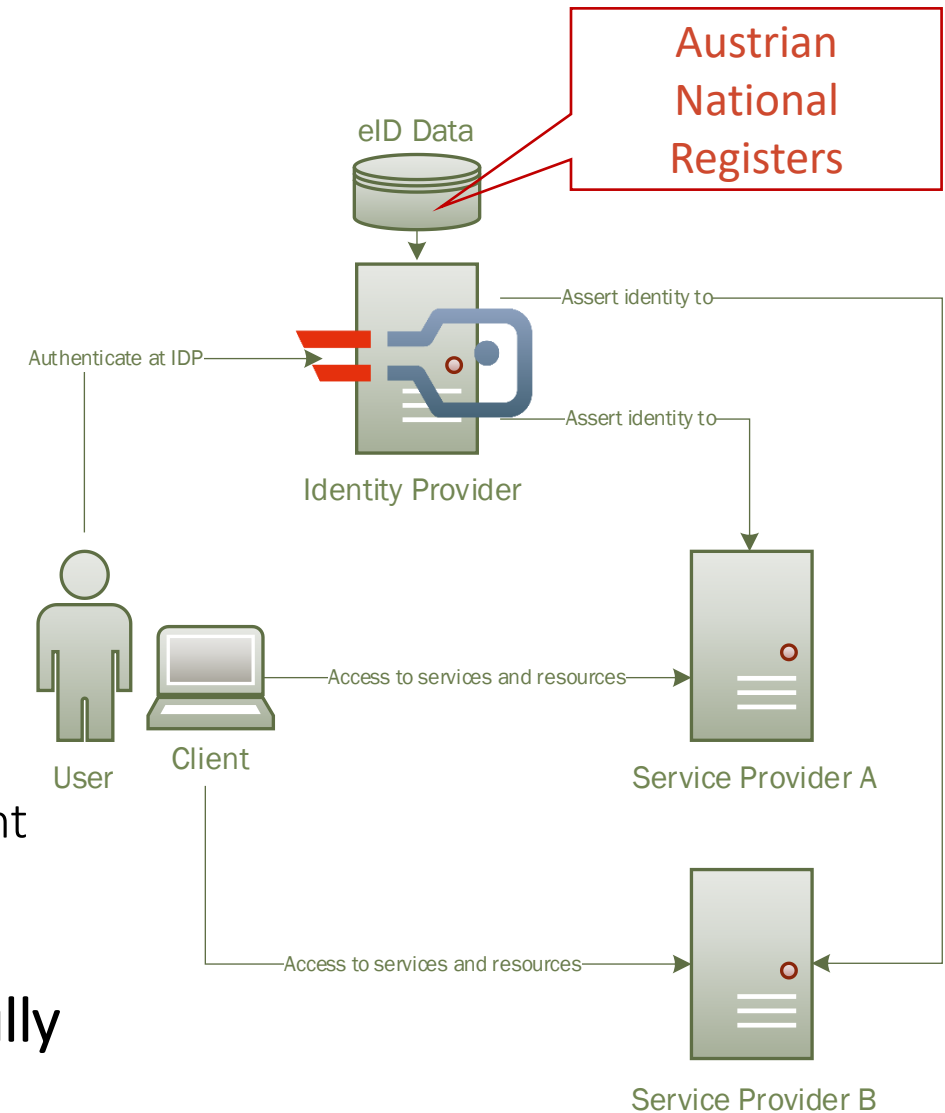
# National Identity Management

- The state (public sector) operates the IDP and provides its citizens with an electronic identity
  - Citizens can use this electronic identity to log in to public-sector services
  - Optionally, log in at private-sector services is supported as well
- Distinguishing feature compared to private-sector IDPs like Google, Apple, etc.: Issued electronic identities are typically linked with national registers and data stored therein
- Example: Austrian national eID: **ID Austria**



# A First Glimpse at ID Austria

- ID Austria is the **official Austrian national eID**
- ID Austria has replaced recently its predecessors „Bürgerkarte“ and „Handy-Signatur“
- ID Austria provides Austrian citizens **2 main features**:
  - **Secure authentication** at service providers
  - Creation of **qualified electronic signatures** (legally equivalent to handwritten signatures)
- In contrast to its predecessors, ID Austria supports **fully mobile usage scenarios**




# ID Austria: Secure Authentication (Example)

## Willkommen bei FinanzOnline!

**Hinweis**

FinanzOnline wird laufend weiterentwickelt und verbessert. Nun ist FinanzOnline dank neuer Gestaltung noch userfreundlicher und individuell anpassbar. Alle Neuerungen und Funktionen werden in unserem Video unter [FinanzOnline - Neues Dashboard - YouTube](#) vorgestellt.

### Anmeldung mit ID Austria

 ID Austria

Diese sichere elektronische Anmeldung können Sie auch mit einer Signaturkarte, mit einem FIDO-Sicherheitsschlüssel oder dem EU-Login nutzen.

**Mit ID Austria anmelden**

[Wie funktioniert das?](#)

### Anmeldung mit Benutzername

**Achtung!** Diese ist erst nutzbar, wenn Sie bereits einen eindeutigen Benutzernamen in FinanzOnline festgelegt haben.

Benutzername

Passwort

**Anmelden**

[Passwort vergessen oder gesperrt](#)

[Welche Zugangskennungen kann ich nutzen?](#)

### Anmeldung mit Teilnehmer-Identifikation

Teilnehmer-Identifikation

Benutzer-Identifikation

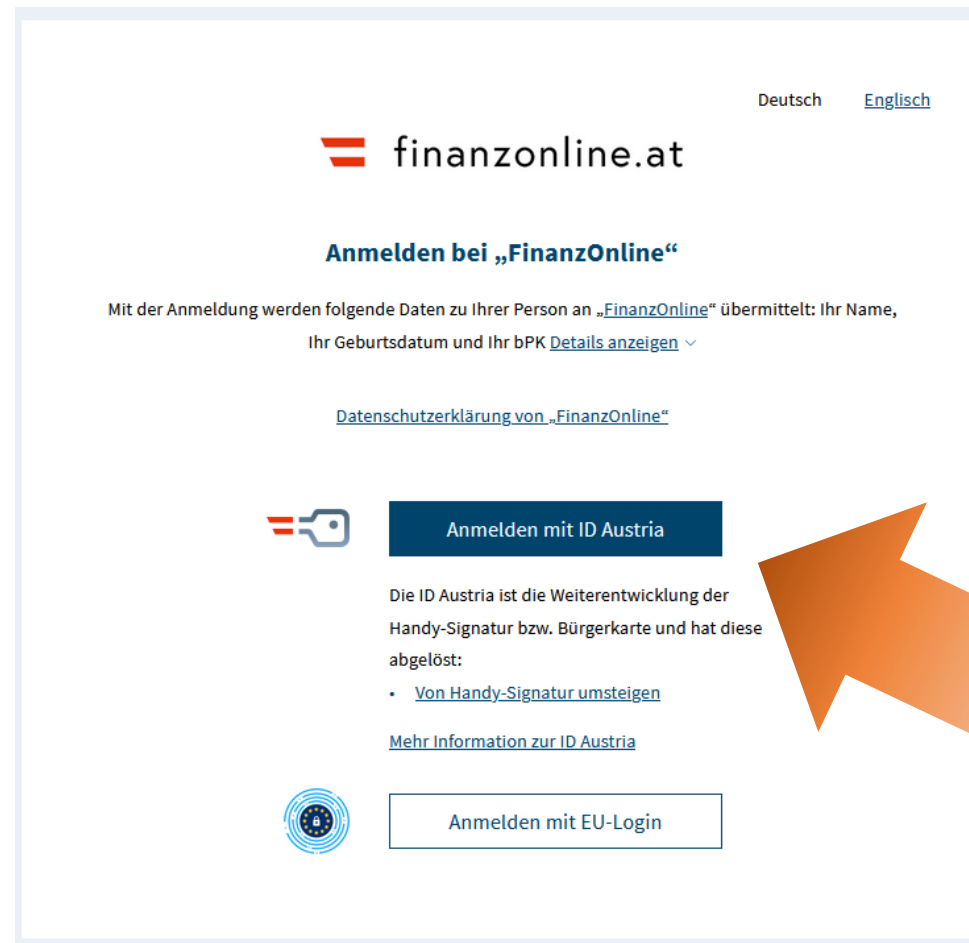
Passwort

**Anmelden**

[Passwort vergessen oder gesperrt](#)


[Welche Zugangskennungen kann ich nutzen?](#)

# ID Austria: Secure Authentication (Example)



The screenshot shows the login page for FinanzOnline. At the top right, there are language options for "Deutsch" and "Englisch". The main heading is "finanzonline.at". Below this, the title "Anmelden bei „FinanzOnline“" is displayed. A paragraph explains that registration data (name, birth date, and bPK details) will be transmitted to the user's profile. A link for the "Datenschutzerklärung von „FinanzOnline“" is provided. Two main login options are shown: "Anmelden mit ID Austria" (highlighted with a blue button and an orange arrow) and "Anmelden mit EU-Login" (in a white button). The ID Austria section includes a key icon, a description of ID Austria as a successor to mobile signatures and ID cards, and a link "Von Handy-Signatur umsteigen". The EU-Login section features the European Union flag icon.


Deutsch [Englisch](#)

 finanzonline.at

**Anmelden bei „FinanzOnline“**

Mit der Anmeldung werden folgende Daten zu Ihrer Person an „FinanzOnline“ übermittelt: Ihr Name,  
Ihr Geburtsdatum und Ihr bPK [Details anzeigen](#) ▾


[Datenschutzerklärung von „FinanzOnline“](#)

 **Anmelden mit ID Austria**

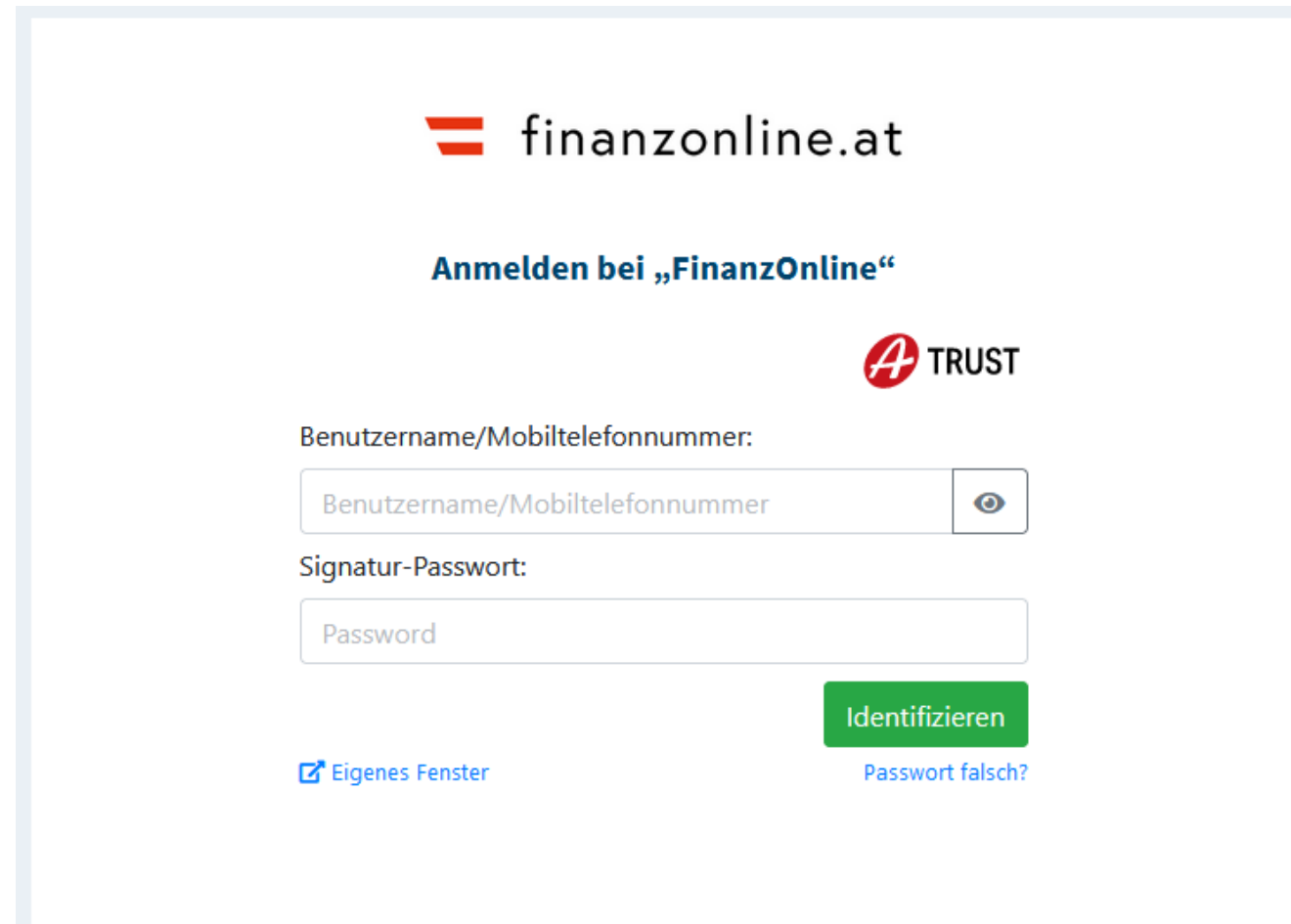
Die ID Austria ist die Weiterentwicklung der Handy-Signatur bzw. Bürgerkarte und hat diese abgelöst:


- [Von Handy-Signatur umsteigen](#)

[Mehr Information zur ID Austria](#)


 **Anmelden mit EU-Login**

# ID Austria: Secure Authentication (Example)



 finanzonline.at

**Anmelden bei „FinanzOnline“**

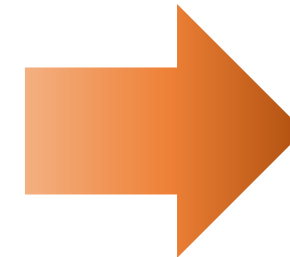
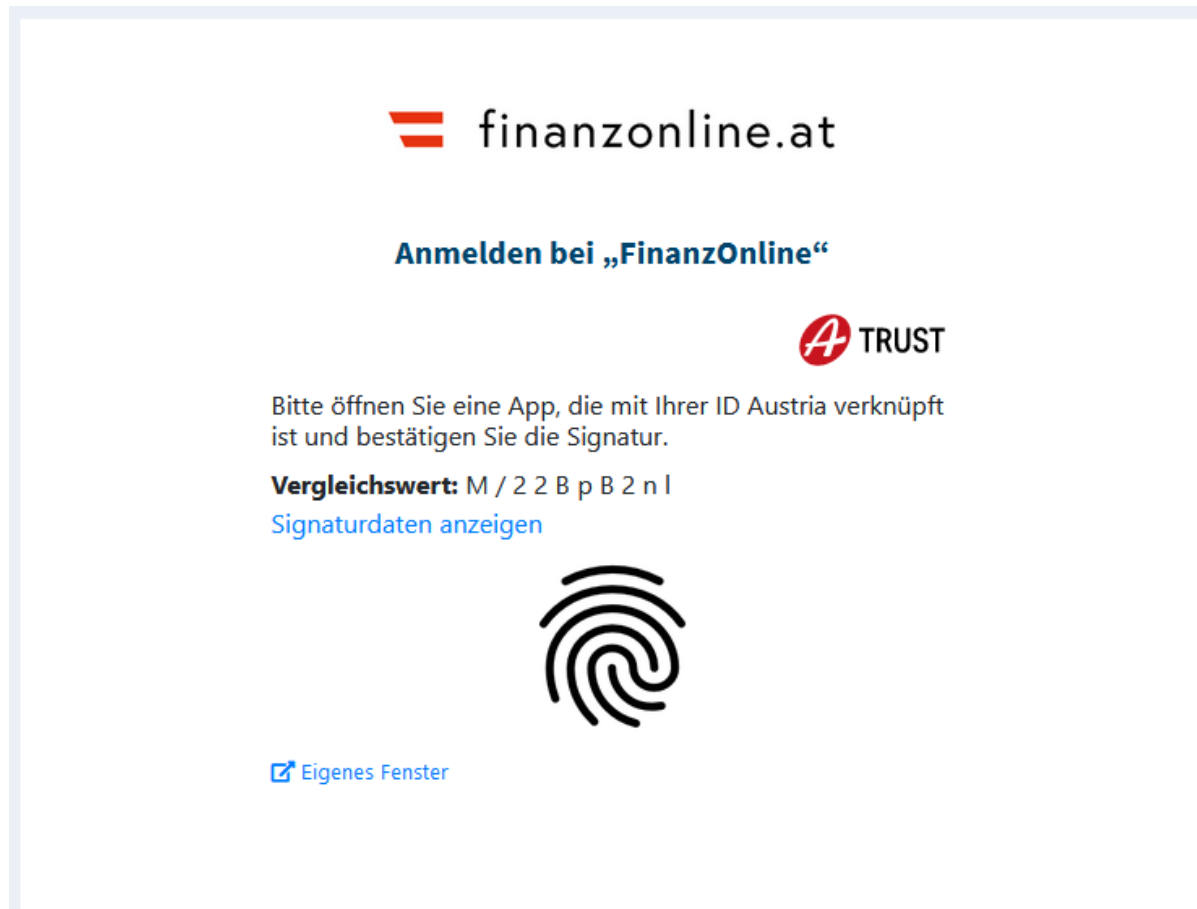


Benutzername/Mobiltelefonnummer:

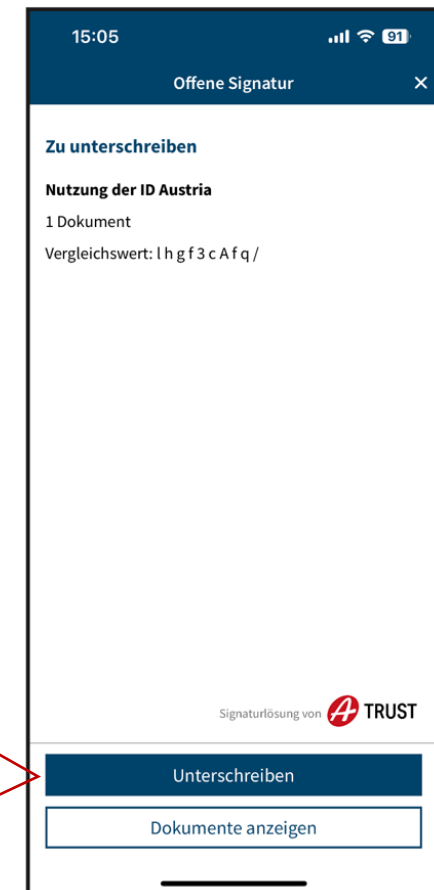
Signatur-Passwort:

[Eigenes Fenster](#) [Passwort falsch?](#)

# ID Austria: Secure Authentication (Example)

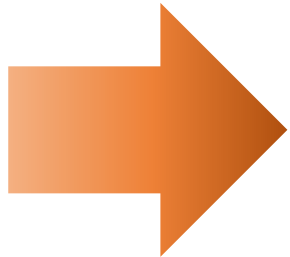


Authorize via  
biometrics





# ID Austria: Secure Authentication (Example)



finanzonline.at

Bundesministerium  
Finanzen

Abfragen ▾ Eingaben ▾ Weitere Services 🔍

Admin ▾ 📧 🖨️ 👤 ⏻

Teilnehmer\*in: Zefferer Thomas Benutzer\*in: Zefferer Thomas

22.02.2024 10:00 Uhr

20.02.2024  
07.02.2024

**Ihre letzten Steuererklärungen →**  
finden Sie auch unter WEITERE SERVICES - [Erklärungen](#)

Steuerjahr 2023

Steuerjahr 2022

**Nachrichten behördlich →**

**Nachrichten persönlich →**  
Keine Einträge vorhanden

# ID Austria: Secure Authentication (Example)

- Example has shown a 2-device usage scenario
  - Access service provider (finanzonline.gv.at) via web browser on PC/laptop
  - Use mobile device as second factor (possession, inherence) during authentication
- ID Austria also supports single-device (mobile only) usage scenarios
- So far, we have focused on the user perspective only – we will have a more technical look at ID Austria in one of the next lectures (June)

# Take-Home Messages

- Identity management is crucial to enable personalized online services
- From a technical perspective, user authentication is one of the most challenging parts in identity management
- Various approaches/models exist to implement identity management in practice, each coming with its specific pros and cons
- The identity provider plays a crucial role in all these models
- Trust in the identity provider is highly relevant for all involved entities

# Identity Management Systems

## Questions & Answers

Dr. Thomas Zefferer

*Summer Term 2025*