ID Austria
and
eIDAS-based Cross-Border Authentication

Lecture „Secure Application Design“

Dr. Thomas Zefferer

Summer Term 2025

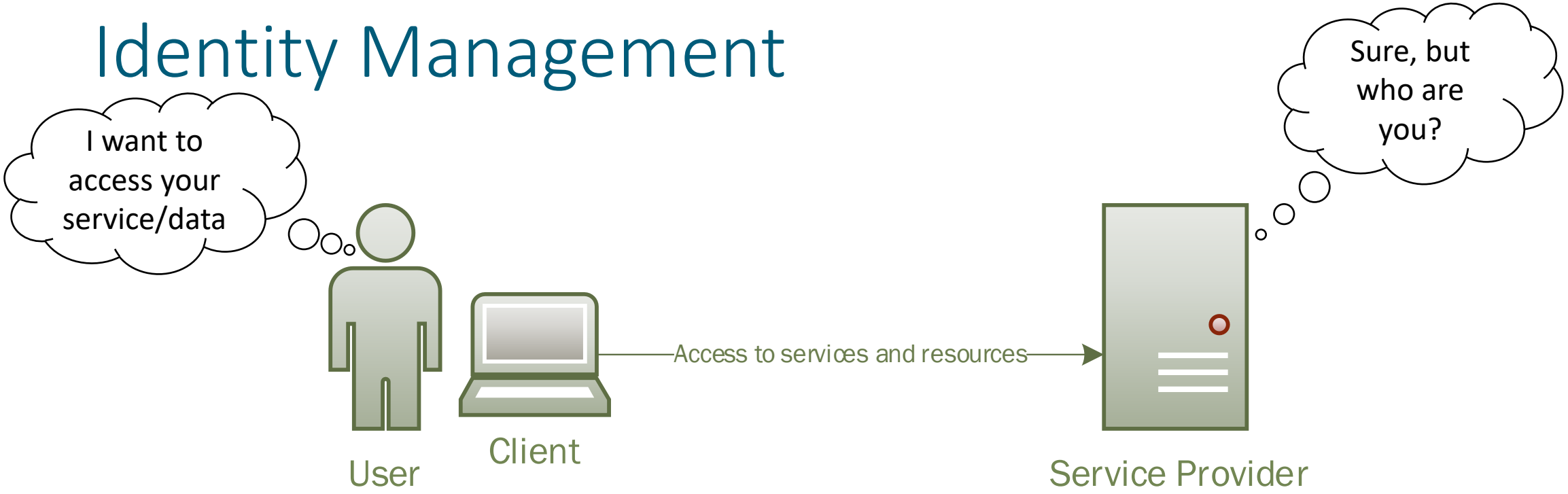
Topics for Today‘s Lecture

- **Goal:** Understand how identity management is done in practice
- **Use Case 1:** National identity management in Austria: ID Austria
- **Use Case 2:** Cross-border national identity management in Europe: The Technical eIDAS Interoperability Framework

Before we get started:

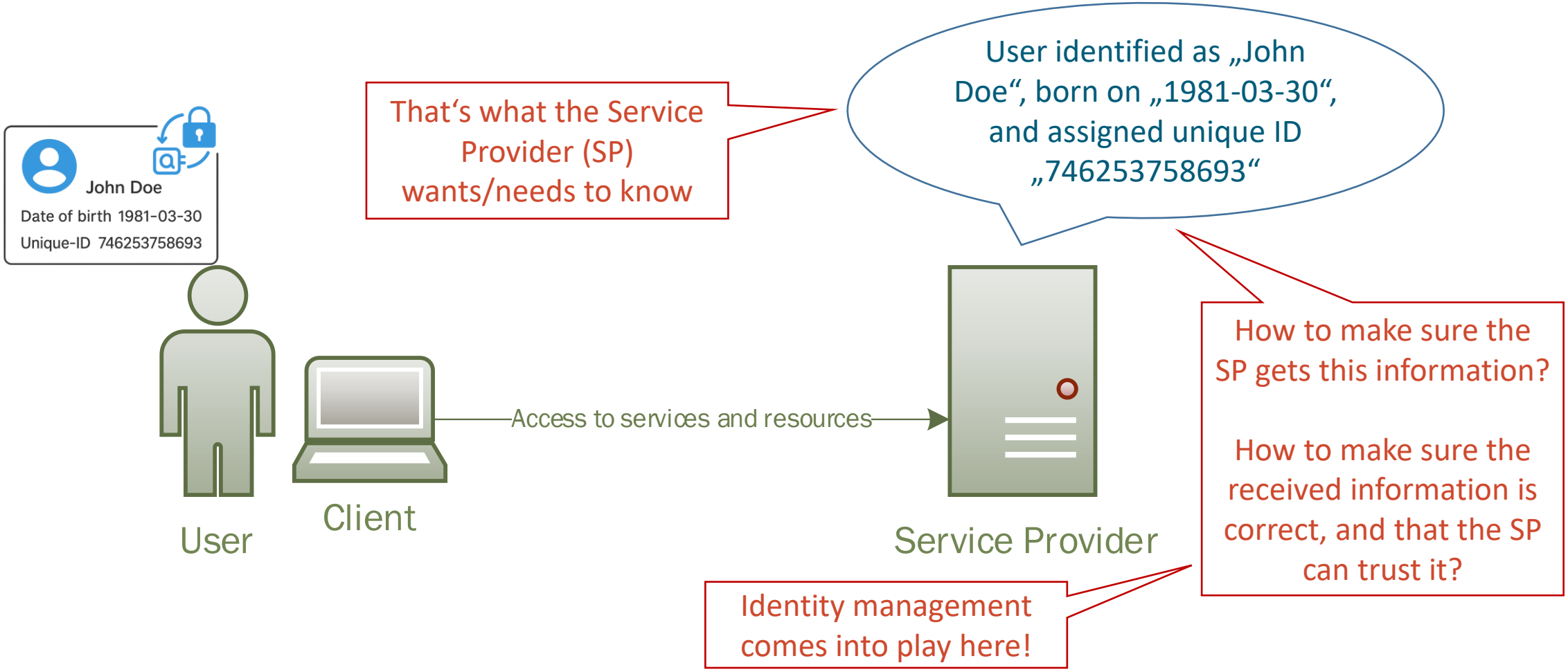
Brief recap of identity management systems (lecture from April 4th, 2025)

Identity Management

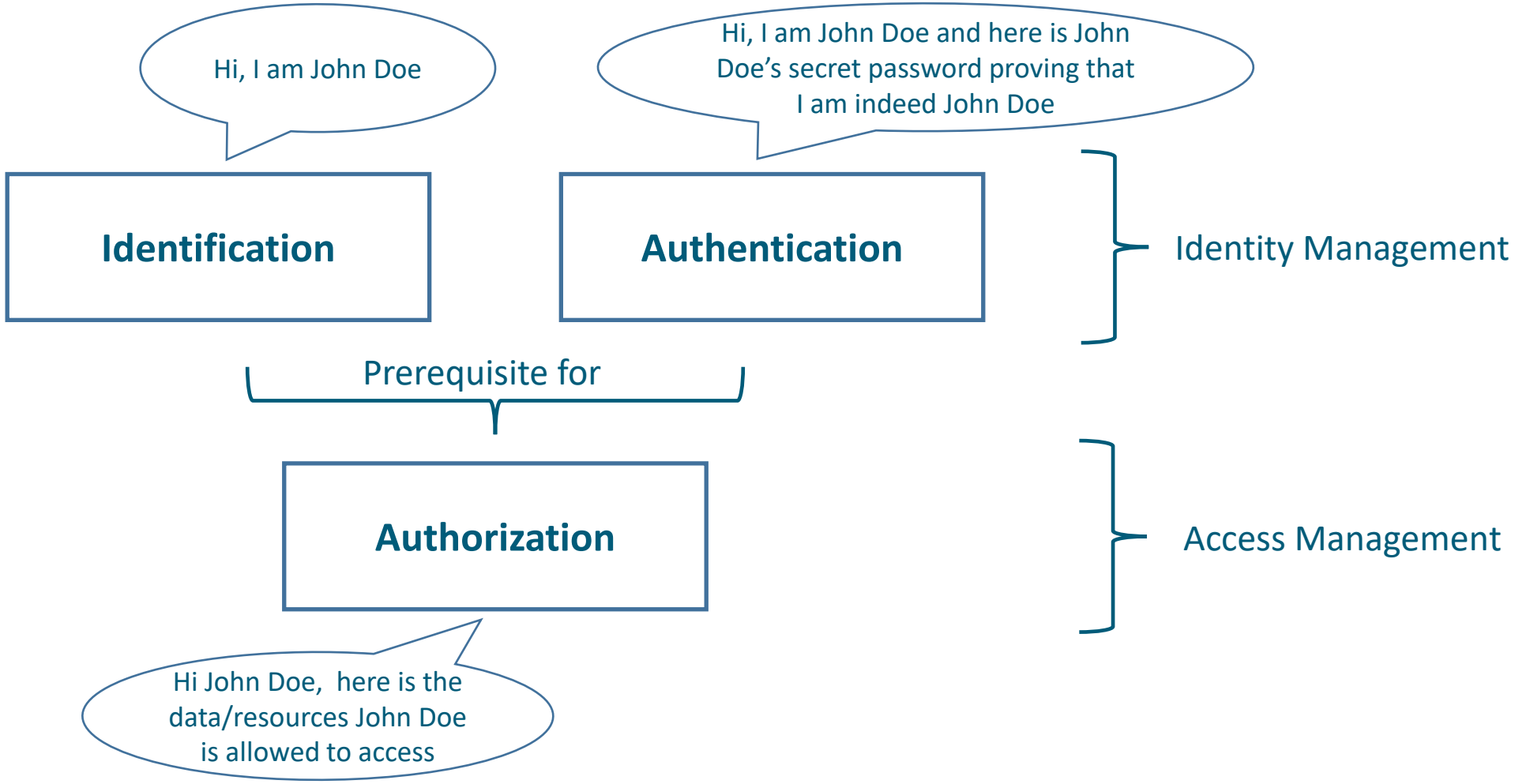


Goal: An IT system („Service Provider“) needs to know the identity of the user, e.g., to decide whether the user is granted access to certain resources (service, data, etc.)

Electronic Identity: Simple Example



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**

Categories of Authentication Factors

- **Knowledge factors:** *„Something you know“*
  - Password
  - PIN
  - …
- **Possession factors:** *„Something you have“*
  - FIDO Token
  - Smart card
  - Smartphone
  - …
- **Inherence factors:** *„Something you are“*
  - Fingerprint
  - Iris scan
  - Behavior (sometimes seen as separate category)
  - …

+ 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

+ 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

+ 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

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

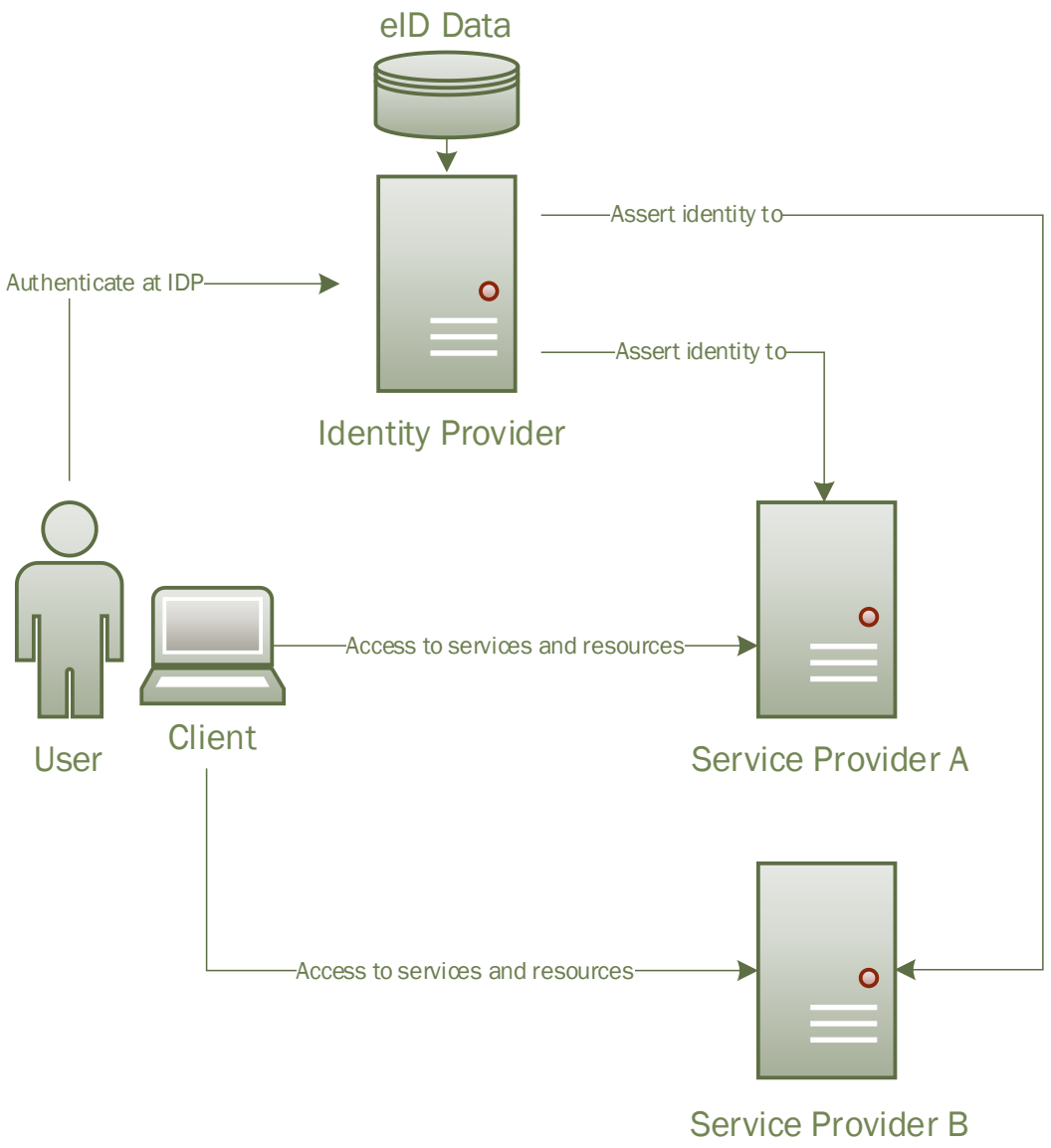
- Different approaches/models to cope with this challenge[1]
  - Isolated model
  - Central model
  - User-centric model
  - Federated model
  - …

- 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

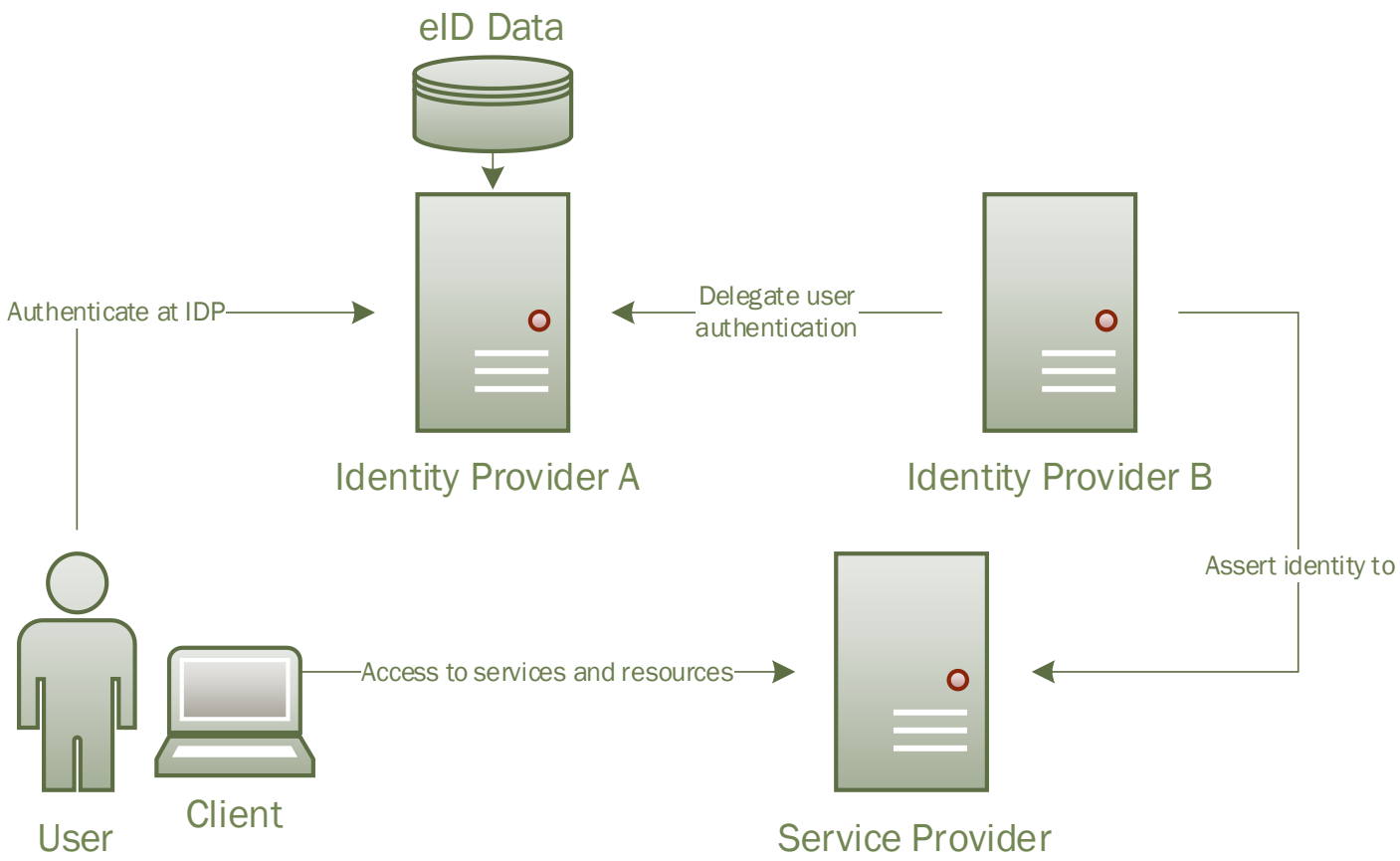
Central Model

- 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



Federated Model

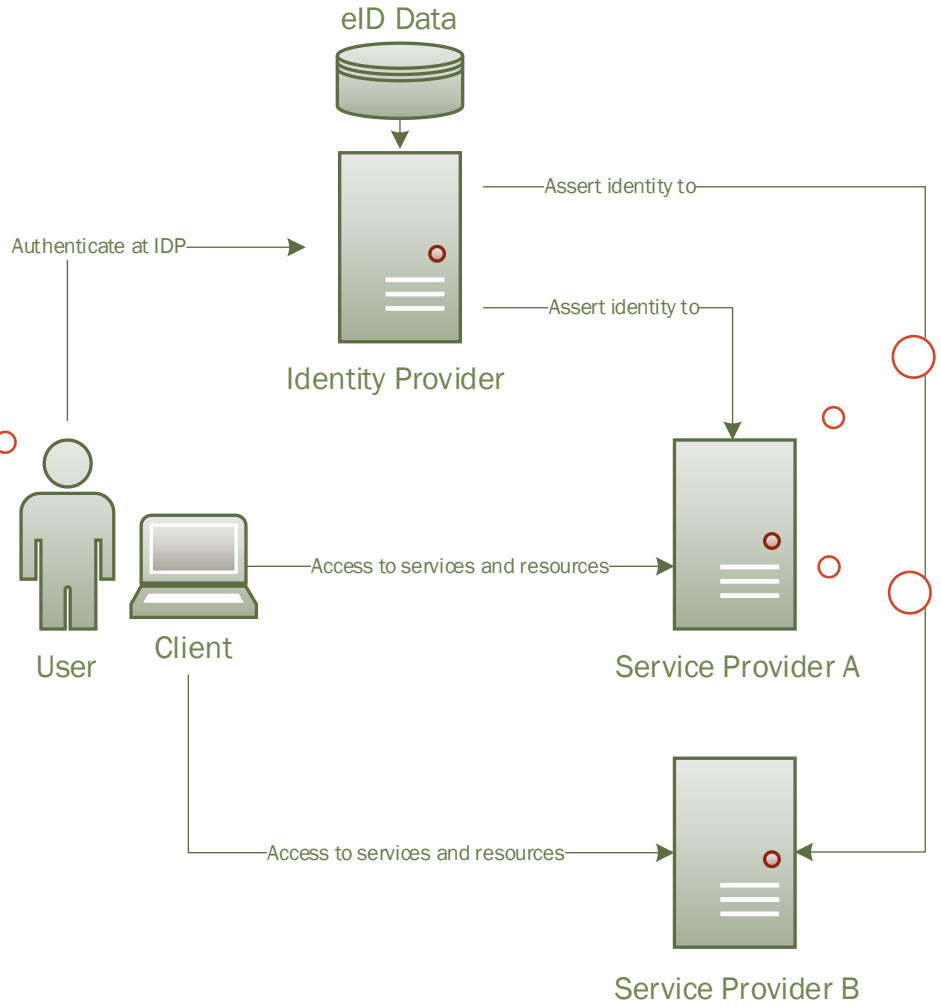
- Multiple IDPs in place, which can delegate user authentication among each other
- Trust between IDPs is crucial
- Pros:
  - Allows for large cross-domain use cases
- Cons:
  - Trust management between IDPs needed



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?

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**

Topics for Today‘s Lecture

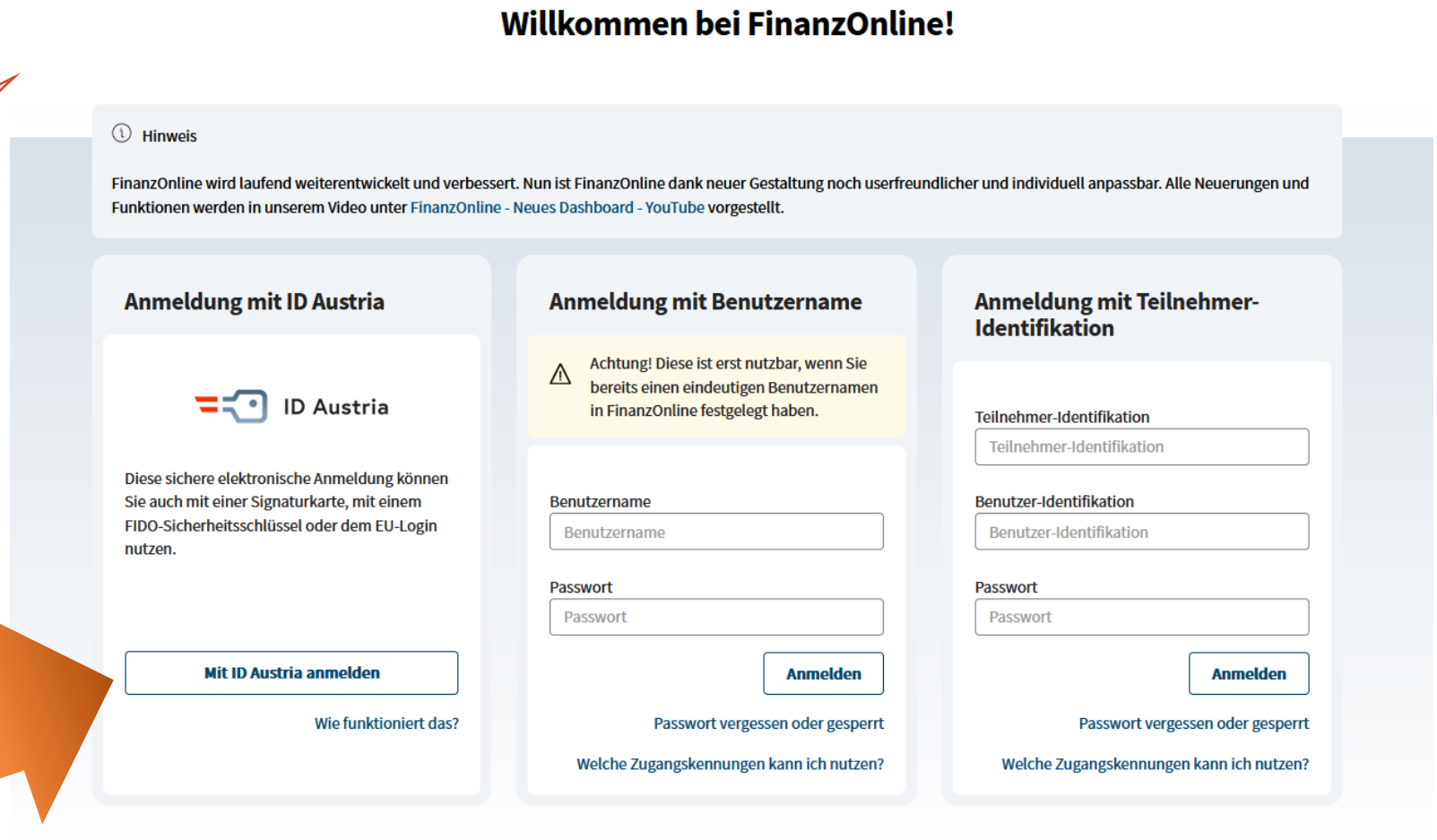
- **Goal:** Understand how identity management is done in practice
- **Use Case 1:** National identity management in Austria: ID Austria
- **Use Case 2:** Cross-border national identity management in Europe: The Technical eIDAS Interoperability Framework

Use Case 1: National identity management in Austria:

ID Austria

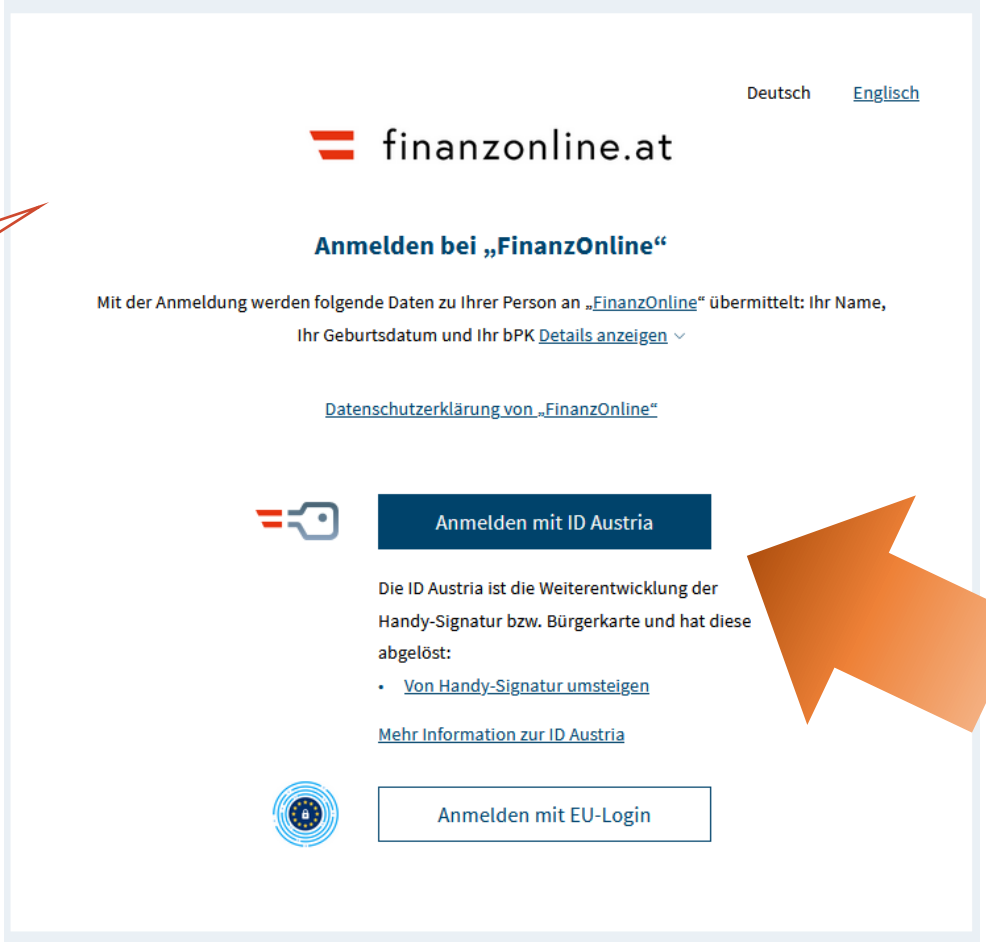
ID Austria: The User Perspective (Example)

Service-Provider Domain (FinanzOnline)



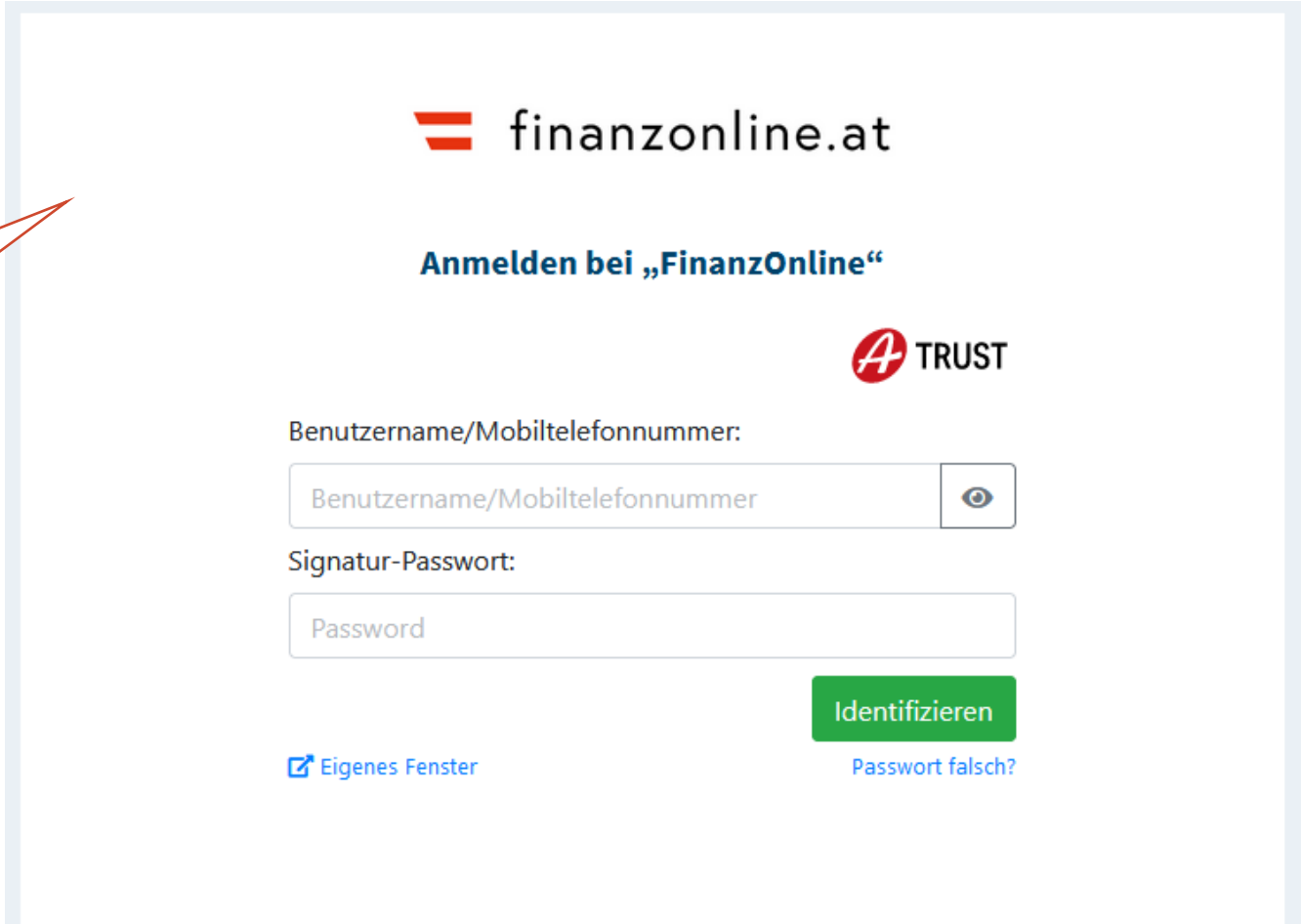
ID Austria: The User Perspective (Example)

ID Austria Domain

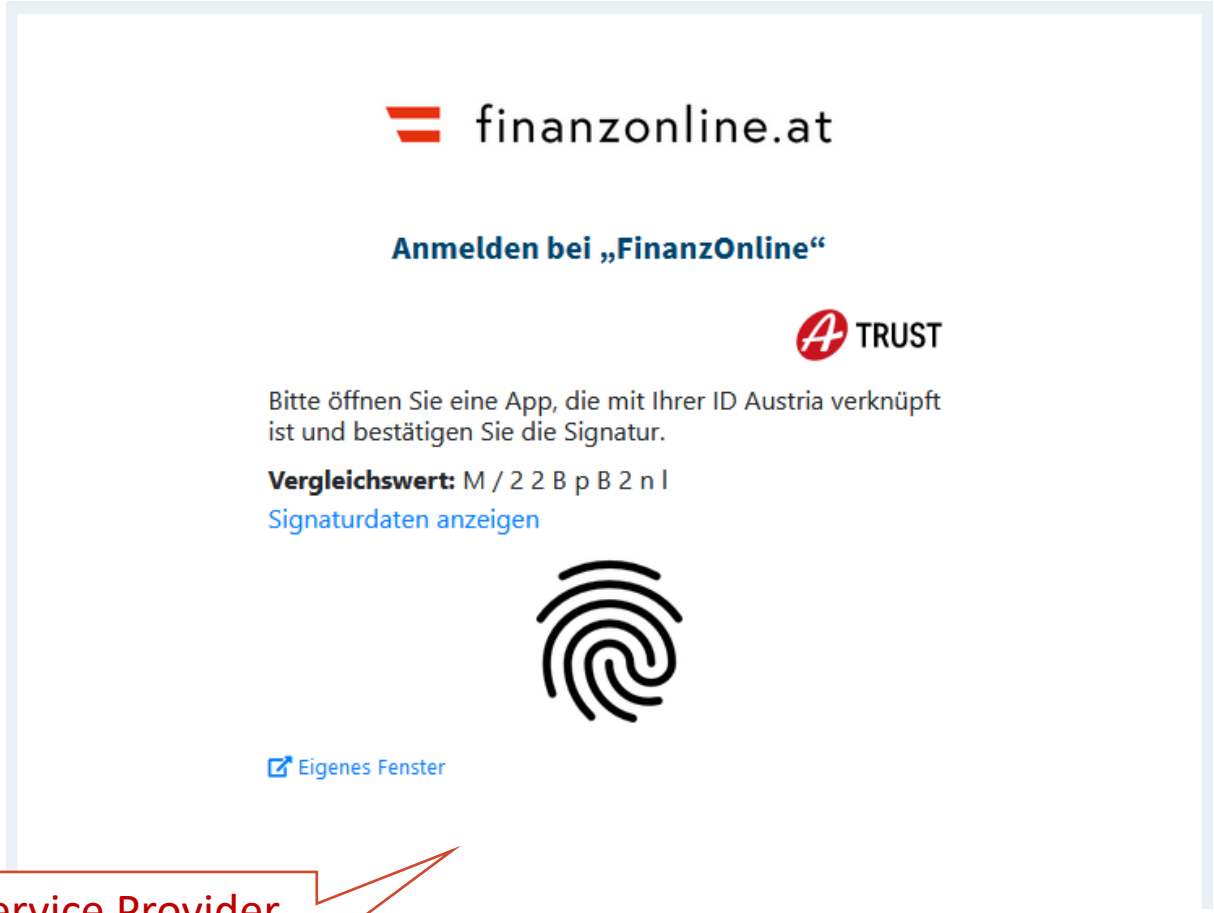


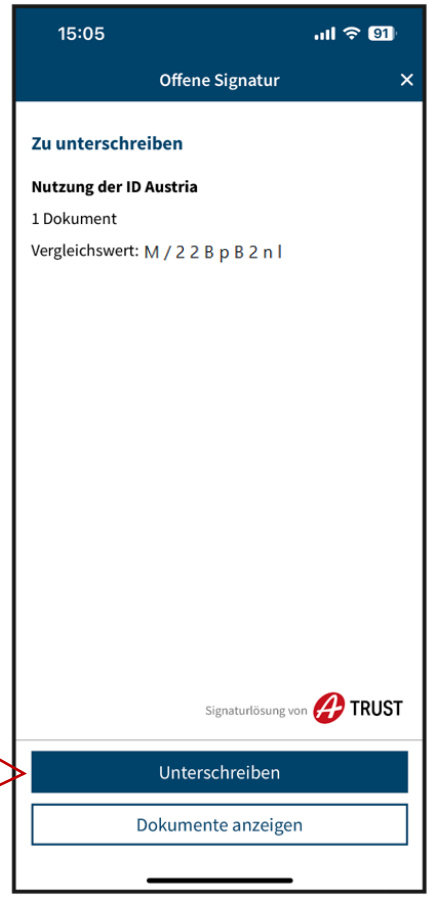
ID Austria: The User Perspective (Example)

Trust Service Provider Domain (A-Trust)



ID Austria: The User Perspective (Example)

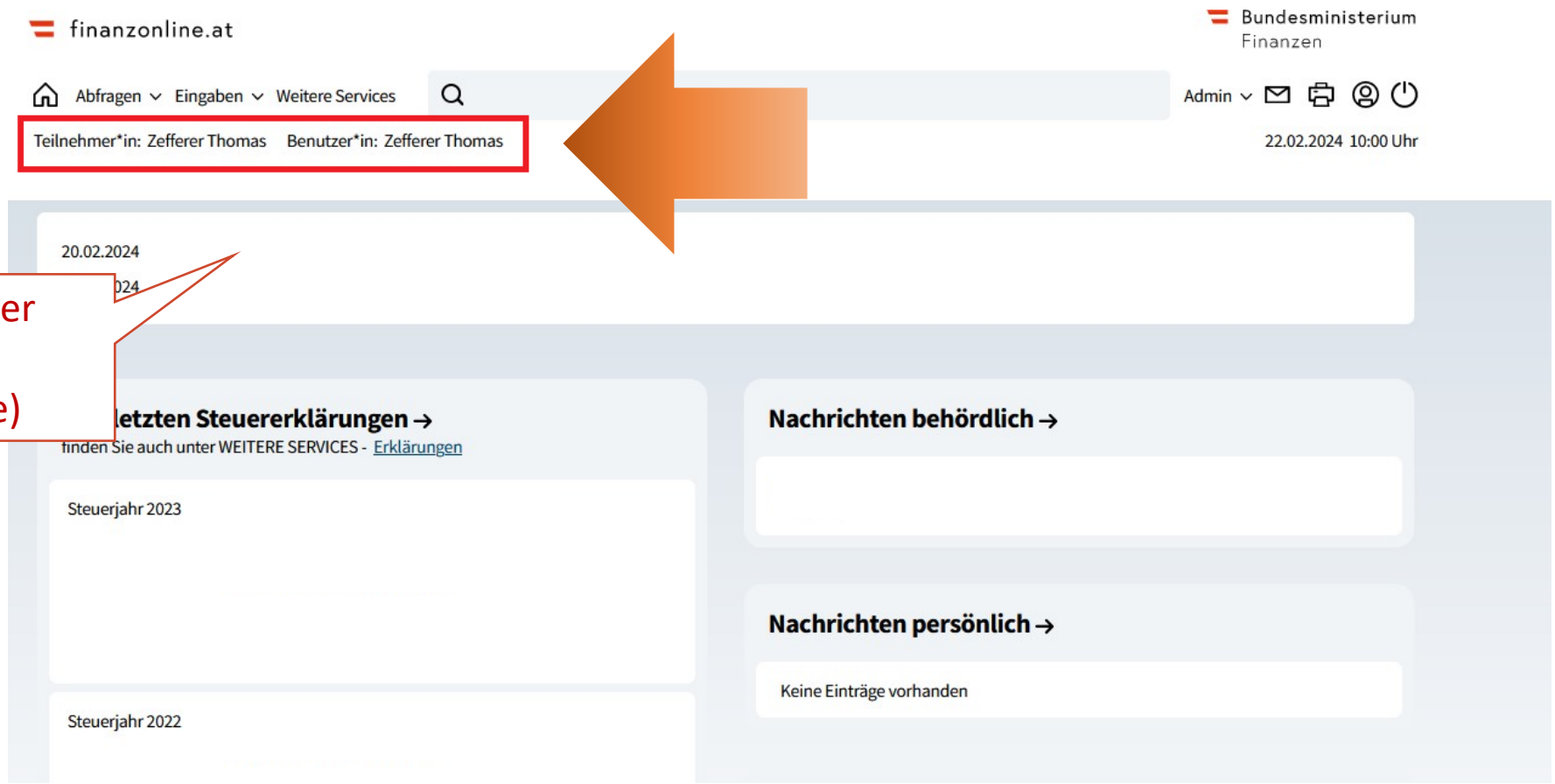




Authorize via biometrics

Trust Service Provider Domain (A-Trust)

ID Austria: The User Perspective (Example)



Service Provider Domain (FinanzOnline)

ID Austria: Under the Hood

- The previous slides have shown the user‘s perspective, i.e., what the user sees and does during an ID-Austria-based authentication process

- And now let’s have a look under the hood, focusing on:
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

ID Austria: Identity Data (Attributes)

- First and foremost: How does an electronic identity provided by ID Austria look like?
- In other words: Which identity data ("identity attributes") does a service provider obtain from ID Austria after a successful user-authentication process?

ID Austria

Minimum Data Set (MDS)

First name: Max
Family name: Mustermann
Date of birth: 30.03.1981
Source PIN: 869373648592

Optional Attributes

Gender: M
Signature: [Image]
Nationality: AT
[…and some more]

Data available for user Max Mustermann (Example)

ID Austria

Minimum Data Set (MDS)

First name: Max
Family name: Mustermann
Date of birth: 30.03.1981
Sector-specific PIN: 455486741599

Optional Attributes

Gender: M

Data provided to SP (Example)

ID Austria: Identity Data (Attributes)

ID Austria

Minimum Data Set (MDS)

First name: Max
Family name: Mustermann
Date of birth: 30.03.1981
Source PIN: 869373648592

Optional Attributes

Gender: M
Signature: [Image]
Nationality: AT
[…and some more]

Data available for user Max Mustermann (Example)

ID Austria

Minimum Data Set (MDS)

First name: Max
Family name: Mustermann
Date of birth: 30.03.1981
Sector-specific PIN: 455486741599

Optional Attributes

Gender: M

Data provided to SP (Example)

- Service providers always receive the MDS
- **But:** Service providers do never receive the user's Source PIN but a derived unique identifier (sector-specific PIN)
- The set of optional attributes sent depends on the service provider and its privileges (determined during registration of the SP)

A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

ID Austria: Unique Identifiers

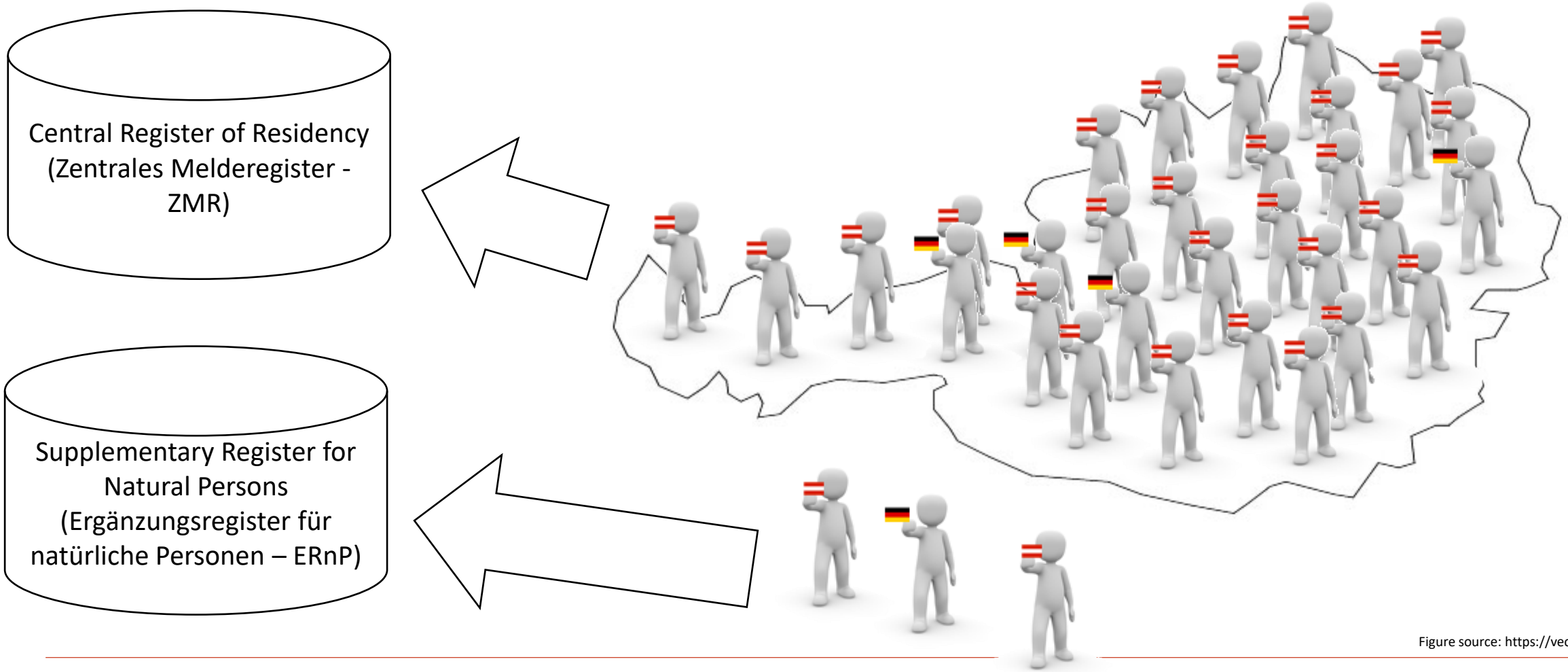


Figure source: https://vectorportal.com

ID Austria: Unique Identifiers

- Each person registered in the ZMR or ERnP is internally assigned a unique number
- Electronic identities issued in Austria are unambiguously linked to the respective number in the two registers
  - **Note:** Link to the number does **NOT** imply that this number is used directly as unique identifier in eIDs
- This requires that the person is identified reliably (e.g., using a passport) before an electronic identity is issued

ID Austria

Minimum Data Set (MDS)

First name: Max
Family name: Mustermann
Date of birth: 30.03.1981
Source PIN: 869373648592

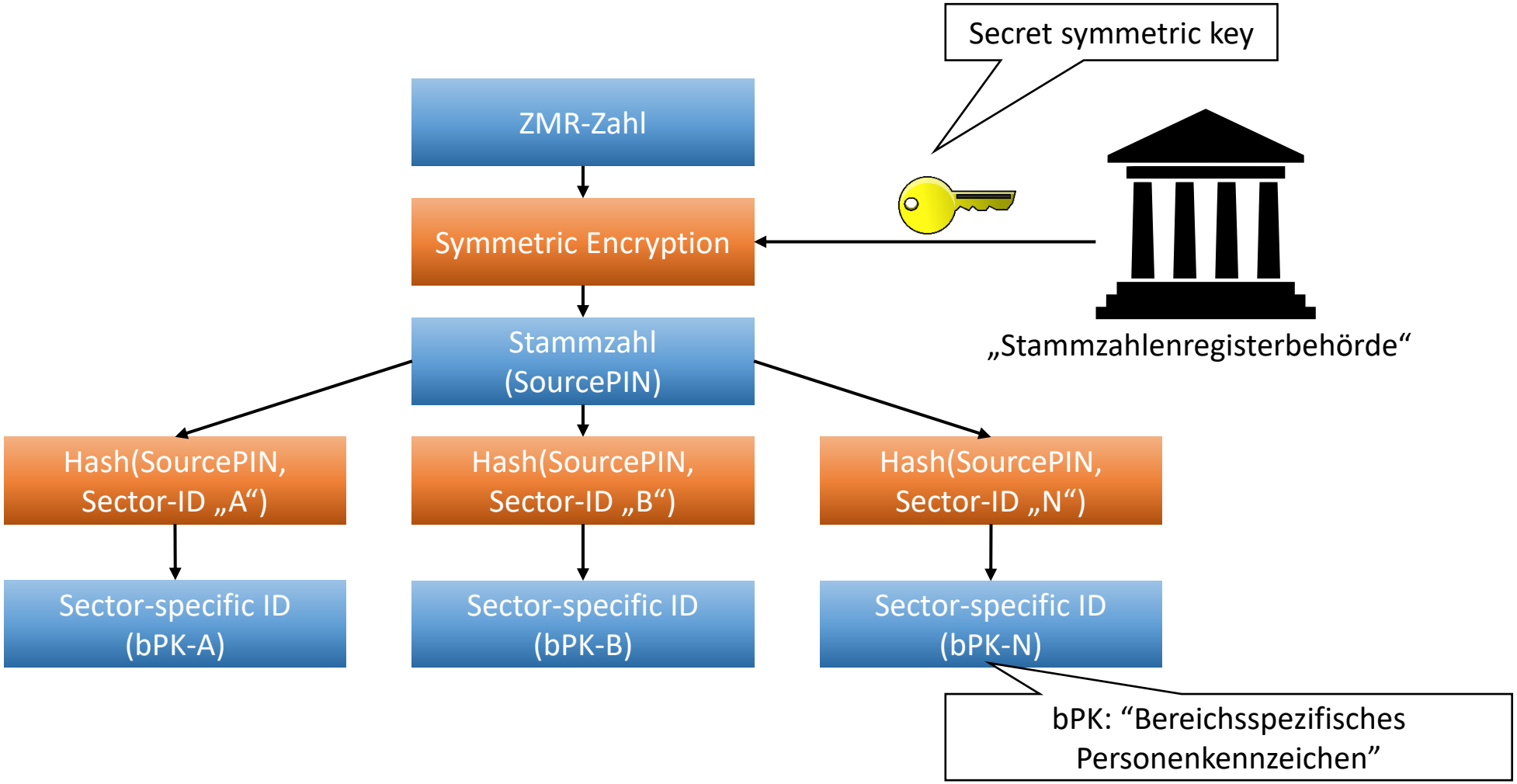
ID Austria

Minimum Data Set (MDS)

First name: Ella
Family name: Musterfrau
Date of birth: 11.03.1993
Source PIN: 945375933363

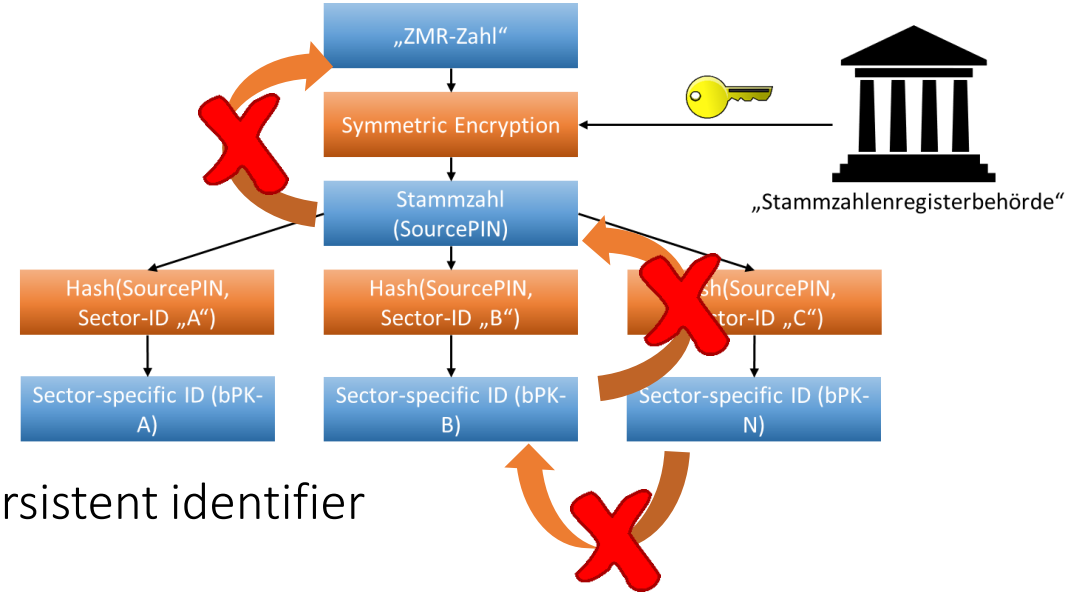
Unique identifier linked to the person‘s entry in the ZMR or ERnP

ID Austria: Unique Identifiers

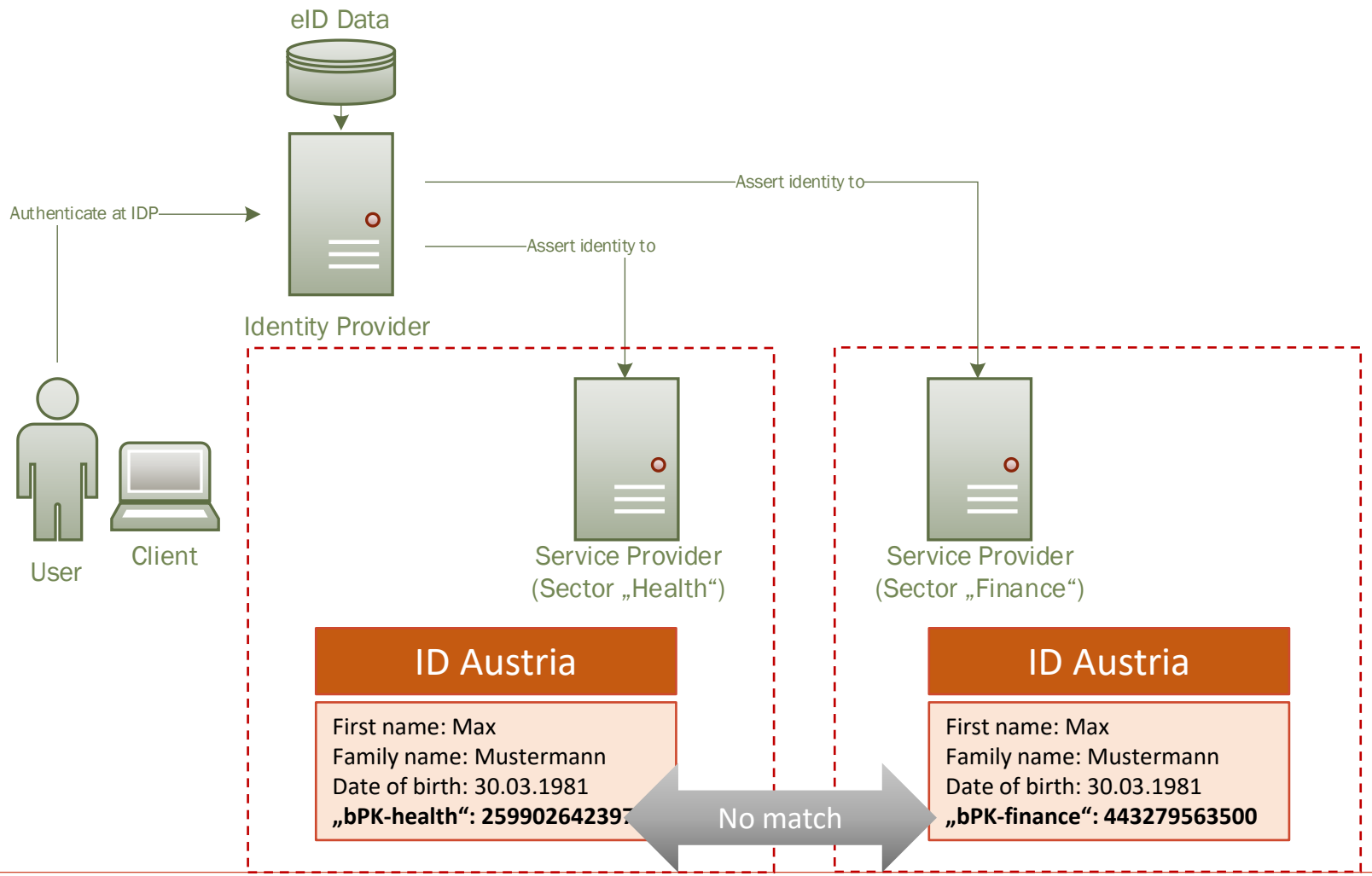


ID Austria: Unique Identifiers

- From the obtained sector-specific identifier (bPK) of a certain sector, no bPKs of other sectors can be computed
- From the obtained sector-specific identifier (bPK), the user‘s SourcePIN cannot be deduced
- Only the „Stammzahlenregisterbehörde“ can compute the ZMR-Zahl for a given Stammzahl (SourcePIN)
- Service Providers from different sectors cannot match their user records
- Service Providers cannot learn the user‘s Stammzahl (or ZMR-Zahl), still they are provided with a unique and persistent identifier



ID Austria: Unique Identifiers



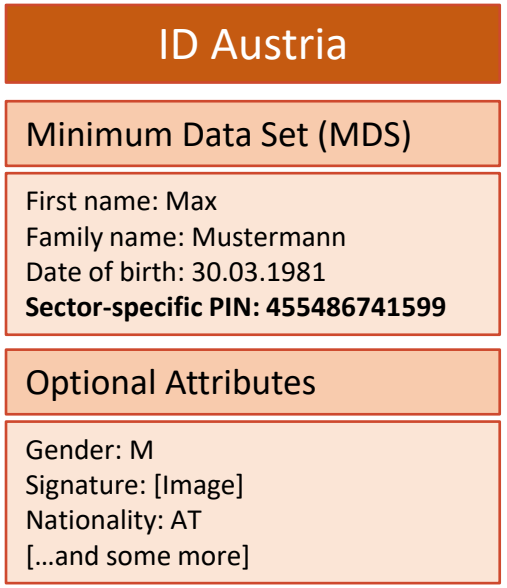
A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

ID Austria

- So far, we mainly know **WHAT** the ID Austria provides service providers
  - Which identity data/attributes
  - What kind of unique identifier



- Next, let's see **HOW** the ID Austria accomplishes that

Legal Requirements (Overview)

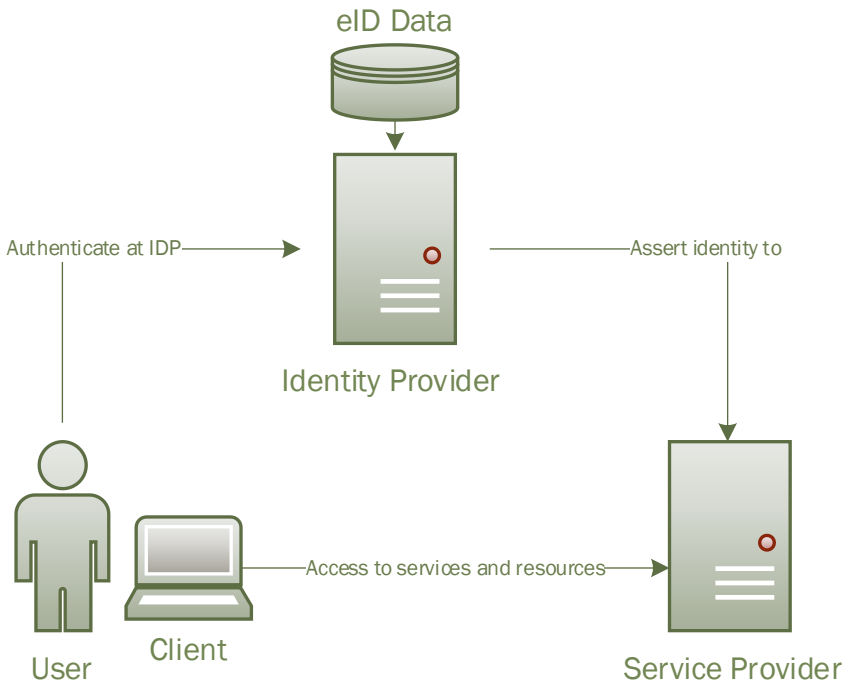
- National identity management systems and their implementation build on a legal basis

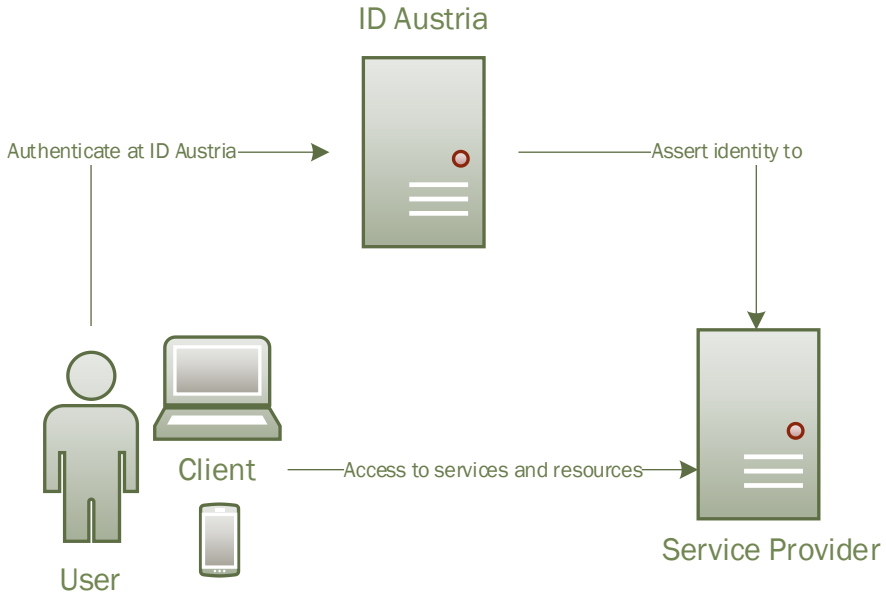
- In most cases, several laws, regulations, etc. need to be considered
  - On national level
  - On EU level

- (Some) legal provisions relevant for ID Austria:
  - Austrian E-Government Act
  - EU eIDAS Regulation
  - EU GDPR
  - …

§

Technical Architecture – High-Level

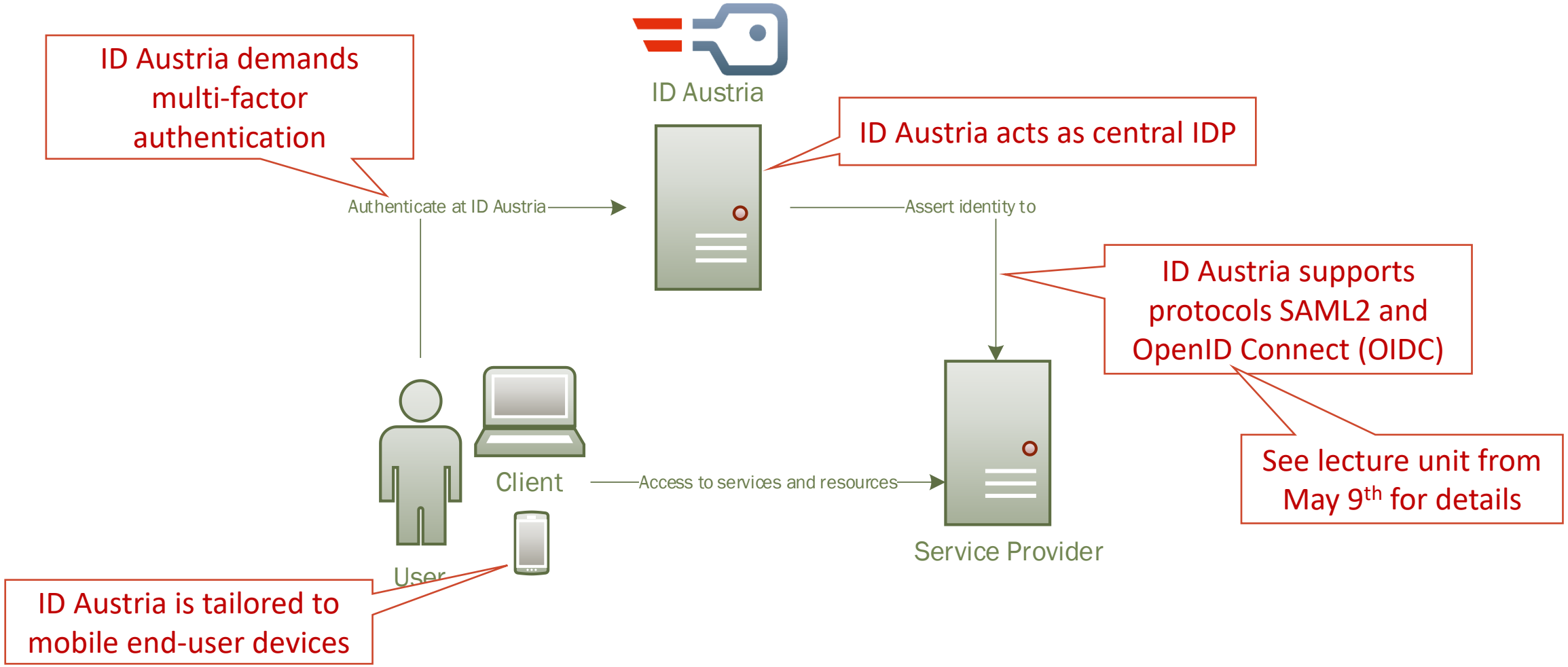




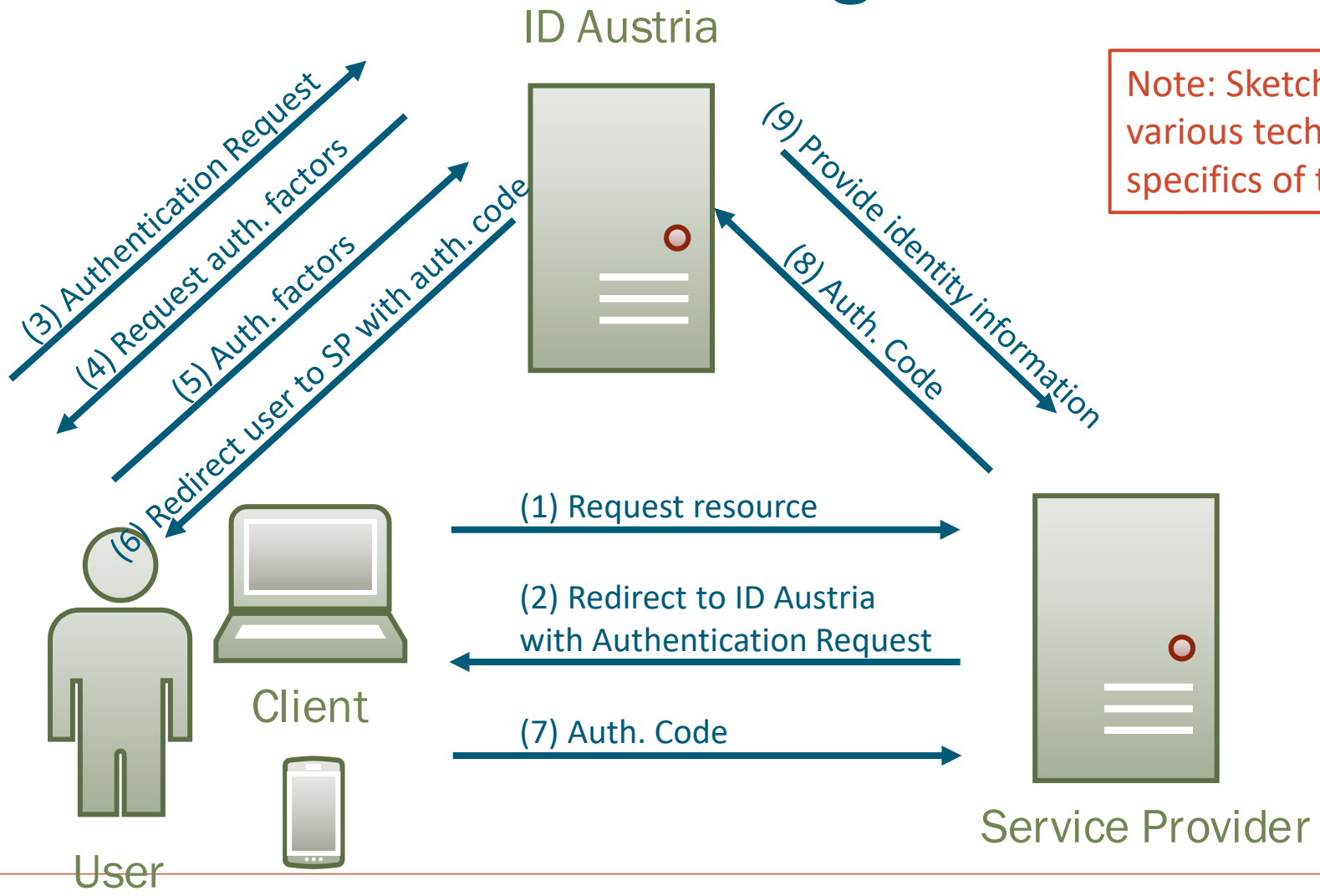
Central IDM Model

ID Austria

Technical Architecture – High-Level



Authentication Process – High-Level



Note: Sketched process flow omits various technical details and specifics of the used protocol

Other Relevant Processes

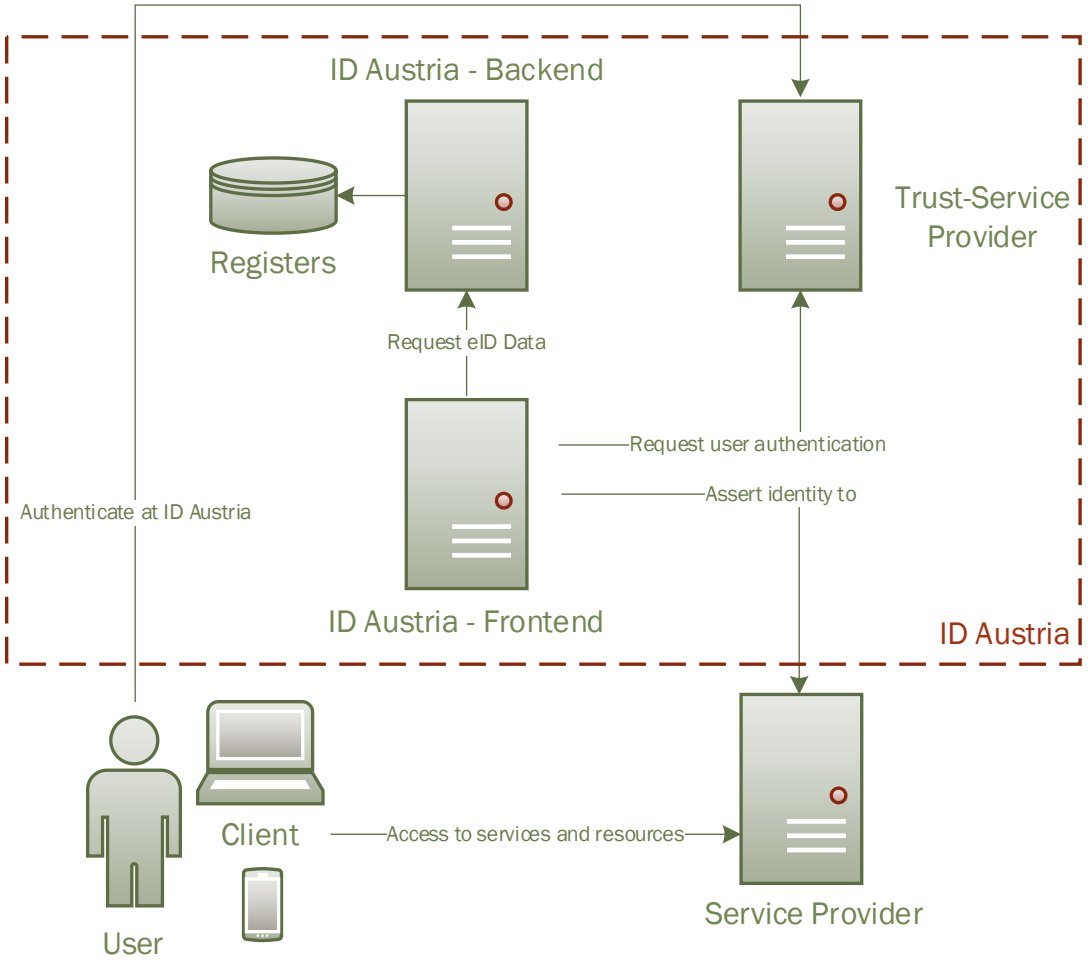
- Other relevant processes missing?
  - Registration
  - Revocation
  - Signature Creation
  - …
- What happens inside the ID Austria building block?

Out of scope for today, but nevertheless highly important

Let’s have a look!

Technical Architecture – Internals

- **IDA-Frontend** serves as contact point for Service Providers
- **IDA-Backend** provides eID data from national registers
- **Trust Service Provider** implements user authentication



A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

23.02.2024 A-SIT Plus GmbH 9

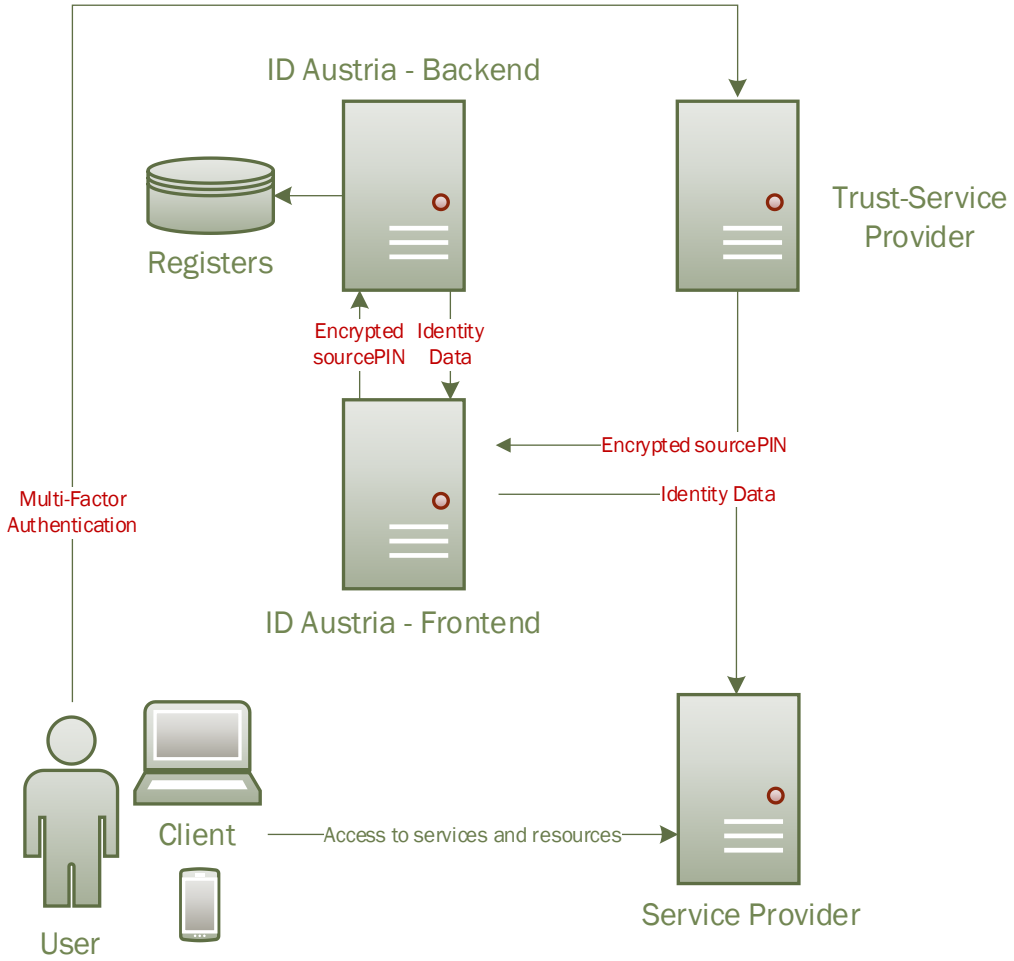
Underlying Concepts: Divide of Responsibility

- Internal architecture of ID Austria reflect 3 main involved parties responsible for its operation:
  - Federal Chancellery (BKA)/Federal Processing Center (BRZ): IDA Frontend
  - Ministry of the Interior (BMI): IDA Backend
  - A-Trust: Trust Service Provider

- Responsibilities are mostly defined by relevant legal basis

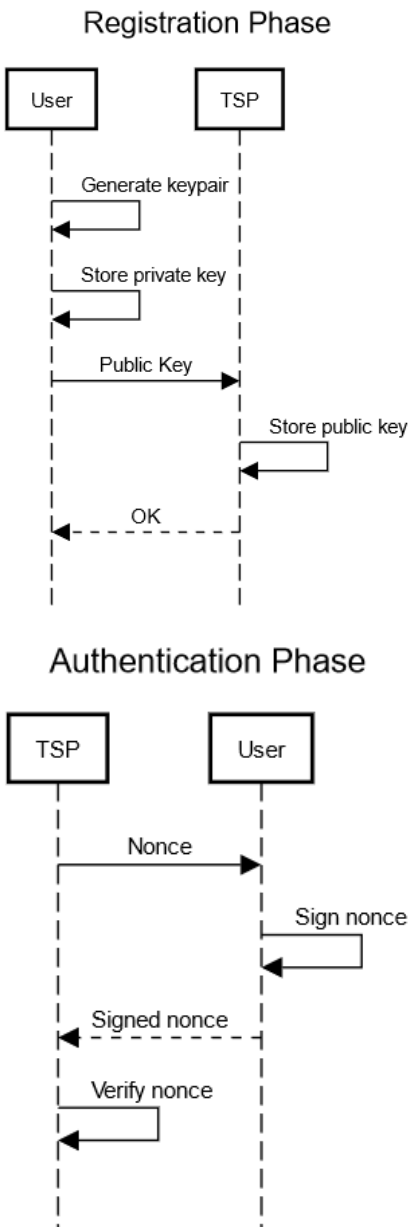
Underlying Concepts: Authentication

- For basics on user authentication see previous lecture units on authentication and on identity management systems
- At ID Austria, user is authenticated by Trust Service Provider (TSP)
- Authentication at TSP is always multi-factor
  - Knowledge (password)
  - Possession (smartphone, FIDO token, etc.)
    - Inherence (<u>local</u> authentication at smartphone with, e.g., fingerprint)
- TSP attests user's identity towards IDA Frontend
  - Attestation contains the user's <u>encrypted</u> SourcePIN
  - Encrypted SourcePIN is then sent to IDA Backend, which decrypts it, and fetches required data from registers (encrypted SourcePIN is stored at TSP during registration/enrolment)



Underlying Concepts: Authentication

- Use of authentication factor “possession” requires cryptographic methods
- During registration, an asymmetric key pair is created on the user’s smartphone
  - Private key never leaves the smartphone and is securely stored in the device’s key store
  - Public key is stored by TSP as reference value
- During authentication, TSP sends a challenge (e.g., a nonce) to the smartphone
- Challenge is signed by using the securely stored private key
  - Key usage is locally authorized with fingerprint/face ID
- Signed challenge is returned and verified by TSP using the stored reference value (public key)
- Proven ability to use private key proves possession of smartphone

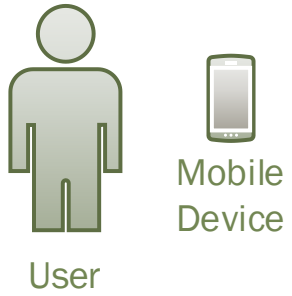


Underlying Concepts: SP Registration

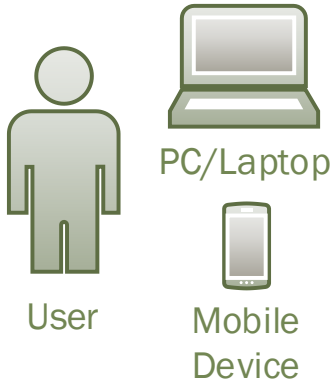
- Who can actually act as Service Provider?
  - In other words: Which applications may use ID Austria as IDP to authenticate users?
- In general: Every online service (public and private sector)
  - Note: For private-sector SPs, each SP gets its own bPK, i.e., each private SP forms its own sector
- SPs that want to use ID Austria need to be registered and accredited
- During accreditation, legitimacy of SP is verified
  - Prevents that user data is sent to dubious applications

Underlying Concepts: Mobile-First Strategy

- ID Austria supports mobile-only use-cases
  - Mobile device is used to access service provider and the same device is also used to authenticate at ID Austria



- ID Austria supports cross-device use-cases
  - A PC or laptop is used to access a service provider
  - An additional mobile device is used to authenticate at ID Austria



- This distinguishes ID Austria from its predecessors like Handy-Signatur, which did not support mobile-only use cases

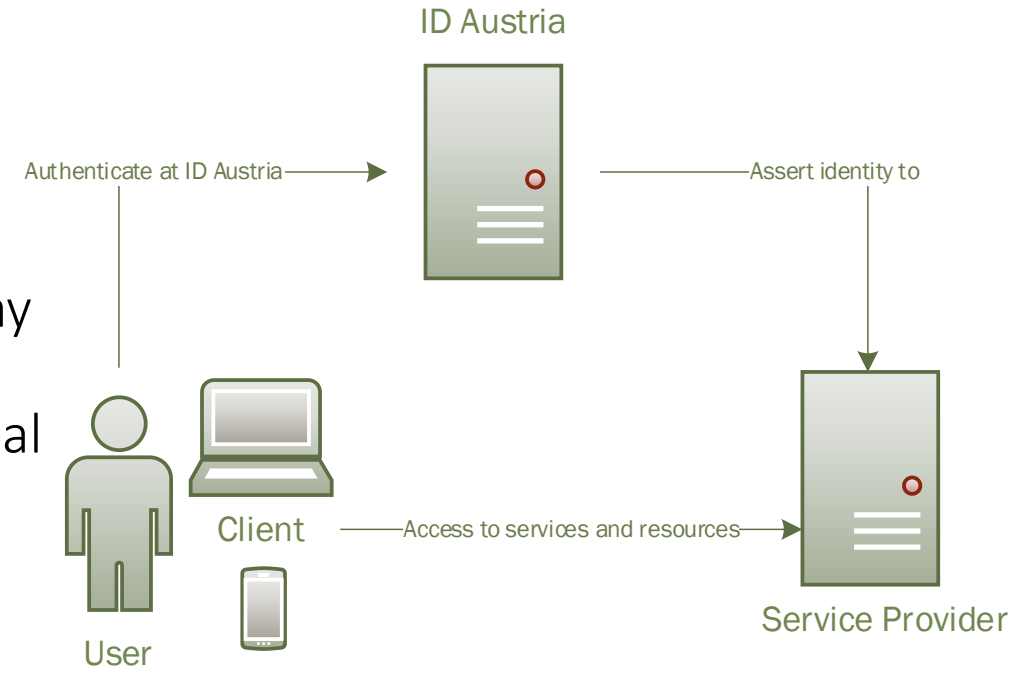
A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

ID Austria: Future Directions

- ID Austria follows the central identity-management model
- Pros:
  - Single point of contact for SPs
  - Central management of privileges (e.g., which SP may obtain which user attributes)
  - All authentication functionality is provided by external component (from the SP's perspective)
- Cons:
  - Single point of failure
  - Central IDP learns all user authentications (user tracking)



Future Directions: Towards Identity Wallets

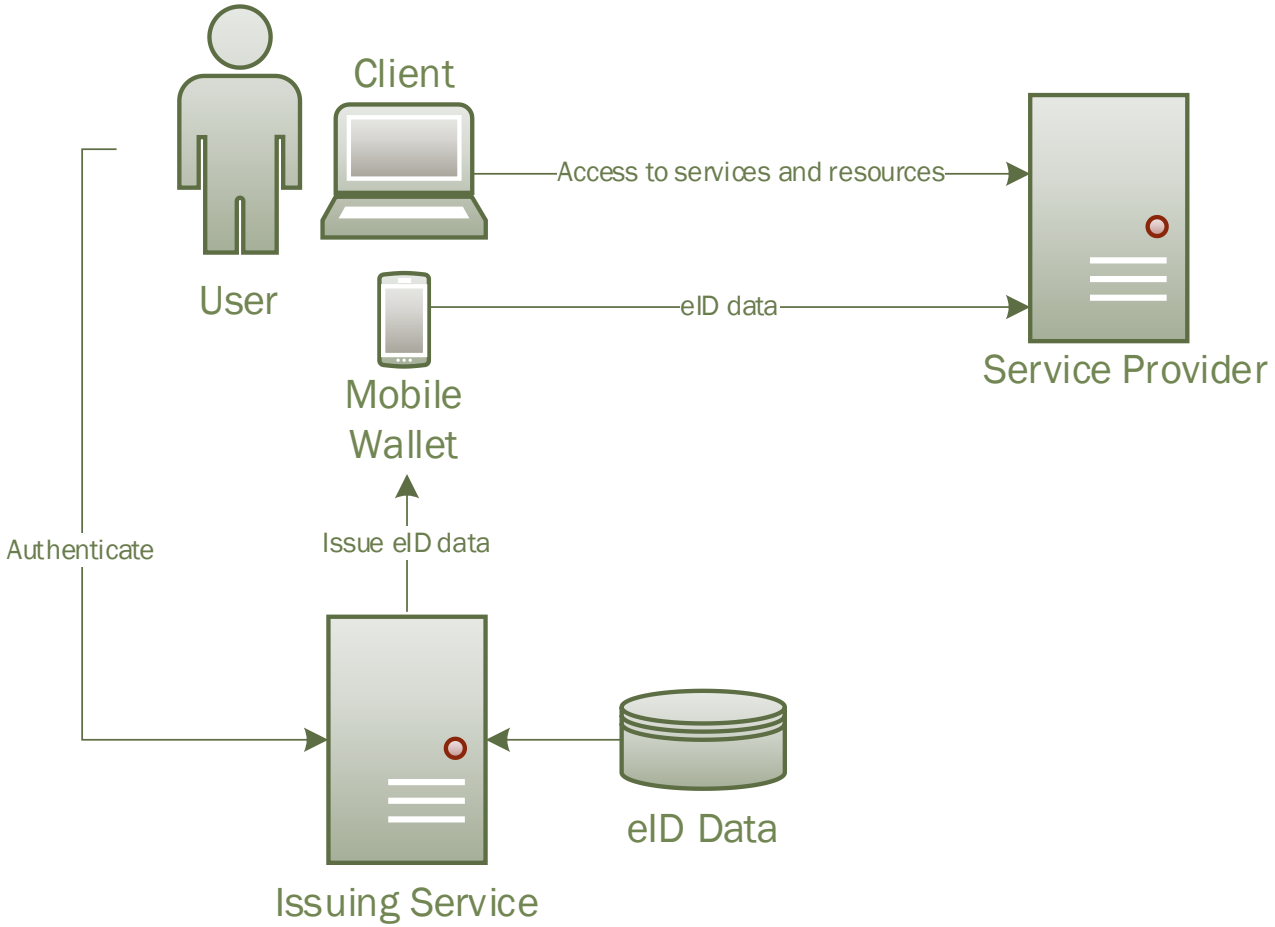
- Idea: Avoid central identity provider in authentication processes
- This way, operator of identity provider (e.g., state) cannot track users anymore (i.e., know when they logged in where)
- Legal foundation: Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing a European Digital Identity Framework ("**eIDAS Regulation**") [2]

[2] https://eur-lex.europa.eu/eli/reg/2024/1183/oj

Wallet-based User Authentication

- 2 timely independent use cases:
  - Issuing
  - Presentation (Authentication)

- **Issuing:** Identity data is stored into wallet
- **Presentation:** Identity data is fetched from wallet and presented to SP to authenticate user



Wallet-based User Authentication

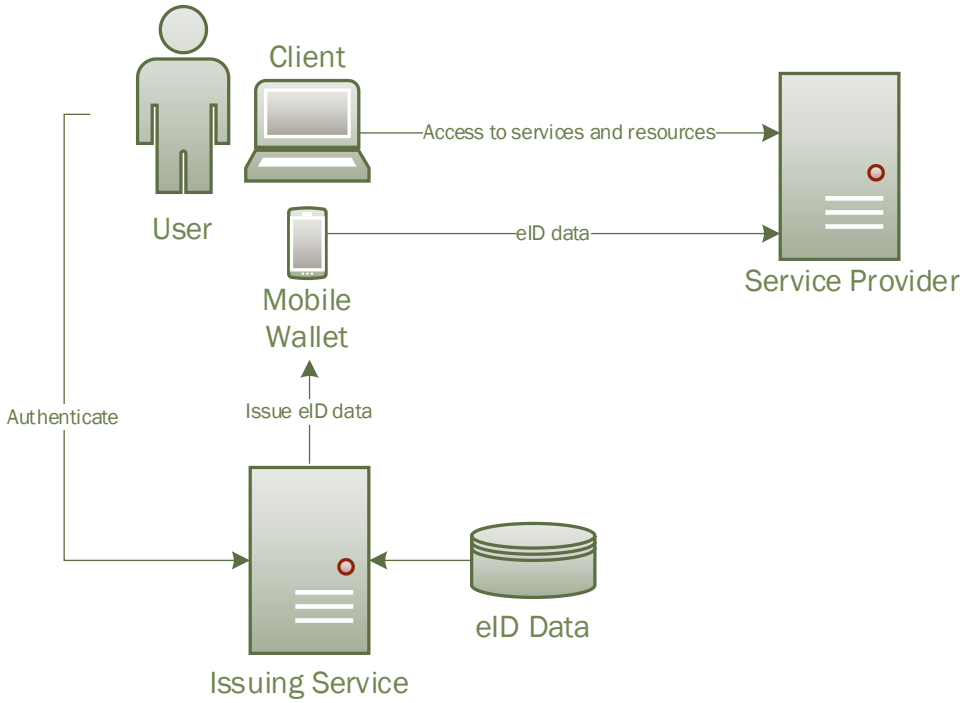
- Challenge: When read from wallet and presented to SP, identity data must still be verifiable by SP
  - In central model, identity data is signed by IDP
  - In wallet scenario, IDP is not involved in presentation/authentication at all
  - Still, SP must be able to establish trust into received identity data

- **Who attests correctness of provided identity data when there is no IDP?**
- **How to make sure that user is involved in the presentation process?**

Wallet-based User Authentication

- **Who attests correctness of provided identity data when there is no IDP?**

- Issuing Service signs eID data before issuing it to wallet
- SP can verify signature of Issuing Service during presentation
- Trust between Issuing Service and SP must be established by appropriate trust framework



Wallet-based User Authentication

- **How to make sure user is involved in the presentation process?**

- A so-called „holder key“ is involved in wallet-based transactions
  - Asymmetric cryptographic holder key is involved in issuing and presentation
  - Holder key is under sole control of the wallet user („holder“)
  - Holder key is cryptographically linked with eID data presented to SP
  - SP can verify that holder has been used during presentation and that hence user (holder) has been involved in presentation process

- Key question: How to appropriately protect and use the holder key?
  - Is local storage/use on smartphone sufficient (i.e., secure enough)?
  - Is secure remote storage/use in central certified hardware security module required?
    - Are we still talking about a decentralized solution then?
  - Can the holder key be misused to again track user behavior?

Wallet-based User Authentication

- Wallet-related protocols and standards already exist

- Issuing
  - OpenID for Verifiable Credential Issuance (OIDC4VCI)
  - ISO/IEC 18013-5 & -7 – mobile-ID / PID issuance for remote and proximity scenarios
  - W3C Verifiable Credentials Data Model 2.0 or SD-JWT VC – structured, selectively disclosable credentials
  - …
- Presentation
  - OpenID Connect 4 Verifiable Presentations (OIDC4VP) plus SIOPv2 – remote presentation flows
  - ISO/IEC 18013-5 – NFC / QR proximity presentation
  - Presentation Exchange v2 + SD-JWT selective disclosure – attribute filtering & proof schemes
  - …

Wallet-based User Authentication – Pros

- No tracking of users possible
  - In principle, no IDP or other central component is involved during authentication
  - Mind the details (holder-key requirements, potentially necessary on-the-fly issuing of eID data, etc.)
- Allows for offline scenarios
  - Example: Prove age when entering a club
- Local control of identity data
  - Identity data is stored locally, so local control mechanisms can be enforced
  - Selective disclosure for data minimization

Wallet-based User Authentication – Cons

- Copies of identity data stored locally in wallet
  - What happens if data change in central registers (e.g., changing family name due to marriage)?
  - More complex revocation mechanisms needed

- Alternative trust model needed
  - No central identity provider to be trusted
  - How to establish trust in attributes stored on the user‘s local device?
    - Yes, verifiable credentials are signed, but how to establish trust in this signature?
    - How to ensure that establishing trust does not again lead to traceability of users?

- Need to support broad spectrum of different end-user devices
  - Functional requirements
  - Security requirements

A-SIT

ID Austria: Under the Hood

- The previous slides show the user's perspective, i.e., what the user sees and does during an ID-Austria-based authentication process
- And now let's have a look under the hood
  - Identity data provided by ID Austria
  - Derivation and use of unique identifiers
  - Technical architectures and processes
  - Selected concepts and features
  - Future directions

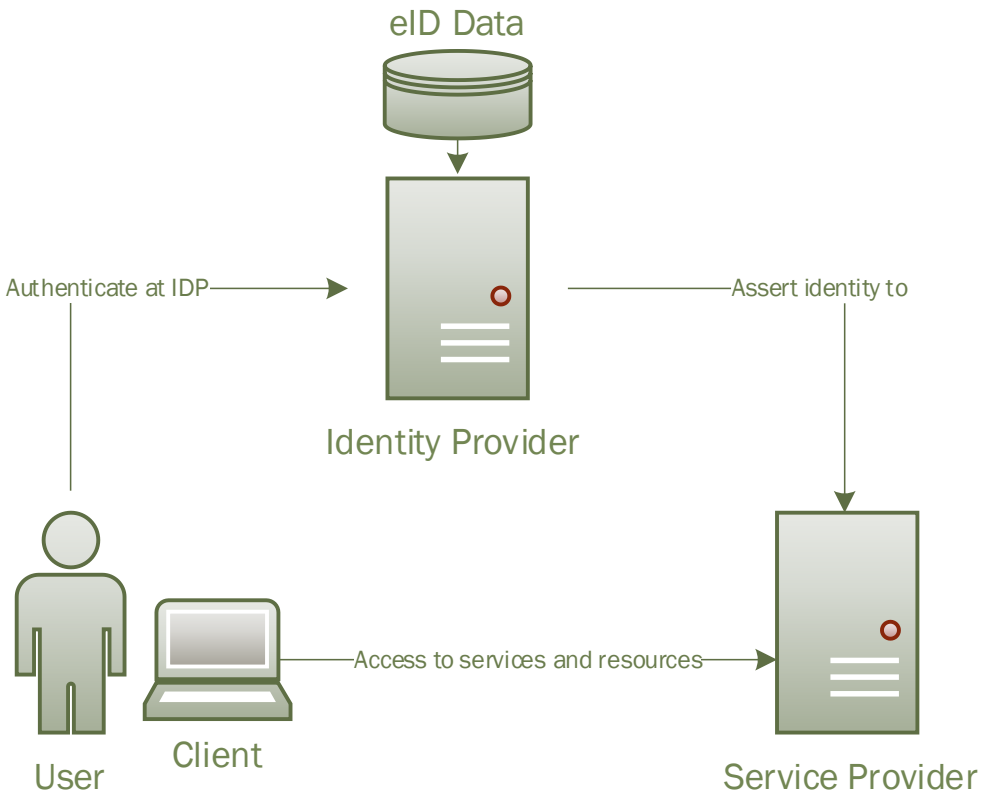
Topics for Today‘s Lecture

- **Goal:** Understand how identity management is done in practice
- **Use Case 1:** National identity management in Austria: ID Austria
- **Use Case 2:** Cross-border national identity management in Europe: The Technical eIDAS Interoperability Framework

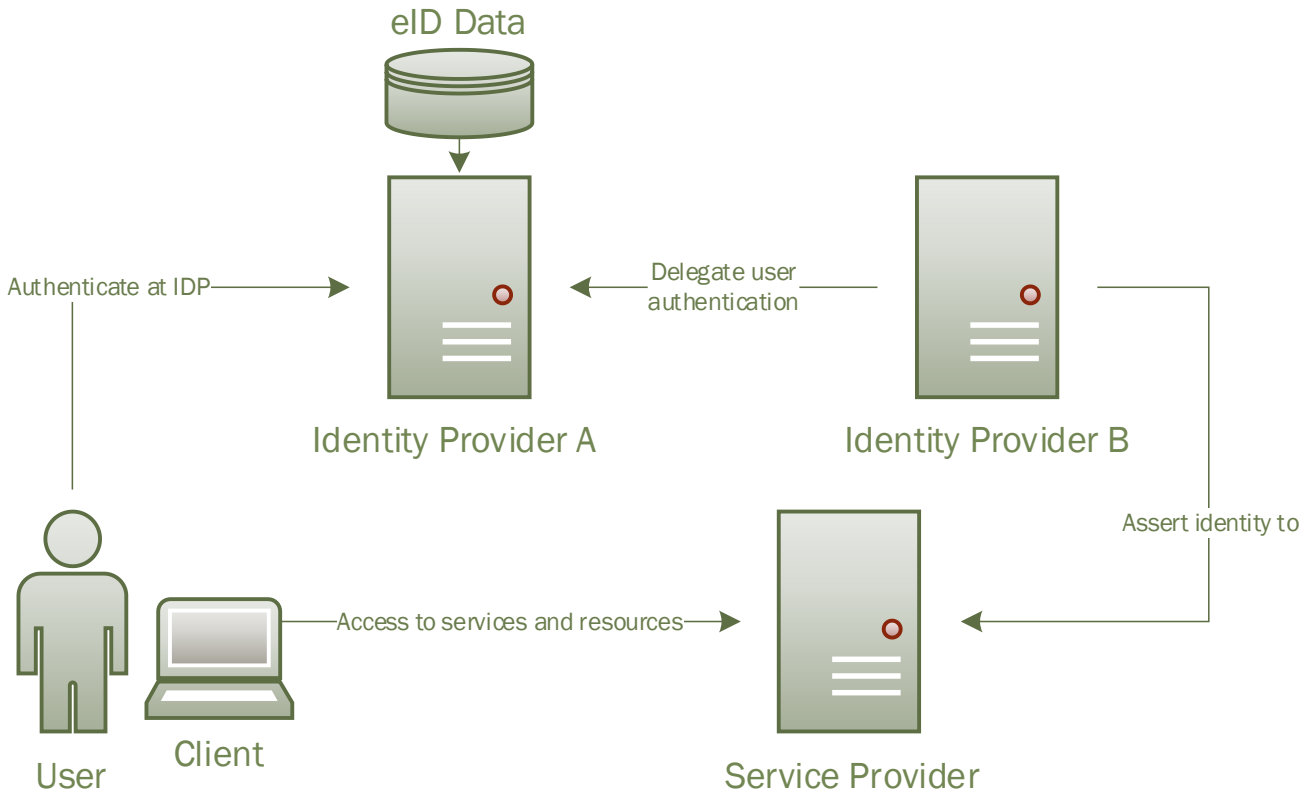
Use Case 2: Cross-border national identity management in Europe:

The Technical eIDAS Interoperability Framework

Recap: Identity Management Models



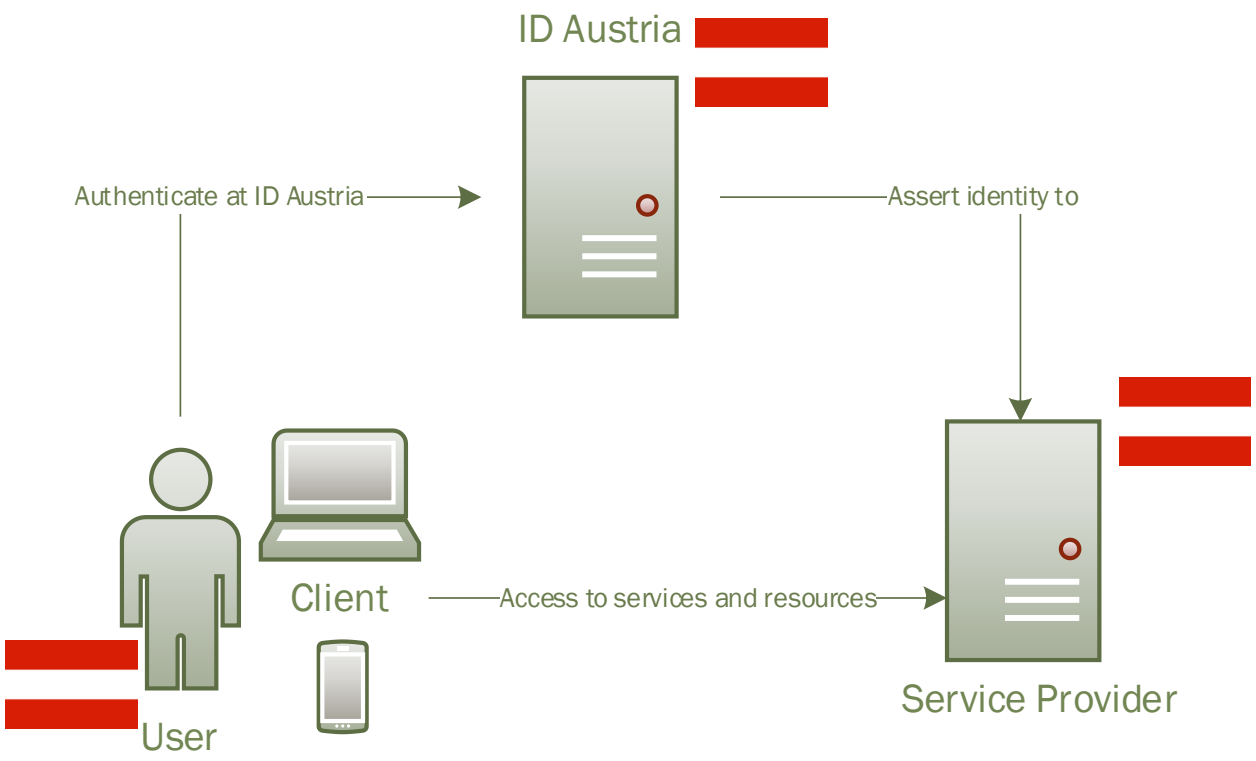
Central Model



Federated Model

Motivation

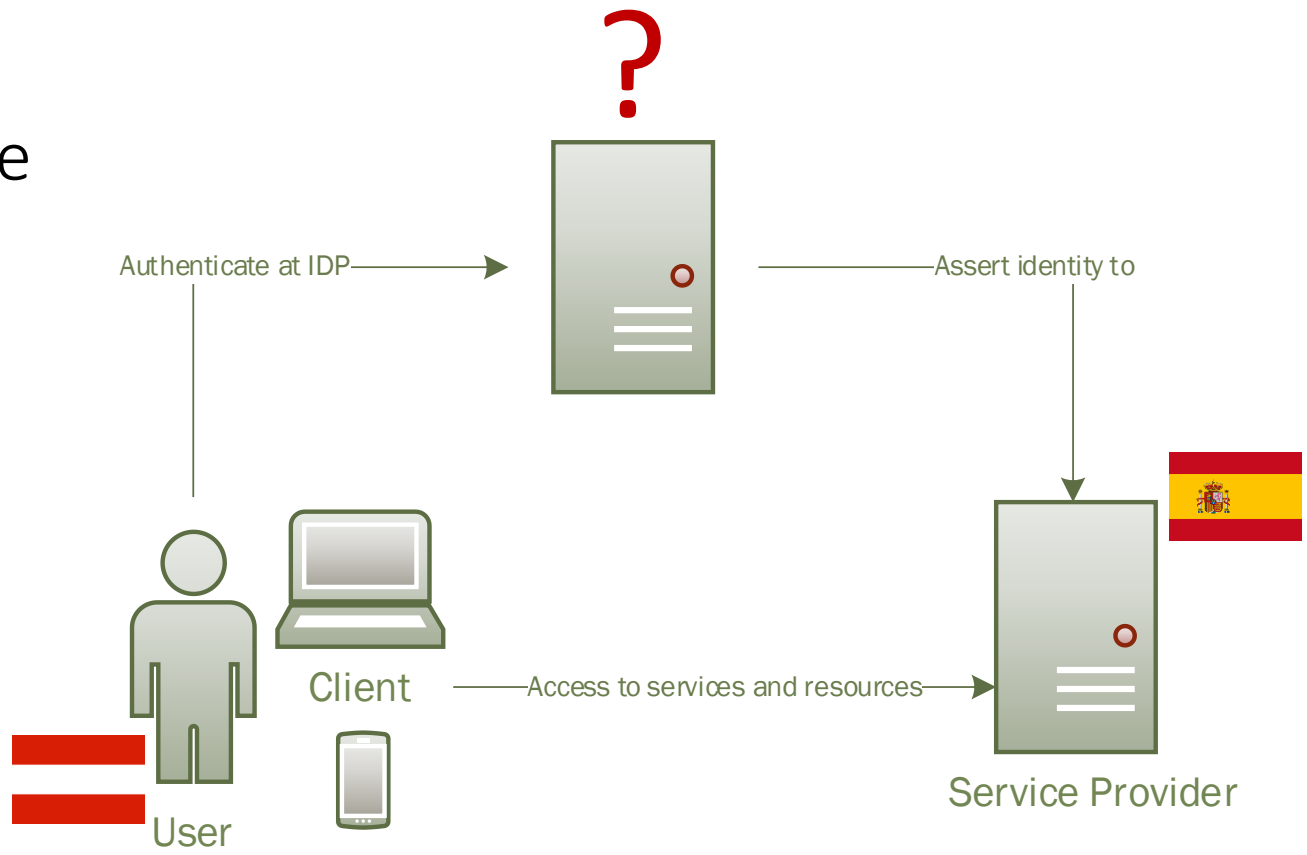
- So far, we have considered a purely national scenario only
  - Austrian user
  - Austrian Service Provider
  - Austrian IDP (ID Austria)
- However, a purely national scope is not sufficient in a European context
- What about more complex scenarios?



Cross-Border Scenario

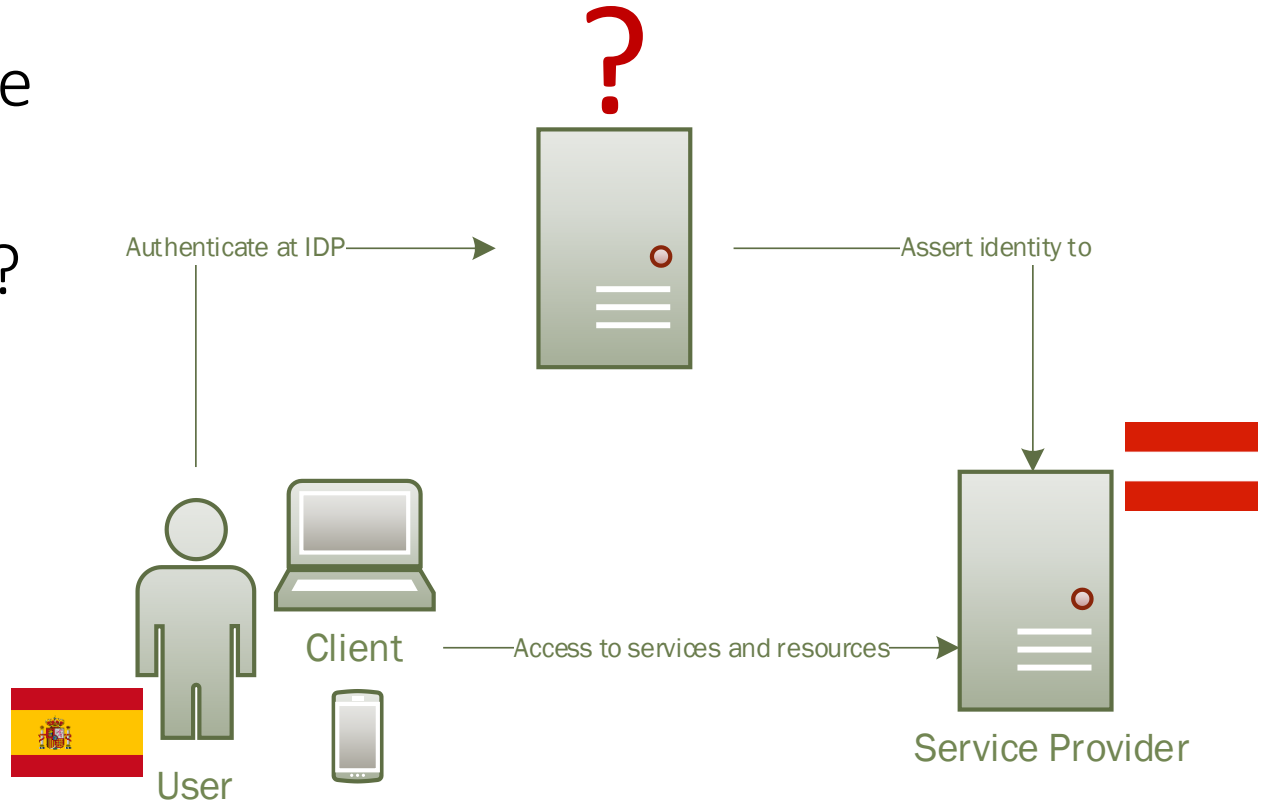
- **Austrian user** wants to authenticate at **Spanish Service Provider**

- Tricky question: Which IDP to use?
  - User has only an Austrian eID (ID Austria)
  - Spanish SP does only support the Spanish national IDP



Cross-Border Scenario

- **Spanish user** wants to authenticate at **Austrian Service Provider**
- Tricky question: Which IDP to use?
  - User has only a Spanish eID
  - Austrian SP does only support the Austrian national IDP (ID Austria)



Problem Definition

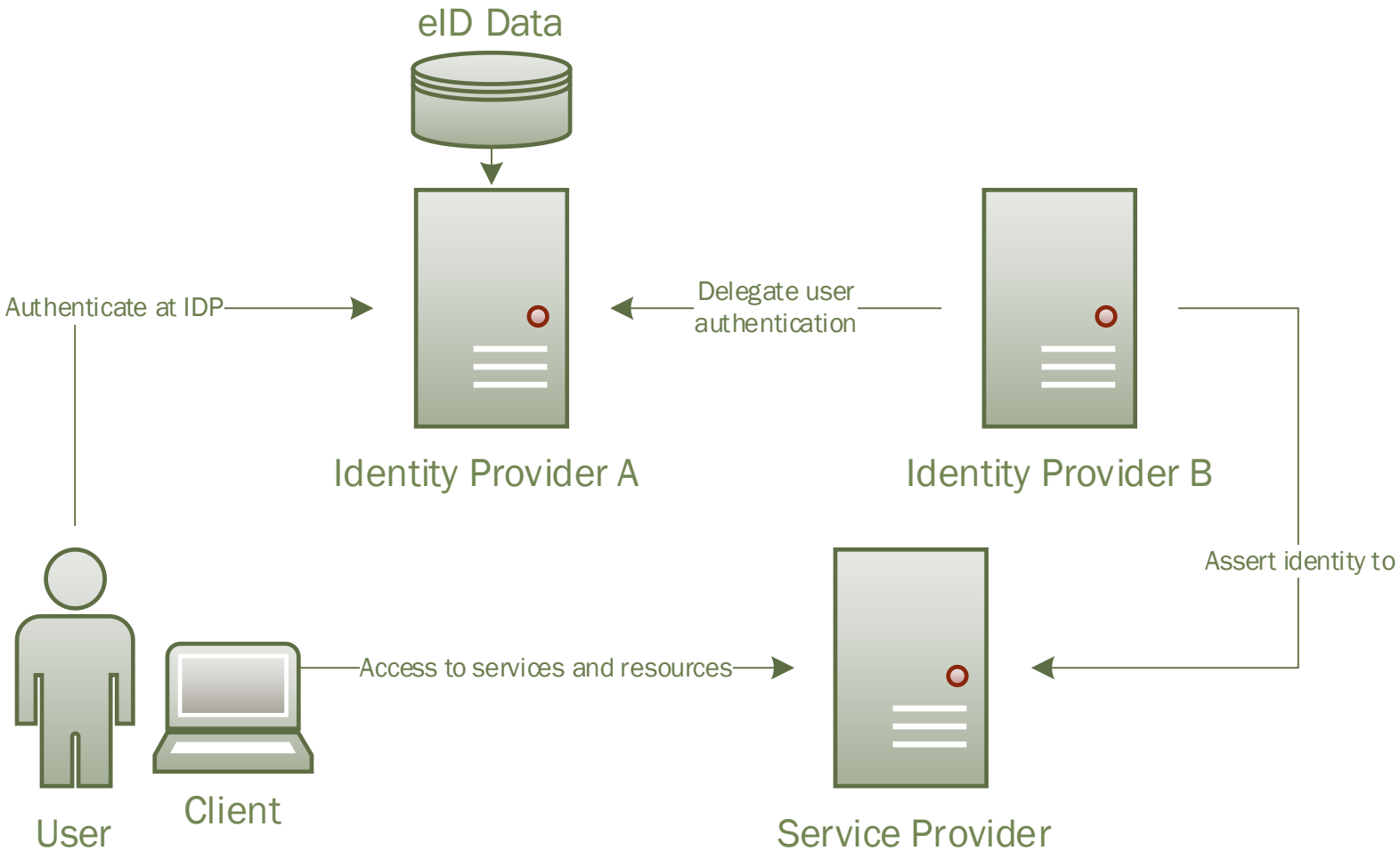
- National identity management systems have evolved independently in EU Member States; hence they are not compatible out of the box

- A service provider only wants to interact with its own national eID solution (IDP)
  - Otherwise, the SP would need to support 20+ different IDPs -> Impractical
  - Furthermore, each IDP would provide the SP with a different eID (identifier)

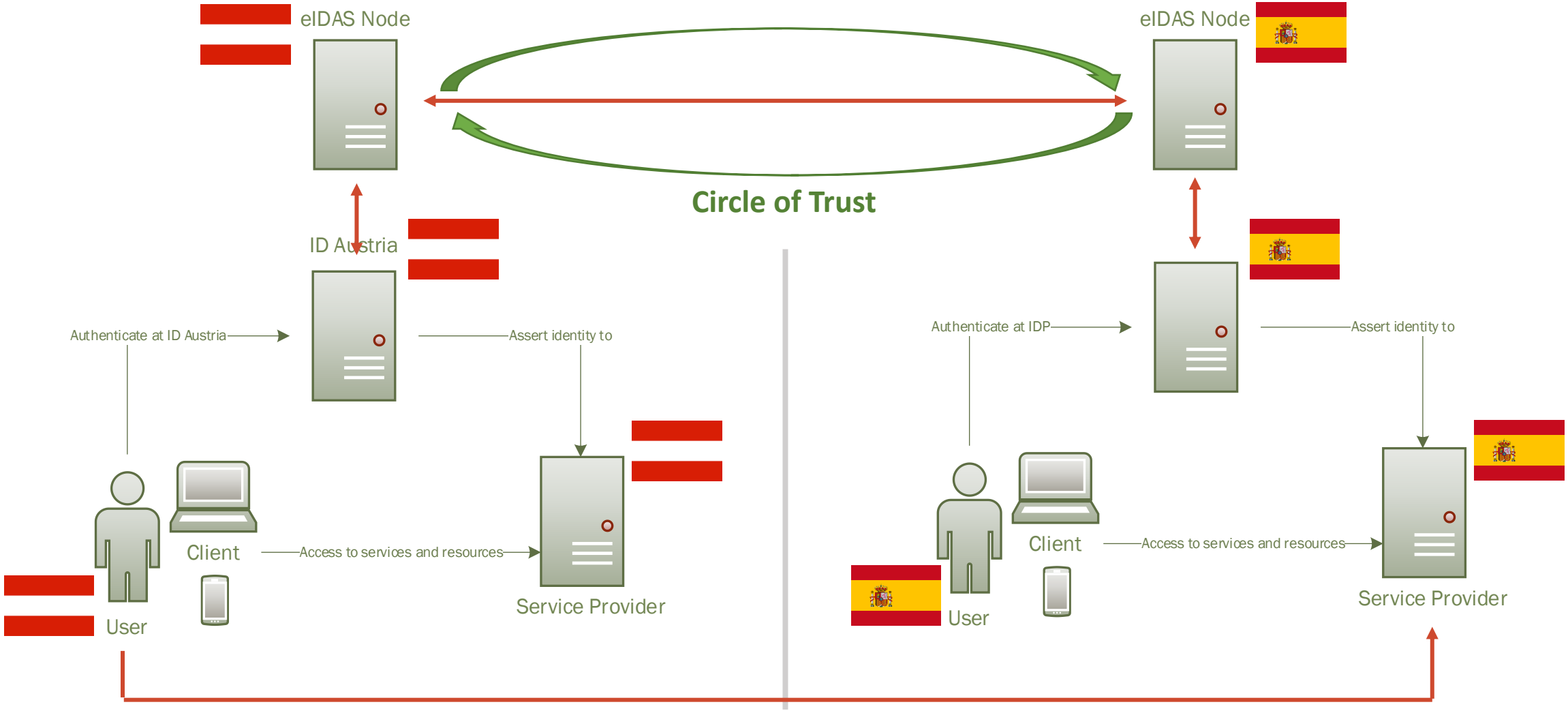
- A user only wants to use her own national eID
  - Even if the user wants to use national eIDs from other countries, this is sometimes infeasible for legal reasons
  - In any case it would be impractical

Solution: Identity Federation

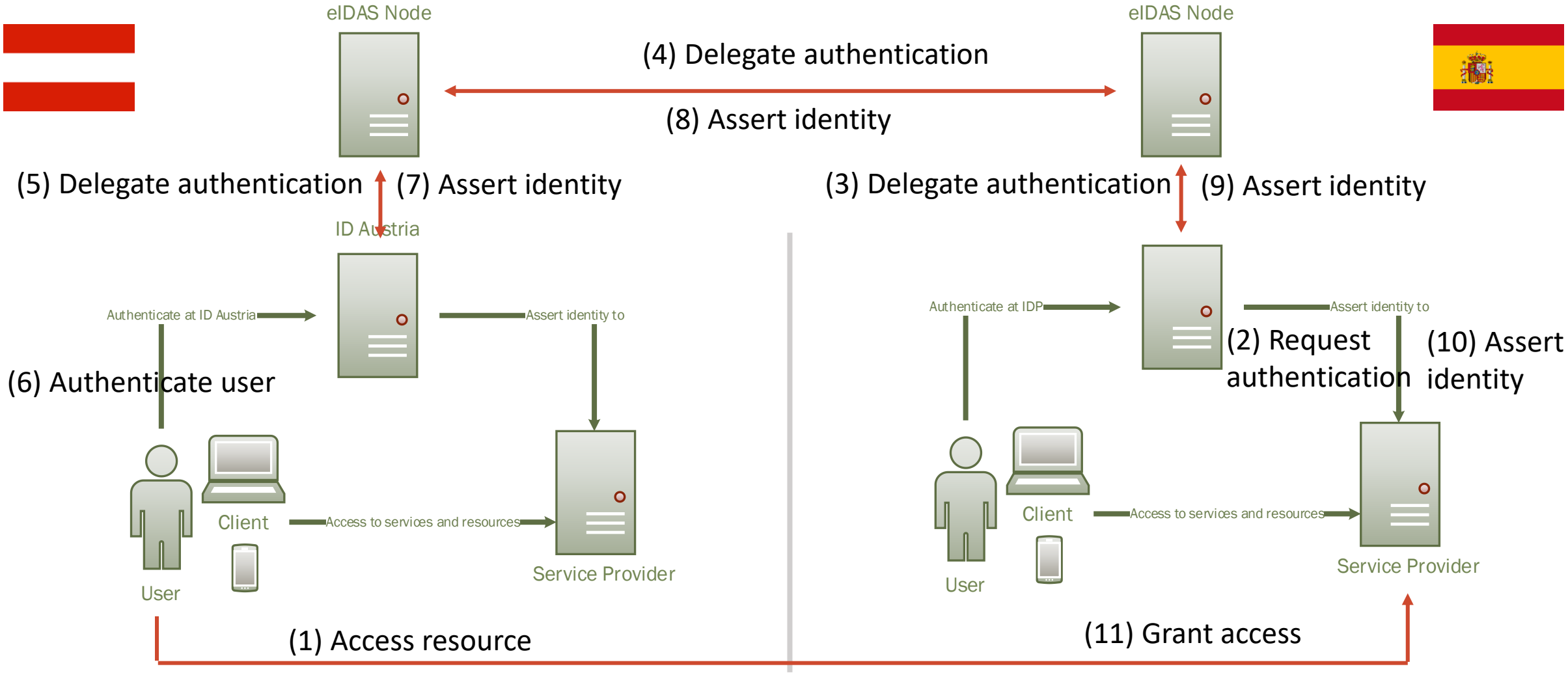
- Let both, user and SP, use their “own” IDP
- Make sure that IDPs can delegate user authentication between each other
- IDPs build a circle of trust



eIDAS-based Cross-Border Authentication



eIDAS-based Cross-Border Authentication



eIDAS-based Cross-Border Authentication

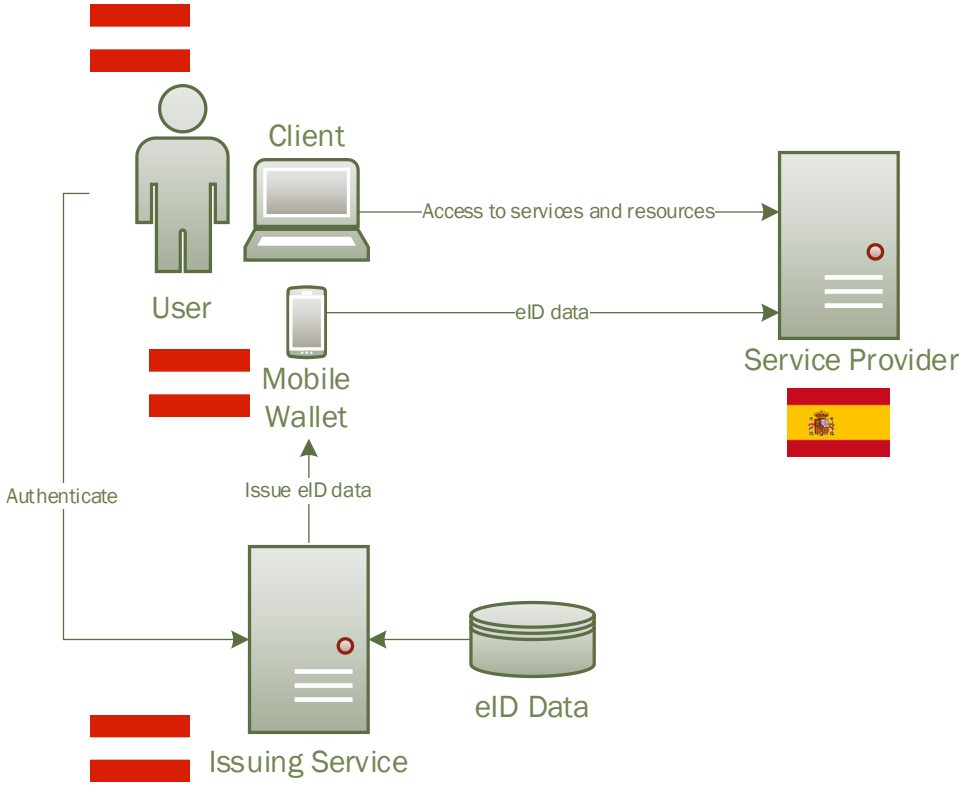
- eIDAS Nodes federate national identity management systems
  - Service Provider only needs to communicate with its national IDP
  - User only needs to communicate with her national IDP
- Conceptually, each EU Member State operates one eIDAS Node
  - Note: Exceptions exist (e.g., Germany)
- Trust relationships:
  - eIDAS Nodes trust each other
  - National components trust their own national eIDAS Node
  - BUT: Components (SP, user, IDP, etc.) do not need to trust explicitly components from other EU Member States

Future Directions

- Amended EU eIDAS Regulation introduces EU Digital Identity Wallets (EUDIW)

- Goals:
  - EU citizens will be provided with a EUDIW by their Member States
  - Common specification, different implementations
  - A step towards harmonization
  - Currently (2025) under development

- Goal: Enable direct communication between service providers and wallet
  - Avoid possible tracking by central components
  - Enable offline use cases



EUDIW in the Cross-Border Context

- Interoperability of classical European eID schemes (ID Austria, etc.) is achieved by federation of national eIDAS nodes

- Conceptually, federated eIDAS nodes are not required any more by EUDIWs
  - Wallets communicate directly with service providers
  - All relevant interfaces are standardized – wallets and SPs from different EU Member States are interoperable out of the box (in theory)

- However, the devil is in the details!
  - Co-existence of legacy eID schemes and wallet solutions
  - Trust framework
  - Identity matching (i.e., find existing foreign user in national registers based on Wallet data)
  - …

EUDIW in the Cross-Border Context

- Legal basis („eIDAS 2“) is there and in force on European level
- Relevant implementing acts are provided gradually
- EU Large scale pilots develop and test first implementations in the field
- Member States try to make the relevant ambitious deadlines
- First enrolments of EUDIW to be expected by the end of 2026

Use-Case EU – Summary

- Classical national identity management systems of different countries are not interoperable out of the box
- Approach: Federate different national systems using eIDAS Nodes that form a circle of trust
- In productive operation for some years already, more and more countries (eID systems) to join
- In future, wallet-based approaches will play an increasingly important role
- Decentralized, wallet-based solution enable direct wallet-to-SP communication through harmonized interfaces but raise new technical and organizational challenges

Topics for Today‘s Lecture

- **Goal:** Understand how identity management is done in practice
- **Use Case 1:** National identity management in Austria: ID Austria
- **Use Case 2:** Cross-border national identity management in Europe: The Technical eIDAS Interoperability Framework

ID Austria
and
eIDAS-based Cross-Border Authentication

Questions & Answers

Dr. Thomas Zefferer

Summer Term 2025