Selected Topics IT-Security 1 (E-Government)

Identity Management in Austria

christof.rabensteiner@egiz.gv.at

Christof Rabensteiner

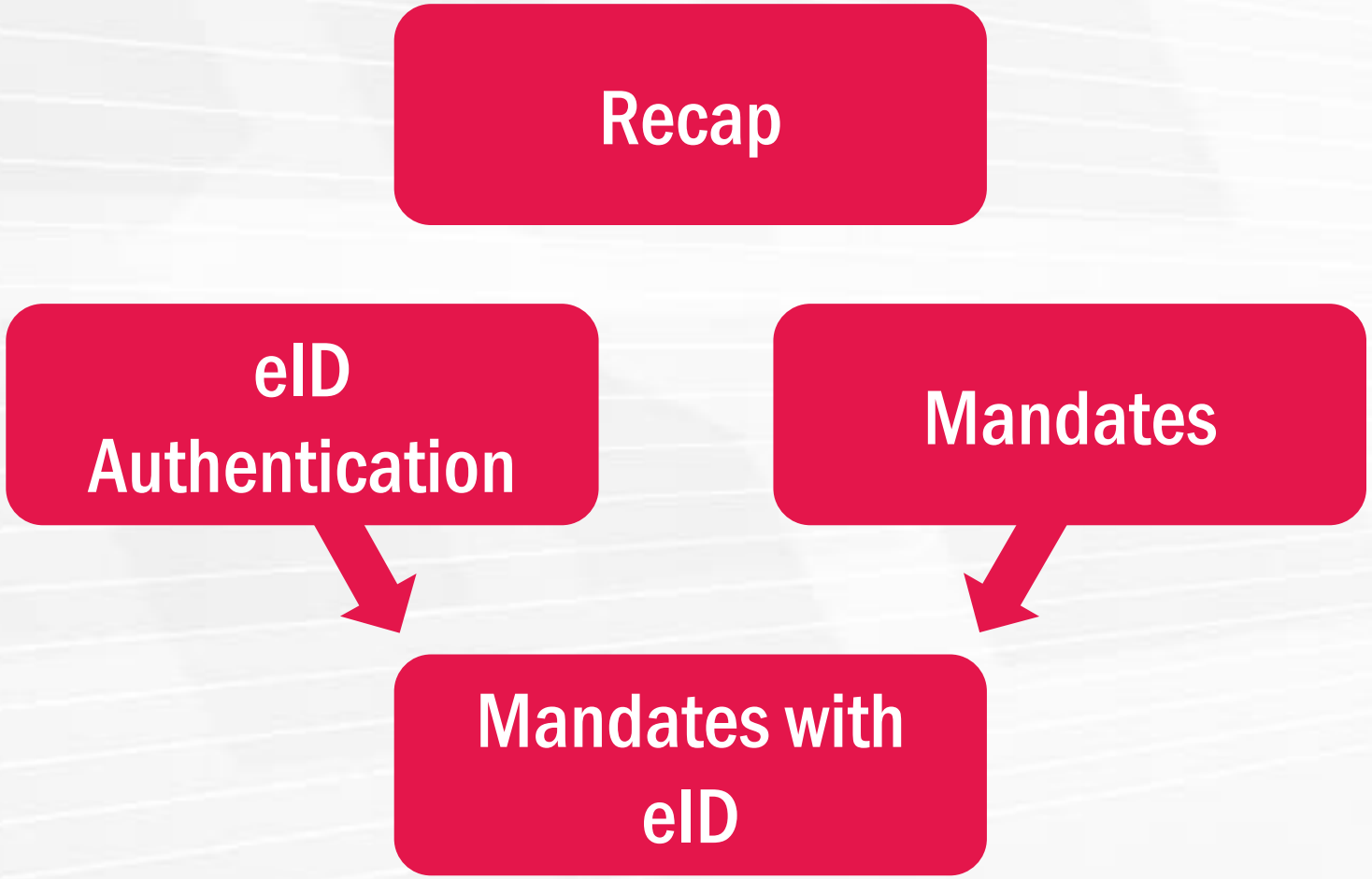
Graz, 30.10.2019

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

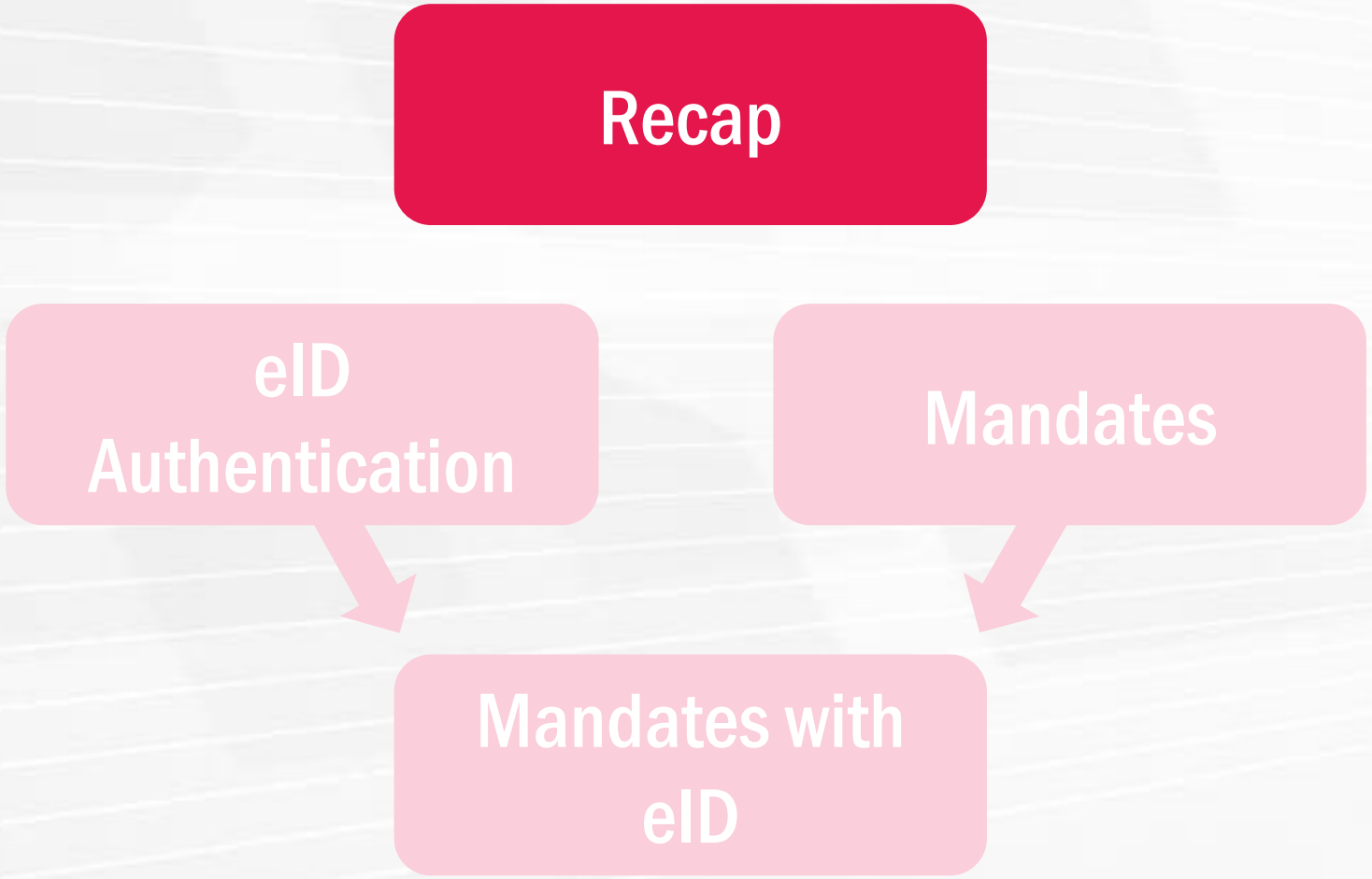
TU Graz

EGIZ
E-Government Innovationszentrum

Outline



Outline



Recap (1/2): IDM by **Example**

Example: Alice withdraws money at the bank

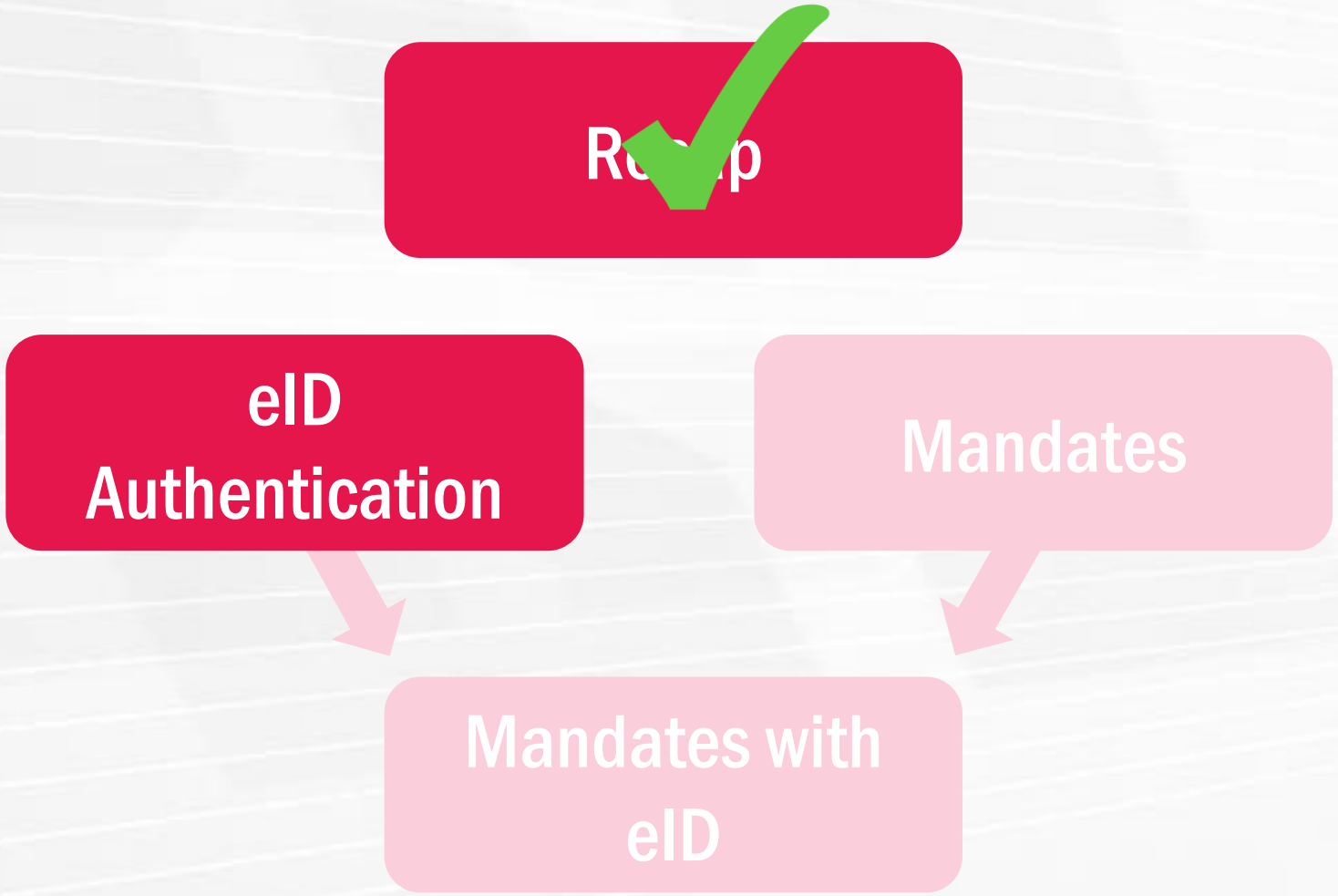
Alice

- **Identity:** Alice
- **Identification:** “I am Alice“
- **Authentication:** Alice shows her passport, bank employee verifies ownership.
- **Authorization:** Bank employee allows Alice to withdraw money.

Recap (2/2): eID Terminology

- **Digital Identity:** Set of attributes, describes entity
- **Source PIN:** Encrypted central population register number which identifies citizens
- **Sector Specific PIN:** Source PIN, hashed with Sector Code
- **CCE:** Citizen Card Environment
- **Identity Link:** XML Data Structure;
  stored in CCE;
  contains identifier (source PIN or SSPIN), attributes, and certificate.

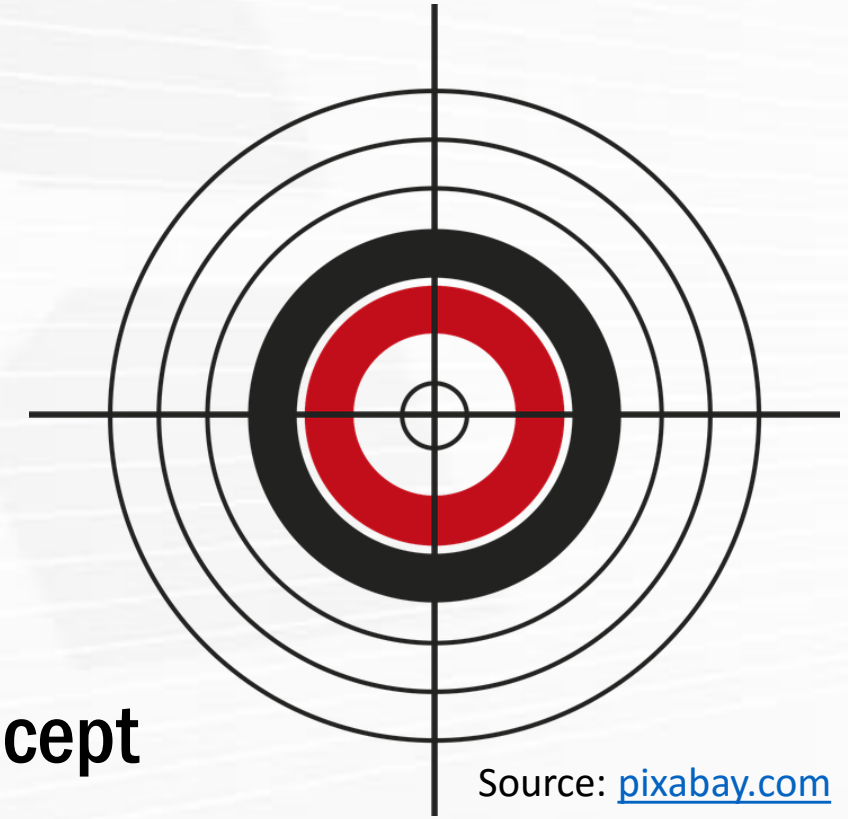
Outline



eID Authentication: Learning Targets

You will be able to…

- describe eID architecture + relation between components
- explain what MOA ID is, what it does
- describe eID authentication sequence & link to *general flow of identity protocols* (from lecture: Identity Management)
- give an overview of eIDAS cross border concept



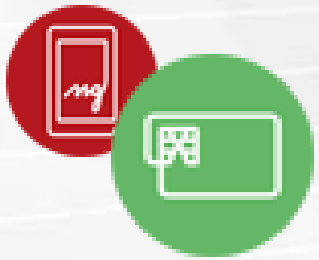
Source: pixabay.com

eID Authentication: Overview

file tax return

FINANZONLINE.AT

ID? Auth?



Reasons why this is a lot of work:

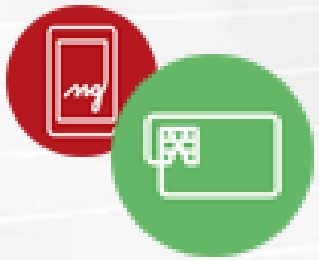
- Multiple CCEs?
- Representation?
- Single Sign On?
- Cross Border?

eID Authentication: Overview

file tax return

FINANZONLINE.AT

send verified identity

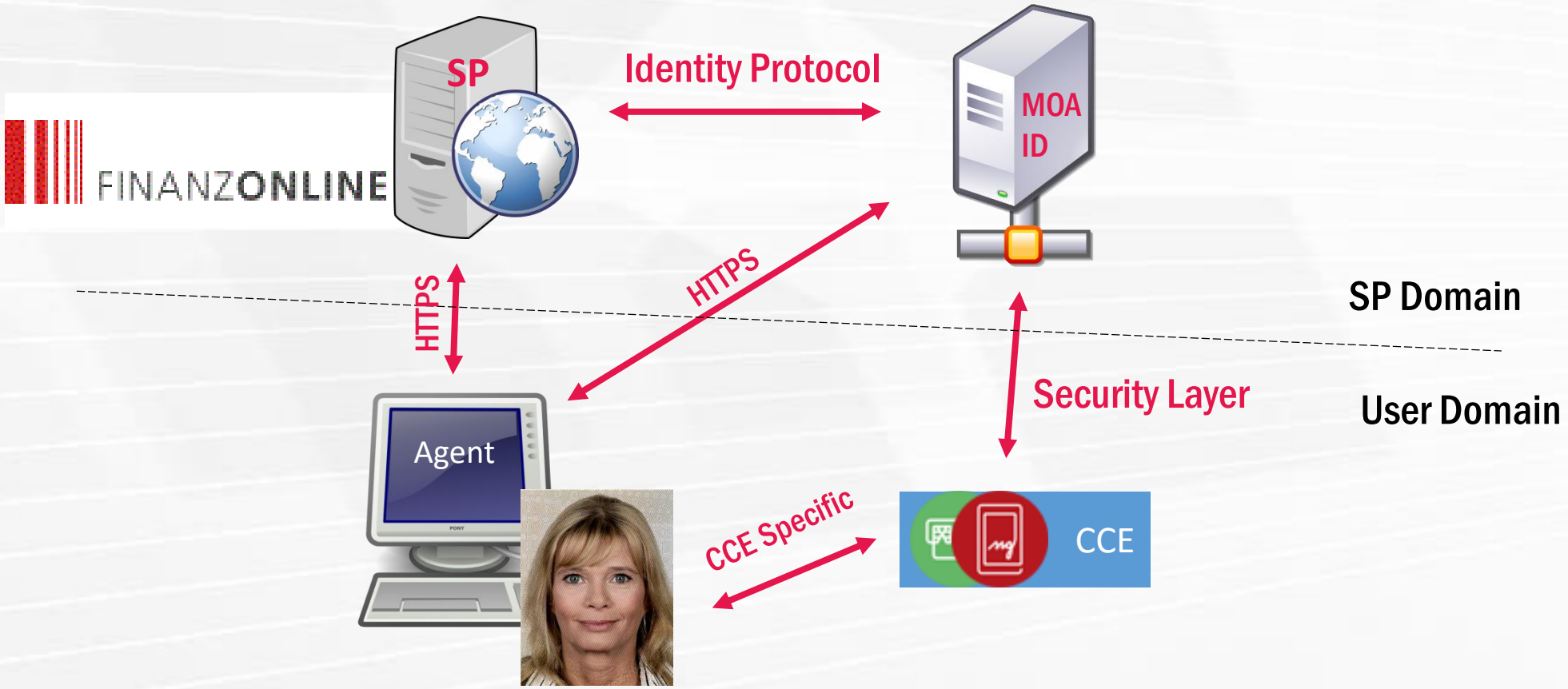


identify & authenticate

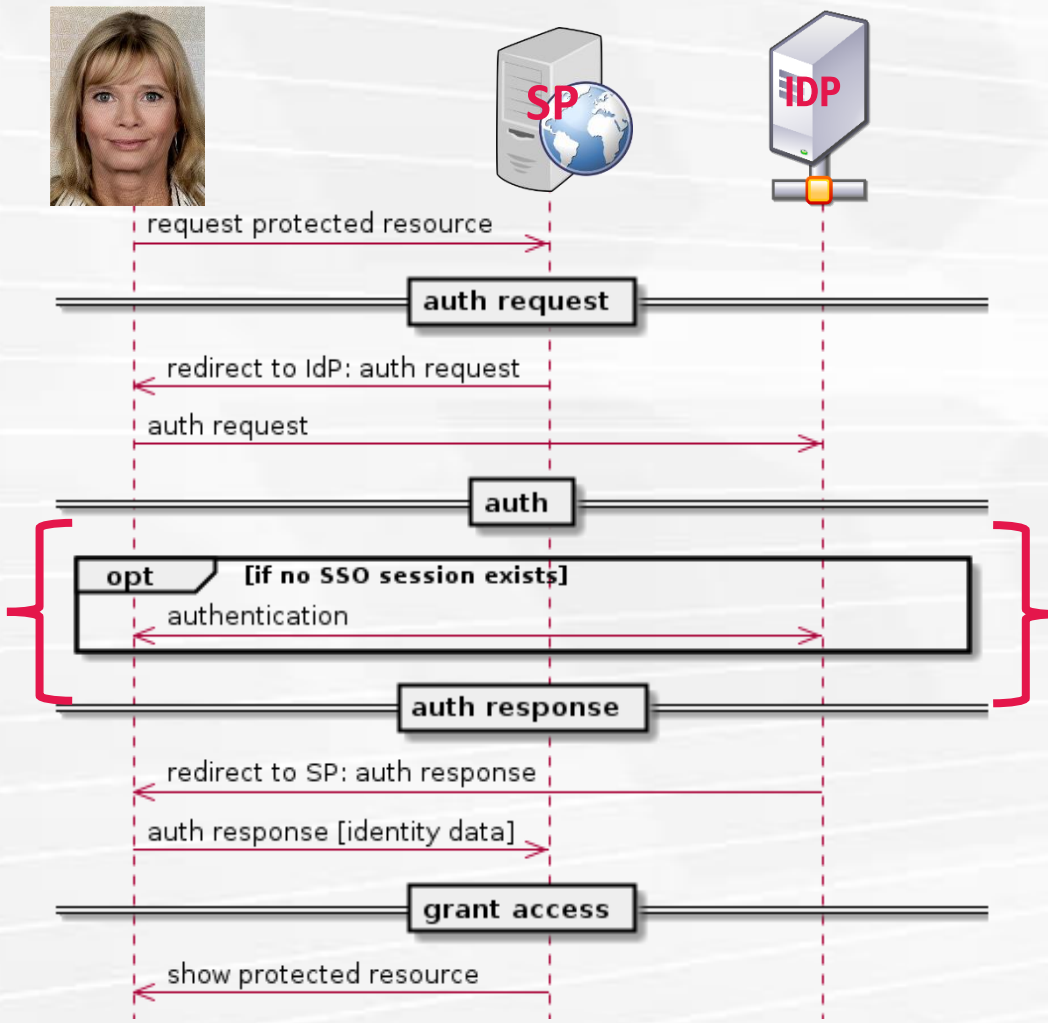
eID Authentication: MOA-ID

- MOA-ID = Online Application Modules - IDentification
- Web application
- Acts as IdP → SPs delegate authentication
- Identifies and authenticates Citizens via CCE
- Can handle mandates
- Can authenticate foreign citizens

eID Authentication: **Architecture**



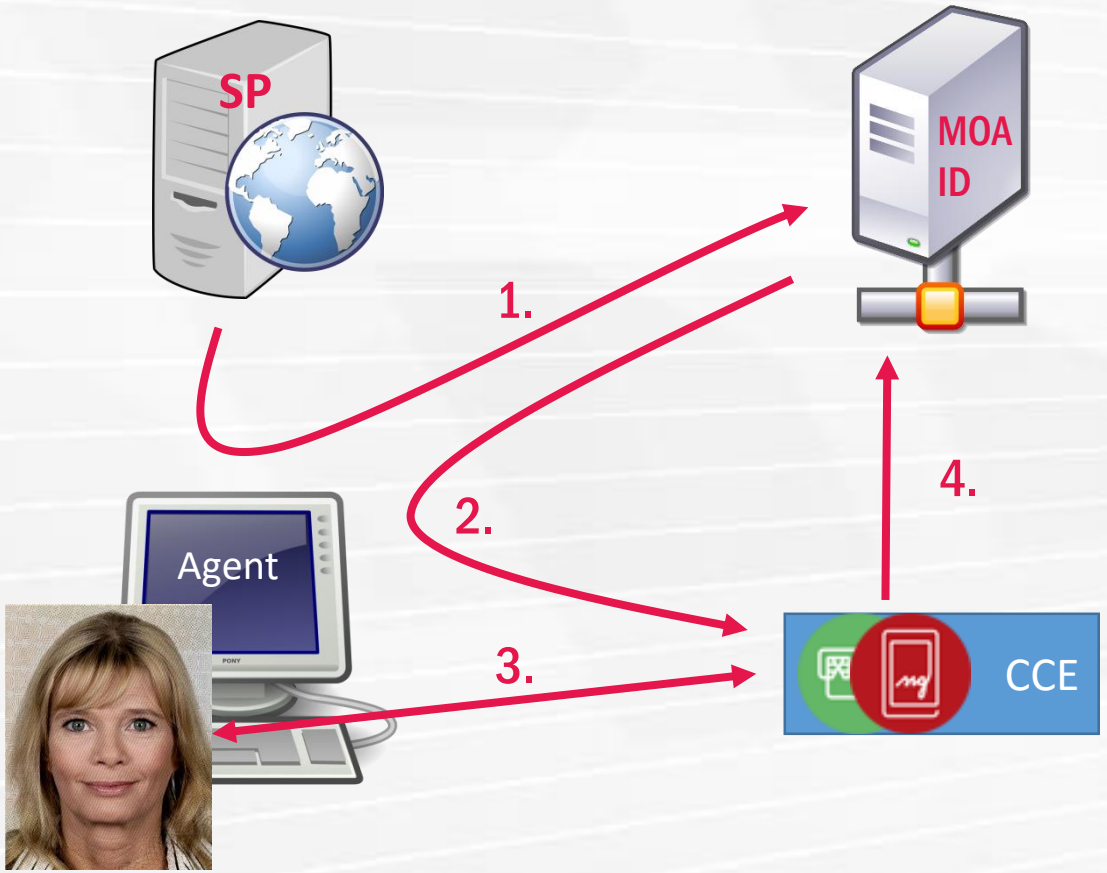
eID Authentication: Sequence (1)



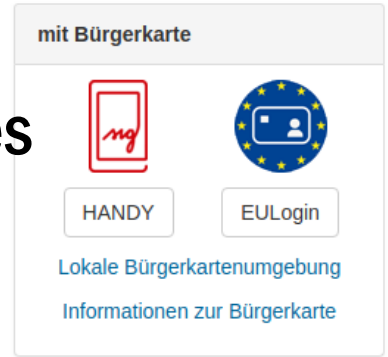
Remember the *general flow of identity protocols* from the IDM lecture?

We discuss this part

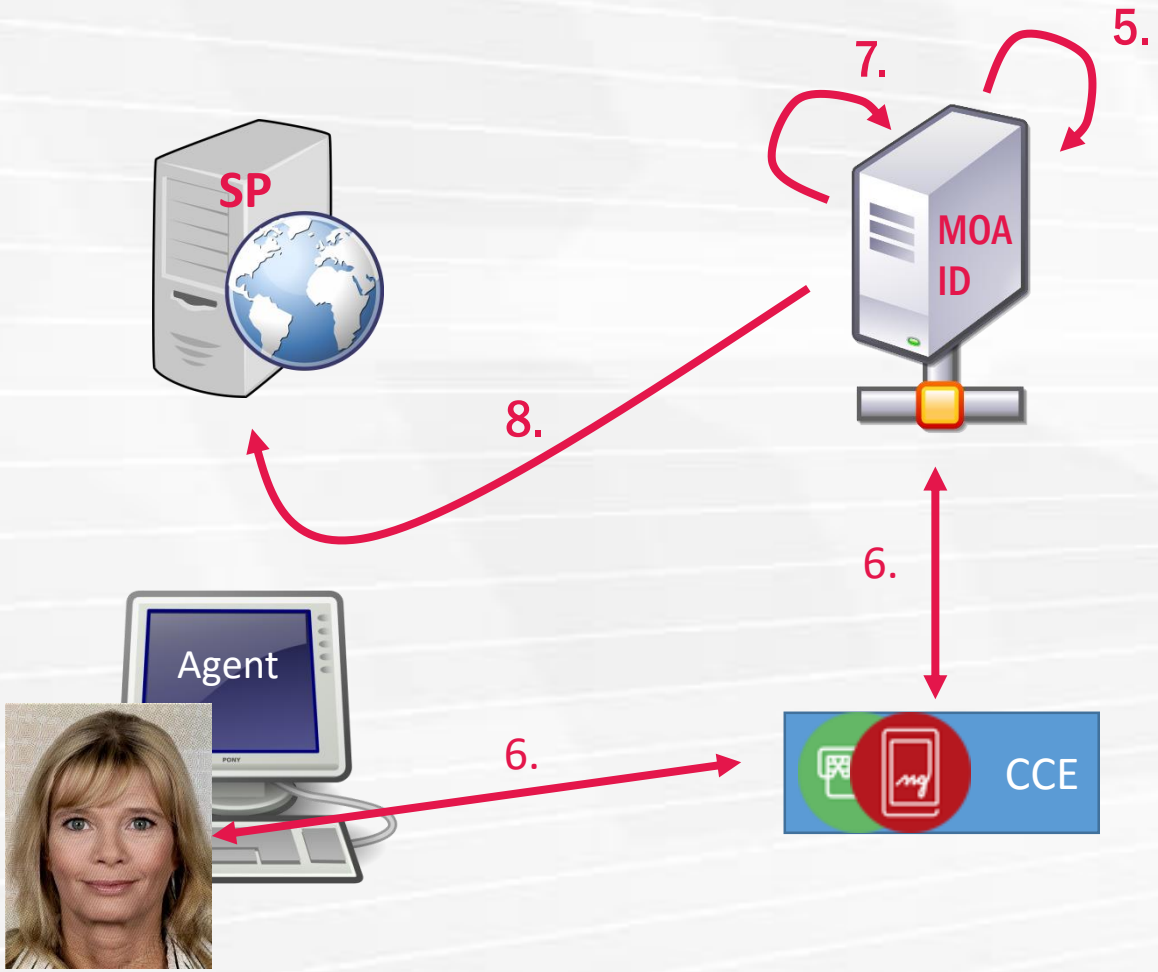
eID Authentication: Sequence (2)



1. Alice requests CCE selection from MOA-ID (="auth request")
2. Alice selects CCE and gets redirected
3. Alice authenticates towards CCE
4. CCE sends Identity Link to MOA-ID



eID Authentication: Sequence (3)



5. MOA-ID verifies Identity Link
6. MOA-ID sends auth block (challenge) to CCE, CCE signs it (response) with user's consent
7. MOA-ID verifies signed auth block
8. MOA generates and forwards *Assertion* ("auth response")

eID Authentication: Auth Block

- XML Data Structure („Challenge“)
- User signs with CCE („Response“)
- Contains information such as:
  - Who signs in (Name, Date of Birth, sspin)
  - ...to which SP
  - Date and time
- Moa ID verifies response with Certificate from Identity Link

Anmeldedaten:

Daten zur Person

Name:	Alice
Geburtsdatum:	7.7.1977

Daten zur Anwendung

Name:	Anmeldesystem der TU Graz
Staat:	Österreich

Technische Parameter

URL:	https://online.tugraz.at
Bereich:	BF (Bildung und Forschung)
Identifikator:	ISGhbGiCIAobdkc6nxhUFaG/FGM=
Datum:	23.05.2014
Uhrzeit:	10:54:10

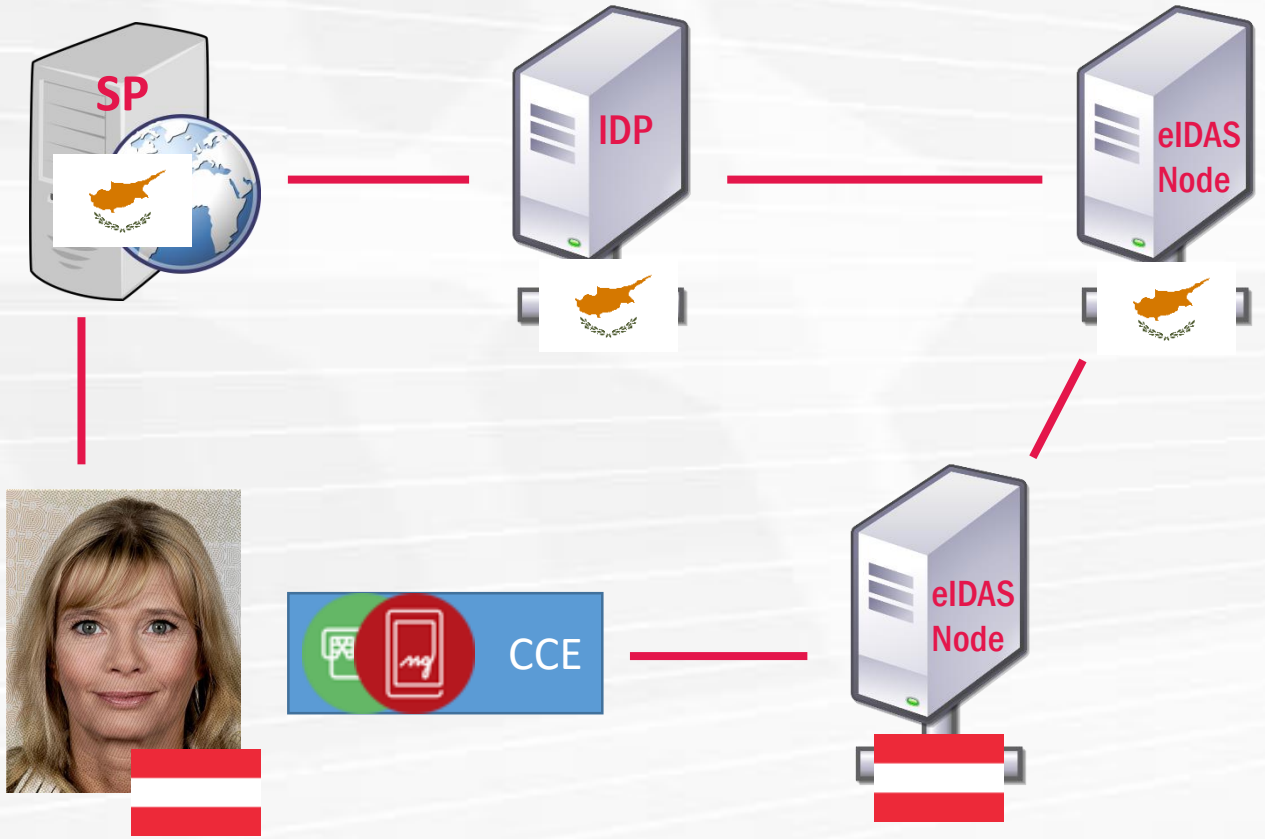
Readable Auth Block Example

eID Authentication: Foreign Citizens (1/2)

- eIDAS = electronic IDentification, Authentication and trust Services
- EU regulation & legal framework
- Goal: Establish common ground for national eIDs, signatures, & trust services (Interoperability)
- = Federated Identity Management

Source: ec.europa.eu

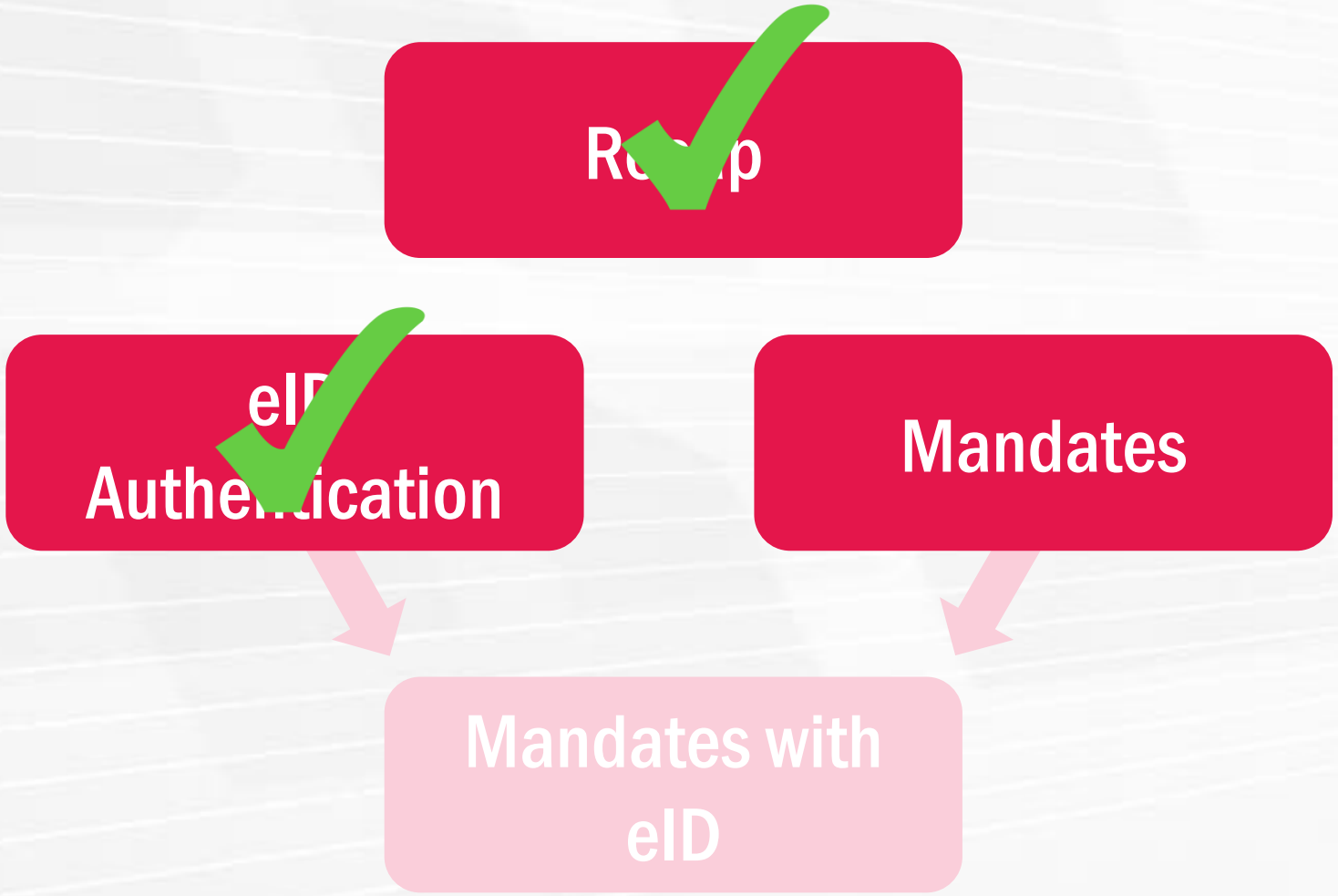
eID Authentication: Foreign Citizens (2/2) Sample Use Case



eID Authentication: Conclusion

- Server Application
- Interface between SP and CCE
  - With SP: Identity Protocol
  - With CCE: Security Layer
- Takes over Identification and Authentication

Outline



Mandates: **Learning Targets**

You will be able to …

- Define and motivate the concept of mandates
- Describe the actors of mandate relationship
- Describe and motivate the approach of electronic mandates

Mandates

Alice

Bob

Source: pngimg.com

Company

FINANZONLINE.AT

Mandates: **Definition**

- From latin mandare :
  to entrust, to deliver over, to commission, to command
- “Empowering a person to act for another person”
- Person becomes authorized to act under delegated power

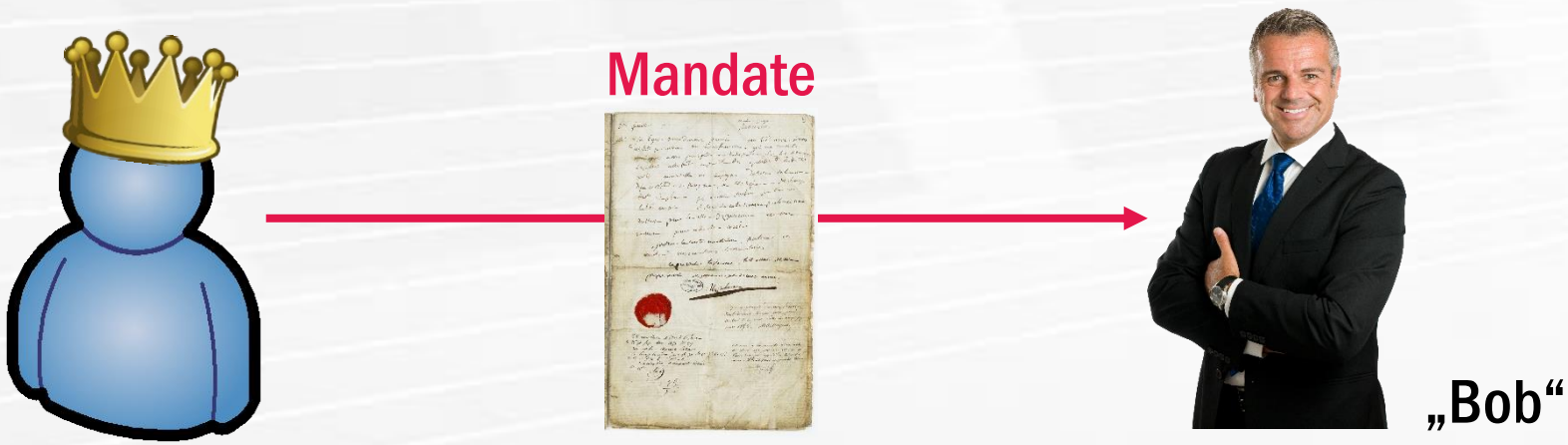
Mandates: **Actors**

Mandator

- Person on who's behalf an action is performed
- In original possession of rights and roles

Proxy

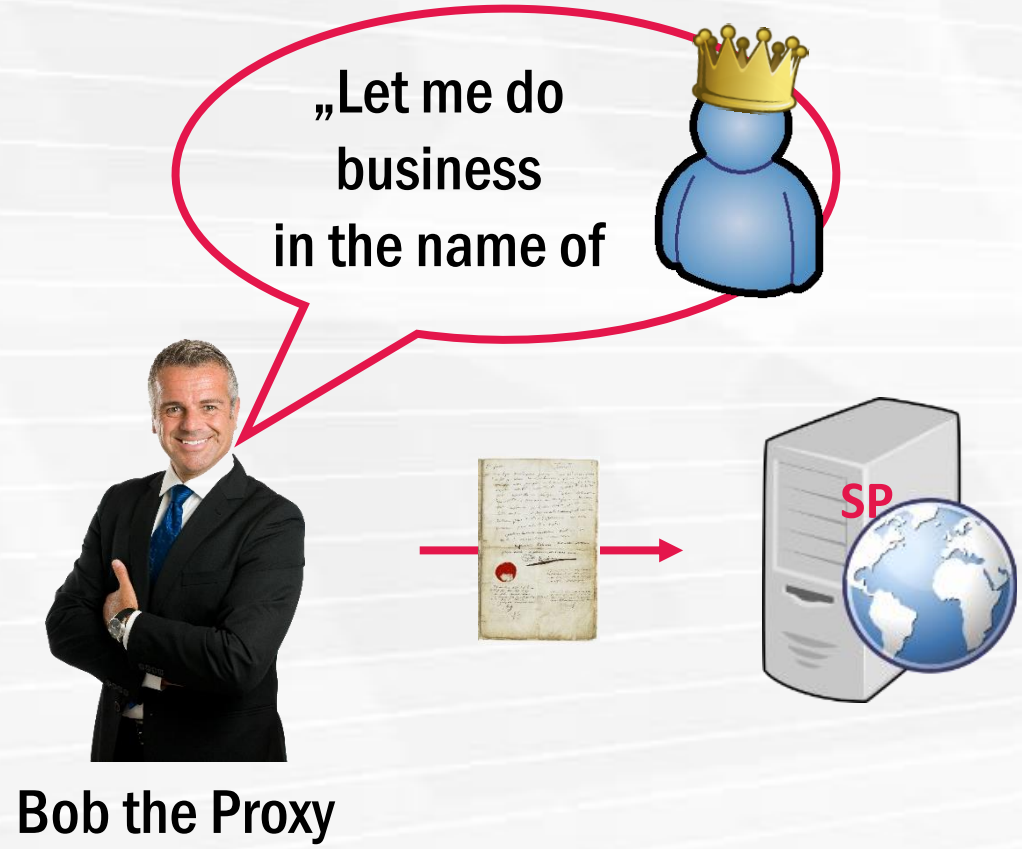
- Person acting on behalf of the mandator
- Rights and roles have been transferred via mandate



Mandates: **Electronic Mandates**

- Many situations require representation; e.g.
  - Parents represent children (by claiming parenthood)
  - Lawyer represents company (by showing card)
- Missing counterpart for digital interaction
- Citizen cards are for citizens
  - Legal persons don‘t have citizen card
  - Legal persons can‘t represent themselves
- → Electronic Mandates

Mandates: Requirements for **Electronic Mandates**



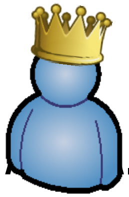
1. How does mandate look like?
2. Where is relationship stored?

Mandates: **Electronic Mandate stored at SP**

= High maintenance costs (for SPs and Mandators)

→ **R1**: SP should not need to store / maintain relationships

Mandates: **Electronic Mandate as Free Text**



Mandate

Me, ..., born on 1.1.1980 living in Graz, authorizes ..., born on the 1.1.1970 living in Vienna, to represent me at the Big-Money-Bank. The mandate covers:

- Dealing in stocks

The mandator is not allowed:

- To execute deals over 1.000.000 Euro

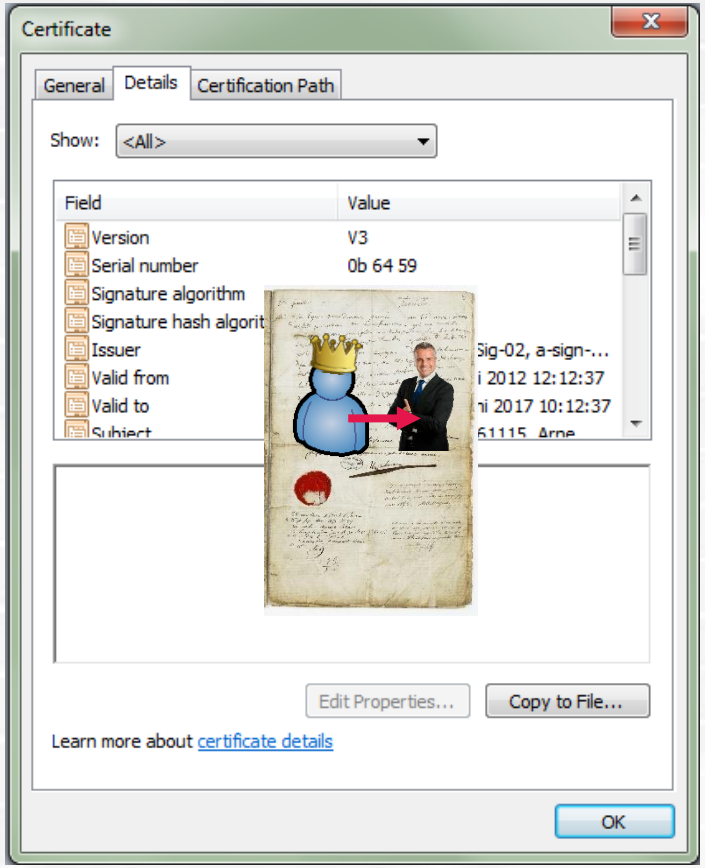
The mandate ends with the 1.1.2015.

Signature Value	[illegible]	
	Signatory	DI Dr. Arne Tauber
	Issuer-Certificate	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	746595
	Method	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:sha1
Verification	Signature verification at: http://www.signature-verification.gv.at	
Note	This document is signed with a qualified electronic signature. According to § 4 art. 1 of the Signature Act it in principle is legally equivalent to a handwritten signature.	
Date/Time-UTC	2012-10-24T11:53:04Z	

Hard for SP to process

→ **R2**: Mandate needs structure

Mandates: Electronic Mandate stored in Certificate



Certificate from Identity Link

Works...

But what if relationship changes?

= New Certificate?

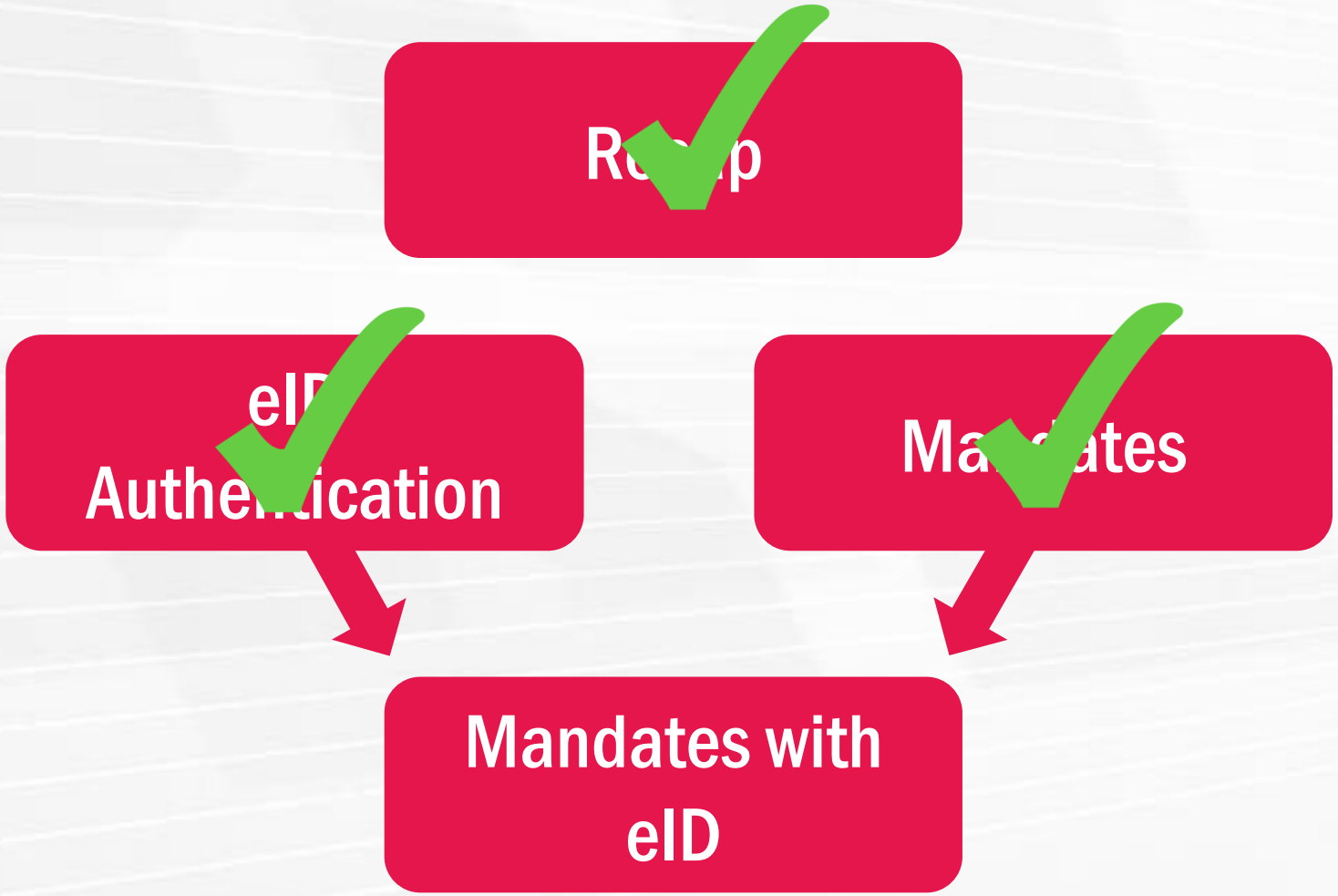
→ **R3**: Certificate attributes should contain immutable information

→ **R4**: Mandates should be revocable

Mandates: Conclusion

- « Mandates enable transfer of rights and roles
- « Mandator transfers rights to proxy
- « Proxy acts on behalf of mandator
- « Electronic mandates enable representation in digital interactions

Outline



Electronic Mandates: Learning Targets

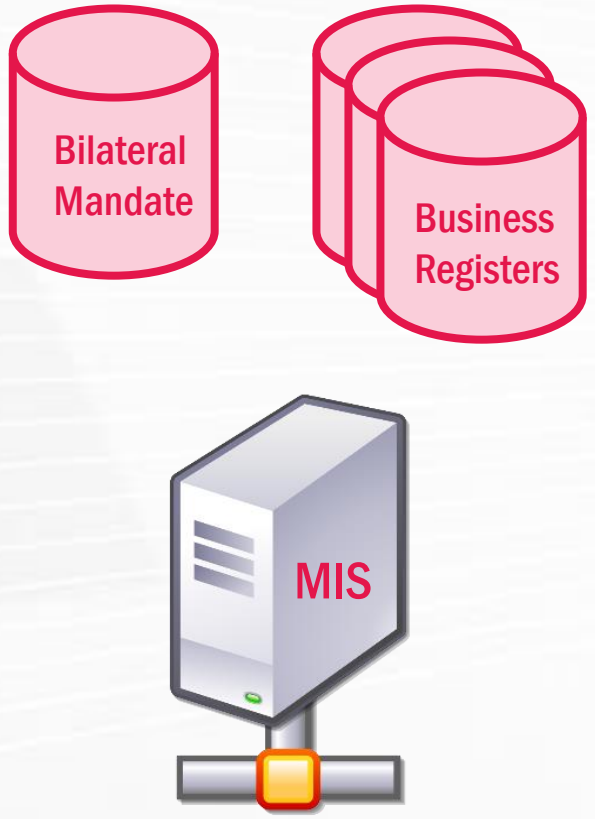
You will be able to ...

- describe the concept of electronic mandates in Austrian eID
- describe how mandates are integrated into the Austrian eID infrastructure
- give an overview on authentication with representative intervention

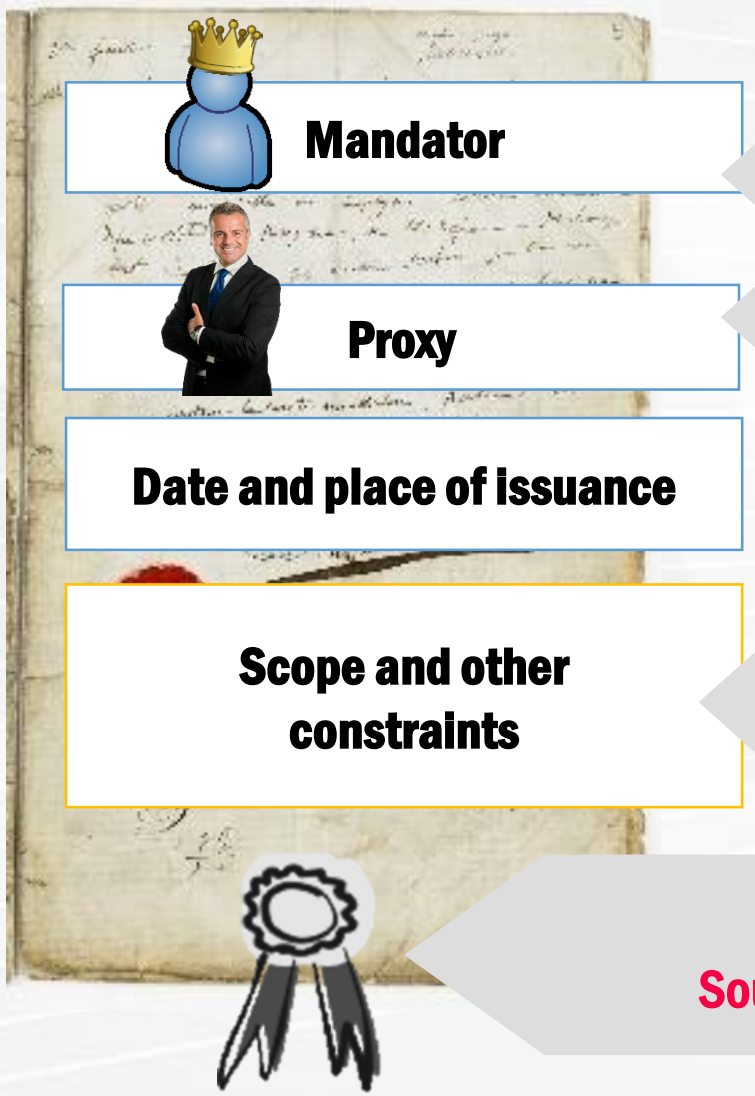
Electronic Mandates in Austrian E-Government

...fulfill requirements R1 – R4

- Relationship: Stored centralized (R1, R4)
  - For natural person: bilateral mandate register
  - For business relationships: business registers
- Issued just in time by Mandate Issuing Service (MIS)
- Mandate: structured XML (R2)
- Immutable right to represent: Stored in certificate
  - Professional representation (lawyer, notary...) (R3)



Electronic Mandate: **Structure**



Mandator

Proxy

Date and place of issuance

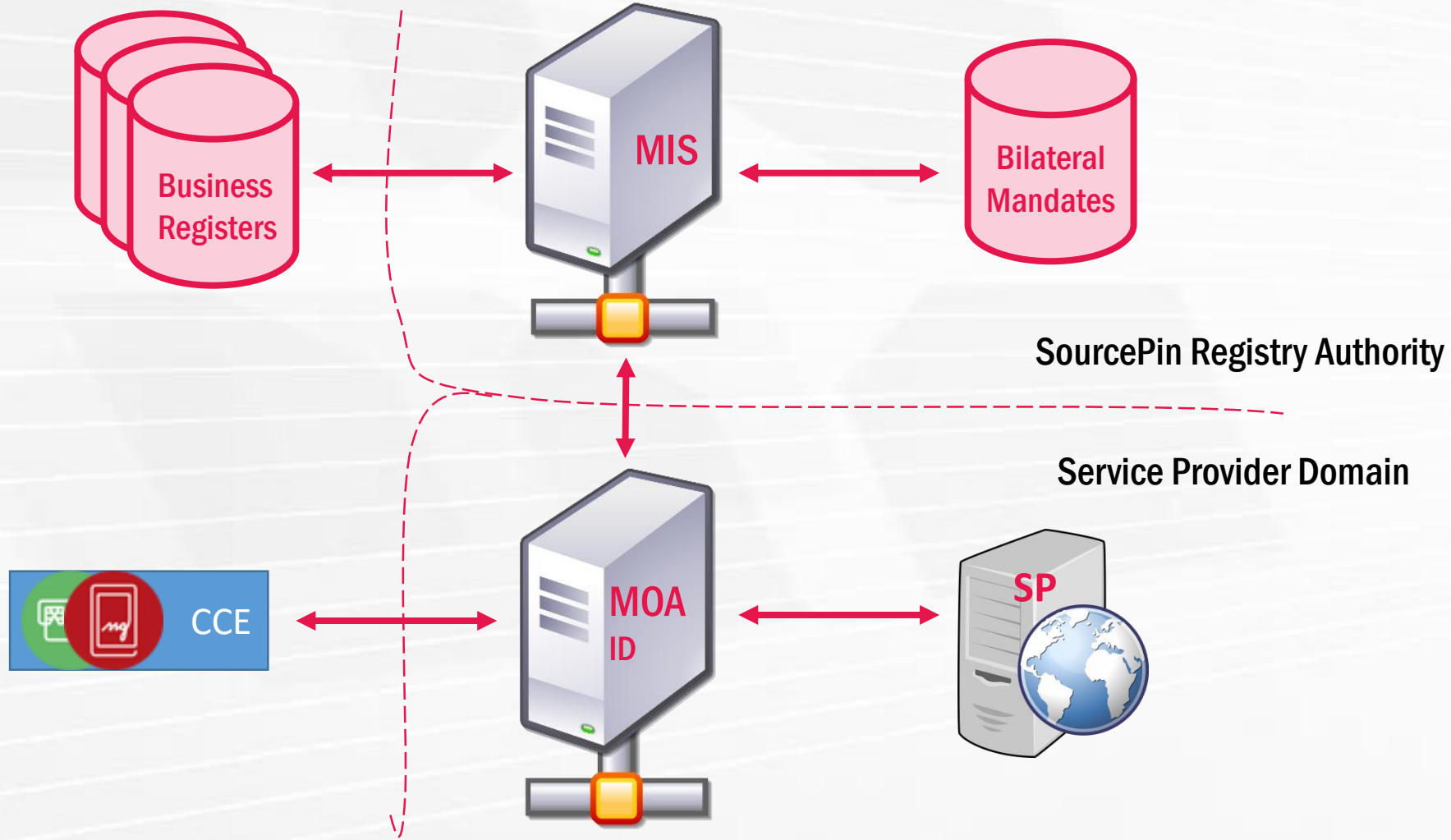
Scope and other constraints

- Name
- Date of birth
- SourcePIN

Short Validity (1d)
→ no need to revoke (R4)

Signed by the
SourcePIN Register Authority

Electronic Mandate: **Architecture**



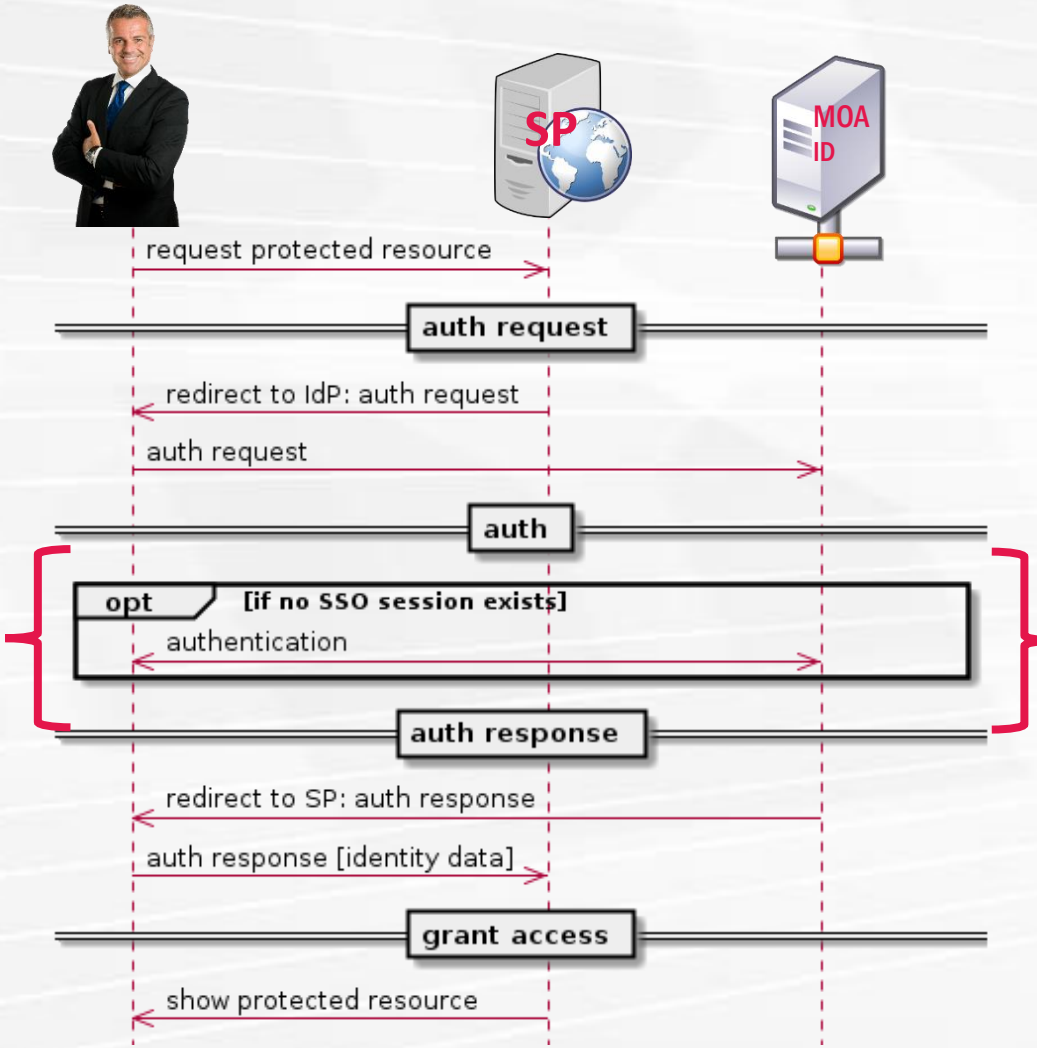
Electronic Mandates: Representative Intervention

« a.k.a: Bob logs in as Alice

Assumption:

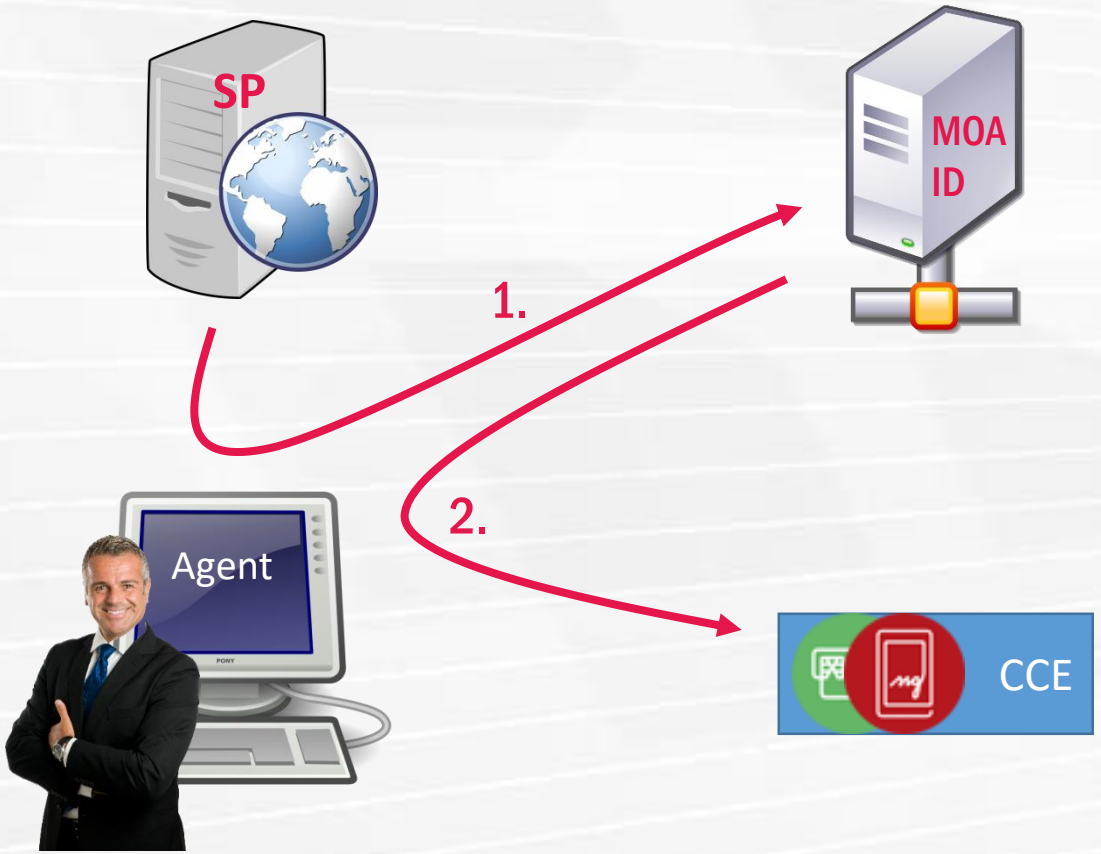
Relationship stored in register

Electronic Mandates: Representative Intervention in IDM



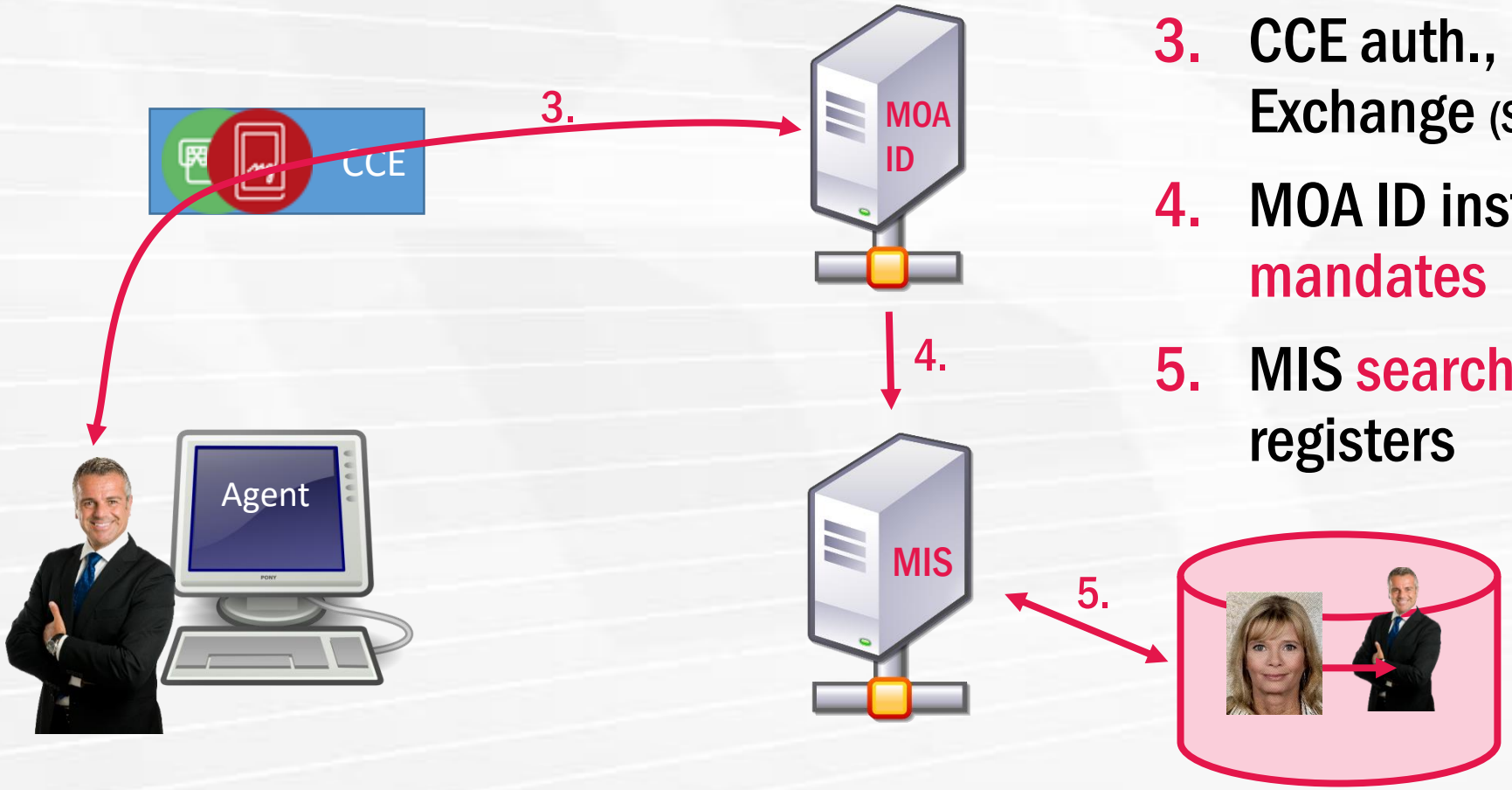
We are here again!

Electronic Mandates: Representative Intervention Flow (1)



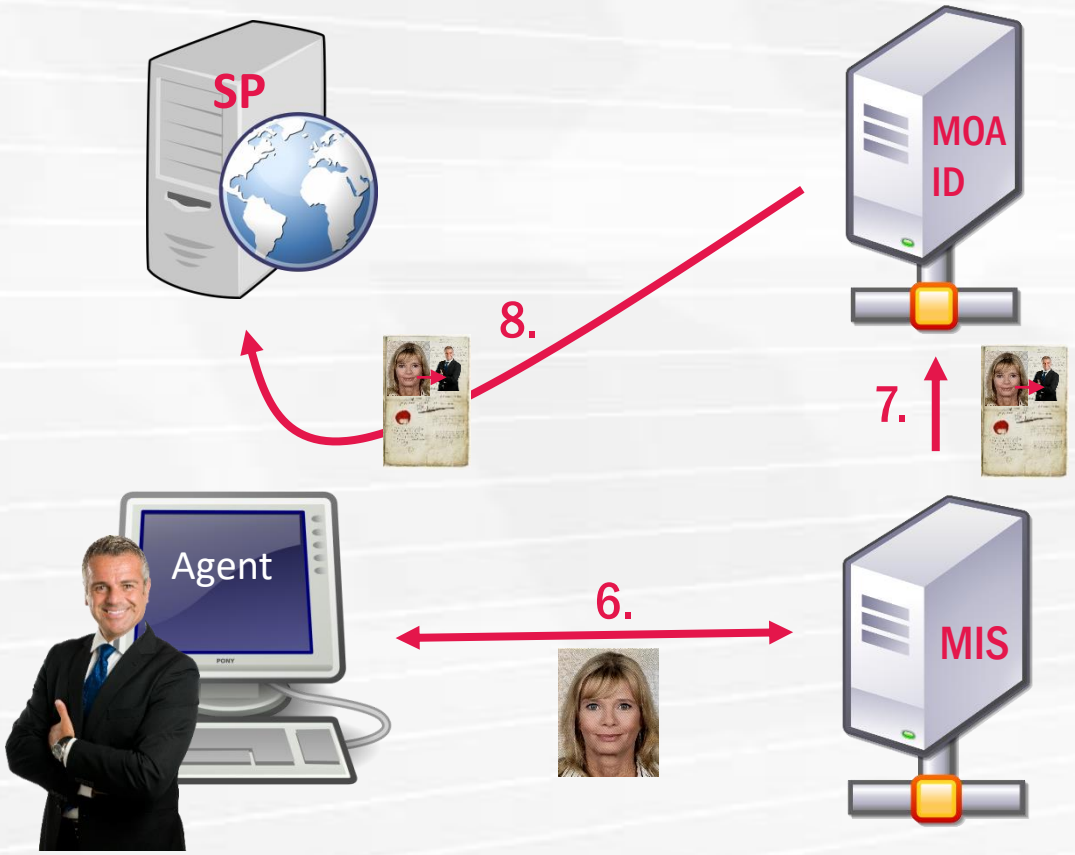
1. Proxy requests CCE selection from MOA-ID
2. Proxy selects CCE, ticks “sign in as representative” (“*in Vertretung anmelden*”) and gets redirected to CCE

Electronic Mandates: Representative Intervention Flow (2)



3. CCE auth., Identity Link & Auth Block Exchange (Steps 3-7 from Slides 13, 14)
4. MOA ID instructs MIS to find mandates
5. MIS searches for mandates in registers

Electronic Mandates: Representative Intervention Flow (3)



6. MIS offers mandates to proxy and proxy selects mandate
7. MIS issues mandate
8. MOA ID generates and forwards assertion and mandate to SP

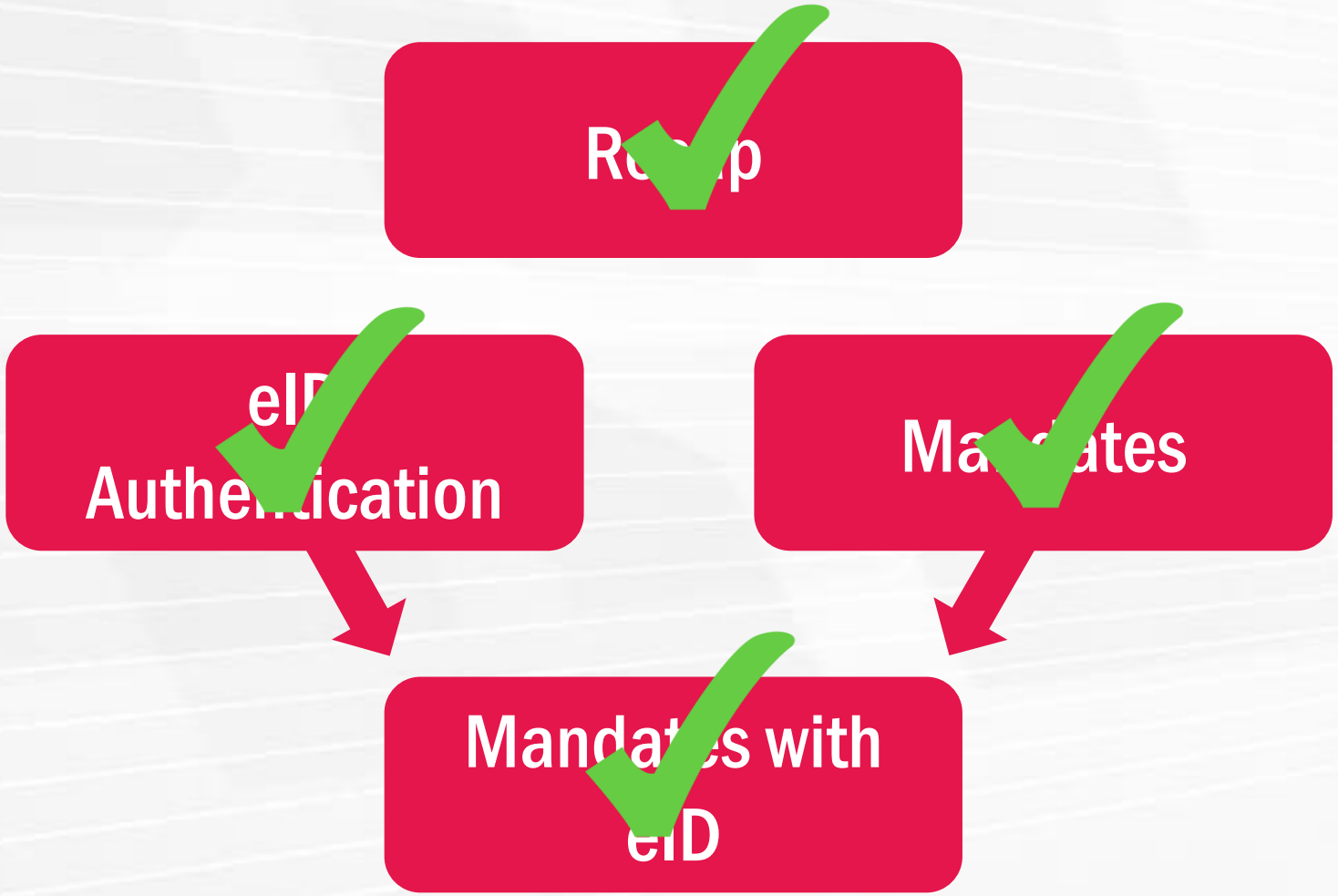
Electronic Mandates: **Side Notes**

- Q: What about professional representation (e.g. lawyer)?
  - Certificate in Identity Link contains "`Profession: Lawyer`" attribute
  - Proxy specifies mandator during flow
  - ⟶ No upfront relationship needed
- Q: How to specify mandate relationship?
  - Mandate Management Service (MMS): for natural person mandators
    https://mms.stammzahlenregister.gv.at
  - Unternehmensservice Portal: for legal person mandators
    https://usp.gv.at

Conclusion

- Austrian eID Infrastructure supports representative intervention via mandates
- Mandate relationships are stored in centralized registers
  - For natural persons: bilateral mandate register
  - For business relationships: business registers
- Professional representation via certificates
- MIS issues mandates on the fly

Outline



References

- E-Government-Law: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
- SourcePIN Register Act: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003943&FassungVom=2009-12-31
- MMS (Productive): https://vollmachten.stammzahlenregister.gv.at/mms/
- MMS (Risk-free Testing): https://vollmachten.stammzahlenregister.gv.at/mms-test/
- MIS (Productive): https://vollmachten.stammzahlenregister.gv.at/mis/
- MIS (Risk-free Testing): https://vollmachten.stammzahlenregister.gv.at/mis-test/
- Demo-Login: http://www.egiz.gv.at/de/testportal
- Electronic mandate specification: http://www.ref.gv.at/Q-BK_Elektronische_Vollmachten.961.0.html
- Example for logins using mandates
  - MyHelp citizen portal: https://www.help.gv.at/
  - Delivery service MeinBrief: https://www.meinbrief.at
  - Delivery service of the Federal Computing Centre (BRZ): https://www.brz-zustelldienst.at/
  - Postserver.at delivery service: http://www.postserver.at
  - DVR-Online: https://dvr.dsk.gv.at/

- Publications:
  - Tauber, A., Rössler, T. Professional Representation in Austrian E-Government, Proceedings of the 8th International Conference EGOV, 2009
  - Leitold H., Tauber A., A Systematic Approach to Legal Identity Management - Best Practice Austria, ISSE 2011
  - Zwattendorfer B., Tauber A., Stranacher K., Cross-Border Legal Identity Management, EGOV 2012
  - Rössler, T. Empowerment through Electronic Mandates – Best Pratice Austria, I3E, Nancy, 2009.
  - Tauber A., Zwattendorfer B., Stranacher K,Elektronische Identität und Stellvertretung in Österreich,DACH 2013