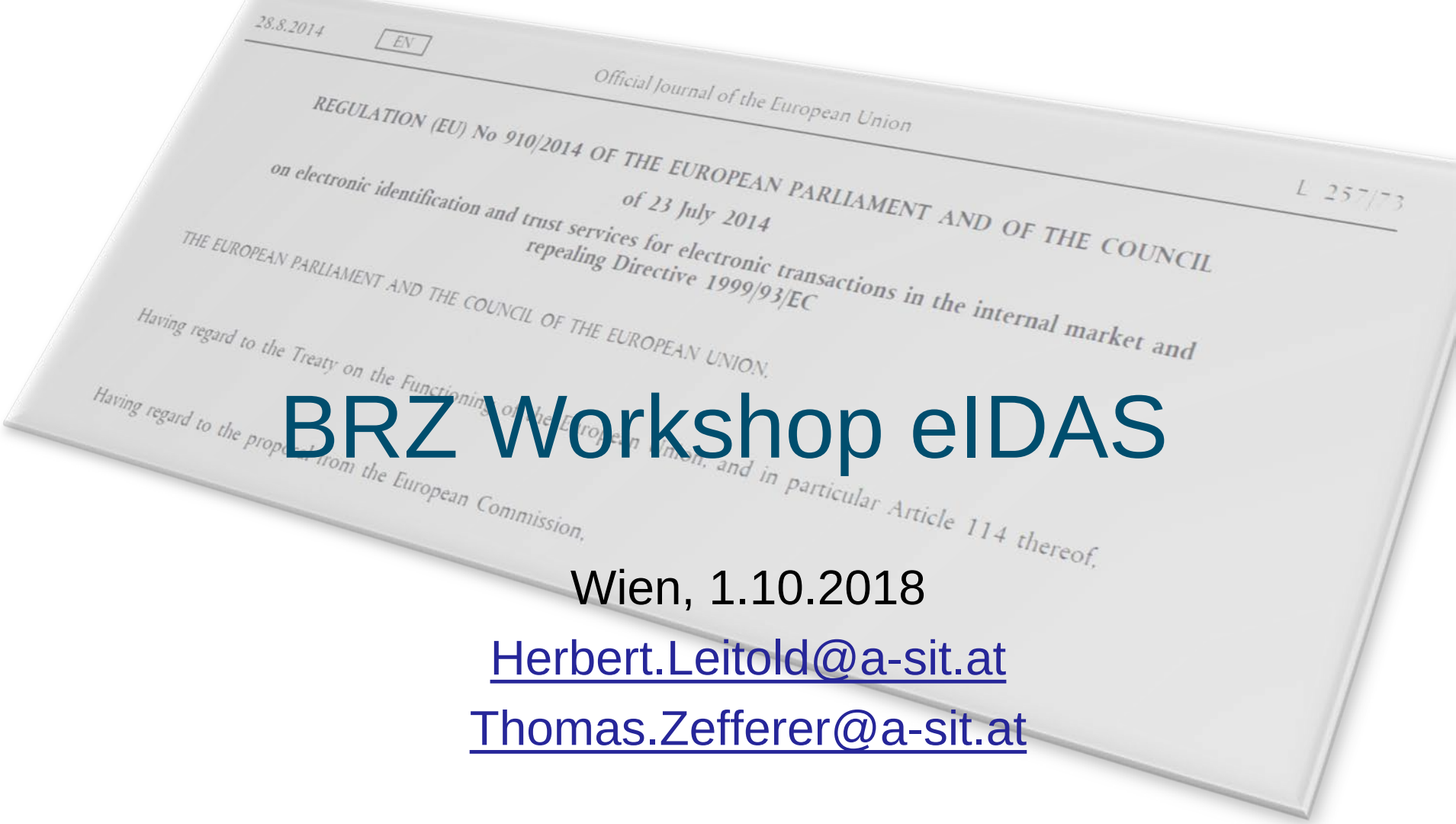


BRZ Workshop eIDAS

Wien, 1.10.2018

Herbert.Leitold@a-sit.at

Thomas.Zefferer@a-sit.at

Folien rechtliches dankenswerter Weise vom BMDW (Peter Kustor, Bernhard Karning)

Über A-SIT und A-SIT Plus

A-SIT

- Gegründet 1999 als gemeinnütziger Verein
  - BMDW
  - OeNB
  - TU Graz
  - BRZ
  - Donau-Uni Krems
- Beratung von Behörden
- eIDAS Zertifizierung und Konformitätsbewertung
- Zahlungssystemaufsicht
- Technologiebeobachtung

A-SIT Plus GmbH

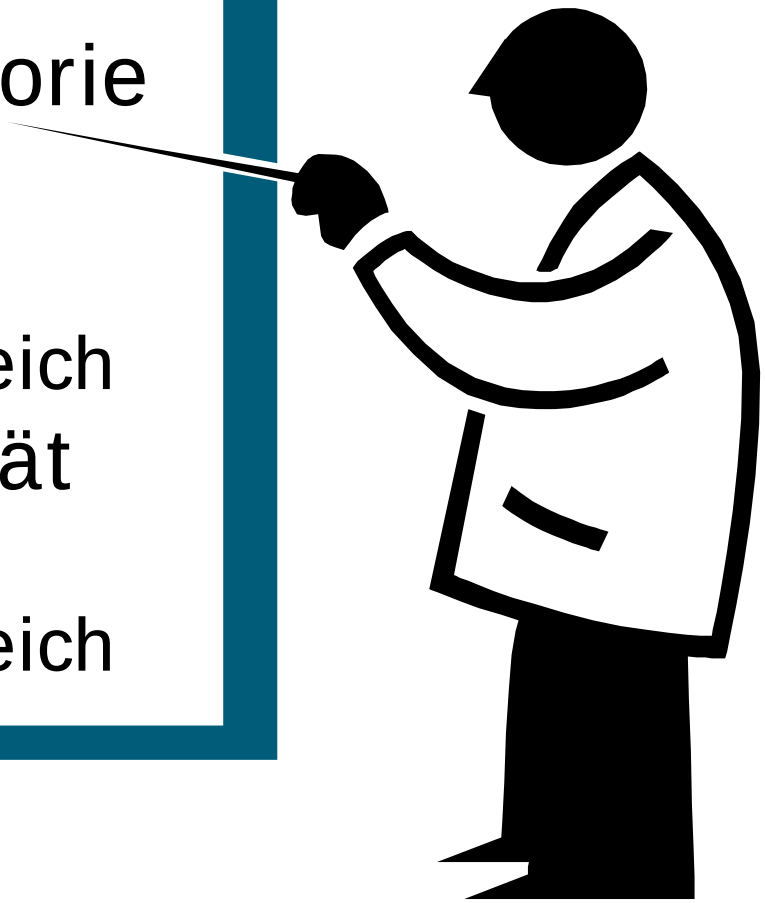
- Gegründet 2015
  - In 100% Eigentum von A-SIT
- Trennung von
  - gemeinnütziger oder in Gesetzen vorgesehener Tätigkeit im Verein
  - Wirtschaftliche Tätigkeit, auch mit Privatwirtschaft, in GmbH
- Aktuelle Schwerpunkte
  - Mobiltechnologien
  - eID und Signatur
  - Risikoanalyse und ISMS

Elevator Pitch

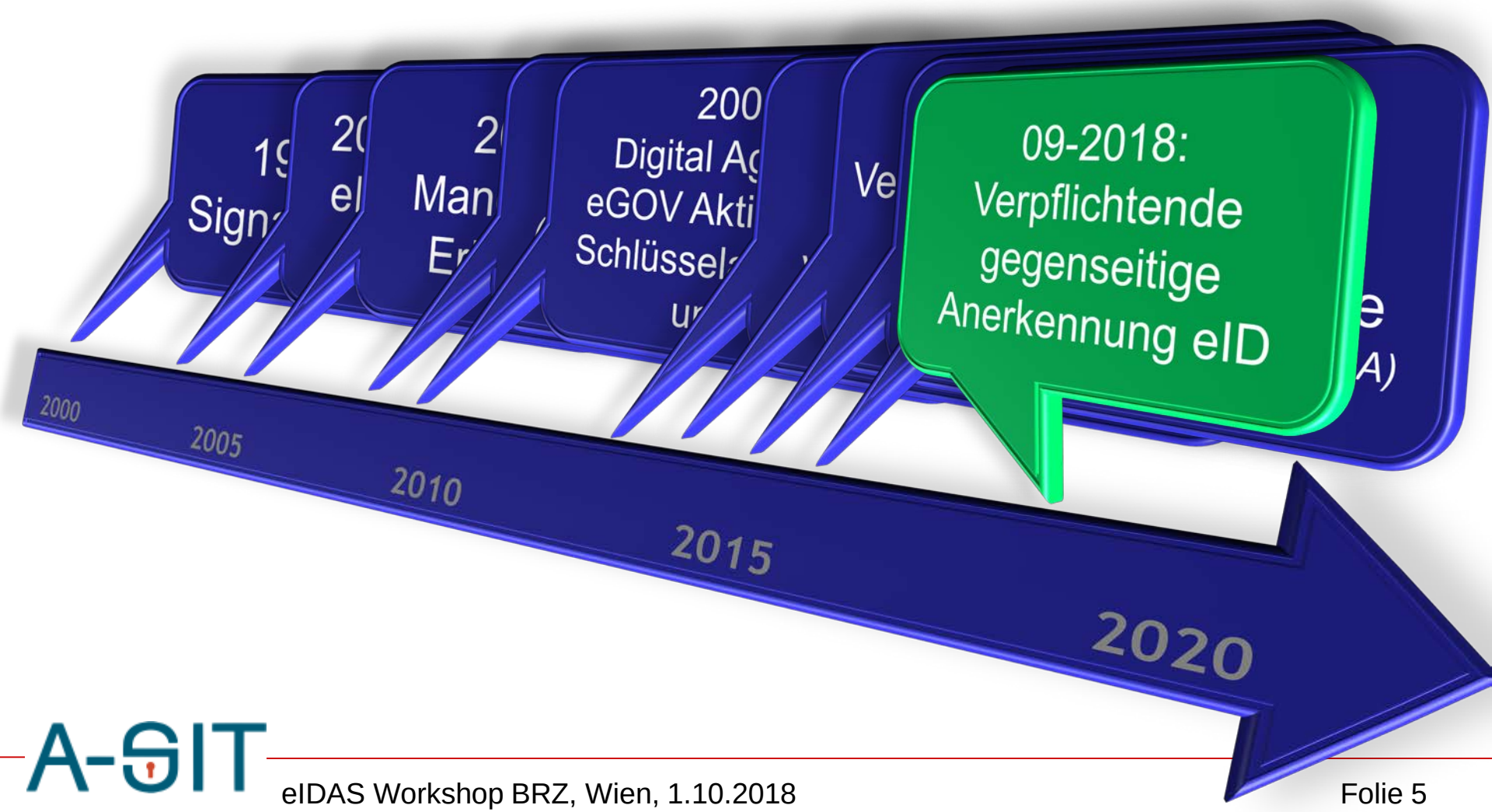
- Wesentliche, mitzunehmende Punkte:
  - eIDAS vollständig in Kraft
    - Vertrauensdienste seit 2016, eID seit 09/2018
  - Vertrauensdienste stark harmonisiert
    - sofern Standards in Durchführungsrechtsakten
    - erst zu Signaturen der Fall (bzw. Trust Lists)
  - eID unter MS-Verantwortung notifizierbar
    - Landschaft in EU heterogen
    - Interoperabilität über Proxies / Middleware
  - Anerkennungsverpflichtung öff. Anwendungen
    - Signaturformate (XAdES, CAdES, PAdES, ASiC)
    - eIDs (2018: DE, 2019: EE, ES, HR, IT, LU; 2020: UK…)
    - in Österreich über aktuelle MOAs (+PDF-AS, ERnP, …)

Inhalte

- Hintergrund und Historie
- Vertrauensdienste
  - Grundlagen
  - Umsetzung in Österreich
- Elektronische Identität
  - Grundlagen
  - Umsetzung in Österreich



Sig-RL und eIDAS auf der Zeitlinie



Politische Vorfeld-Entscheidungen

- Manchester-Erklärung (2005)
  - By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available **under the responsibility of the Member States** but recognised across the EU
- Digital Agenda Key Actions (2010)
  - KA3: In 2011 propose **a revision of the eSignature Directive** with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems;
  - KA16: Propose by 2012 a Council and Parliament Decision to ensure **mutual recognition of e-identification and e-authentication** across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector);

Ergebnis ist …

- Manchester-Erklärung (2005)
  - By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available **under the responsibility of the Member States** but recognised across the EU
- Digital Agenda Key Actions (2010)
  - KA3: In 2011 propose **a revision of the e-Signature Directive** with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems;
  - KA16: Propose by 2012 a Council and Parliament Decision to ensure **mutual recognition of e-identification and e-authentication** across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector);

… mit eIDAS ein gemeinsamer Rechtsakt

Eckpunkte des Ergebnisses

- Ein Rechtsakt für die beiden Themen eSignatur und eID
- Zusätzlich: weitere „Vertrauensdienste“
- Die SigRL wird komplett ersetzt
- Typ des Rechtsakts: Verordnung

Folie mit Dank vom BMDW

„eIDAS-VO“: Überblick

- Kapitel I: Allg. Bestimmungen
- Kapitel II: **Elektronische Identifizierung**
- Kapitel III: **Vertrauensdienste**
- Kapitel IV: Elektronische Dokumente

- Kapitel V: Befugnisübertragungen und Durchführungsbestimmungen
- Kapitel VI: Schlussbestimmungen

- 4 Anhänge (Anforderungen an qual. Zertifikate/ Signaturerstellungseinheiten/ el. Siegel/ Website-Authentifizierung)

Folie mit Dank vom BMDW

Grobe Gegenüberstellung

Vertrauensdienste

- Weitgehend harmonisiert, Durchführungsrechtsakte können Normen festlegen
- Anbieter können privat oder öffentlich sein
- Staatliche Aufsicht, Haftung des VDA
- Konformitätsbewertungen
- Anerkennung Signaturformate

eID

- Koordination, MS erstellen Standards zu Sicherheit und Interoperabilität
- Notifizierung eID obliegt gänzlich den MS
  - IdP privat oder öffentlich
- Staatliche Aufsicht Haftung MS/IdP
- (*unverb.*) Peer-Review
- Anerkennung notif. eID in eID-fähigen öff. Anwendungen (*LoA high/sub.*)

Bedarf grenzüberschreitend BürgerInnen?

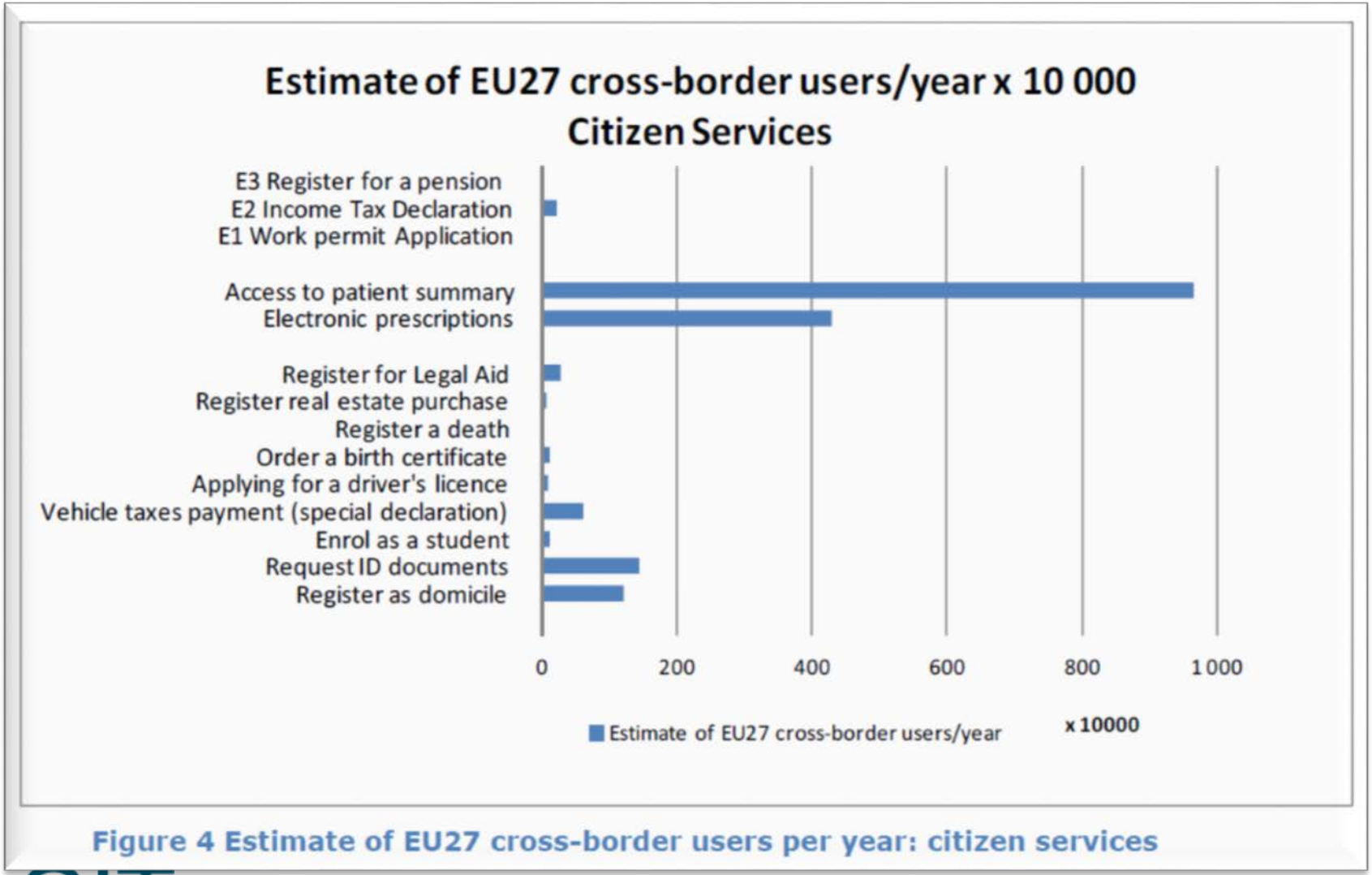


Figure 4 Estimate of EU27 cross-border users per year: citizen services

Quelle: EC Study on Analysis of the Needs for Cross-Border Services … (2013)

Bedarf grenzüberschreitend Wirtschaft?

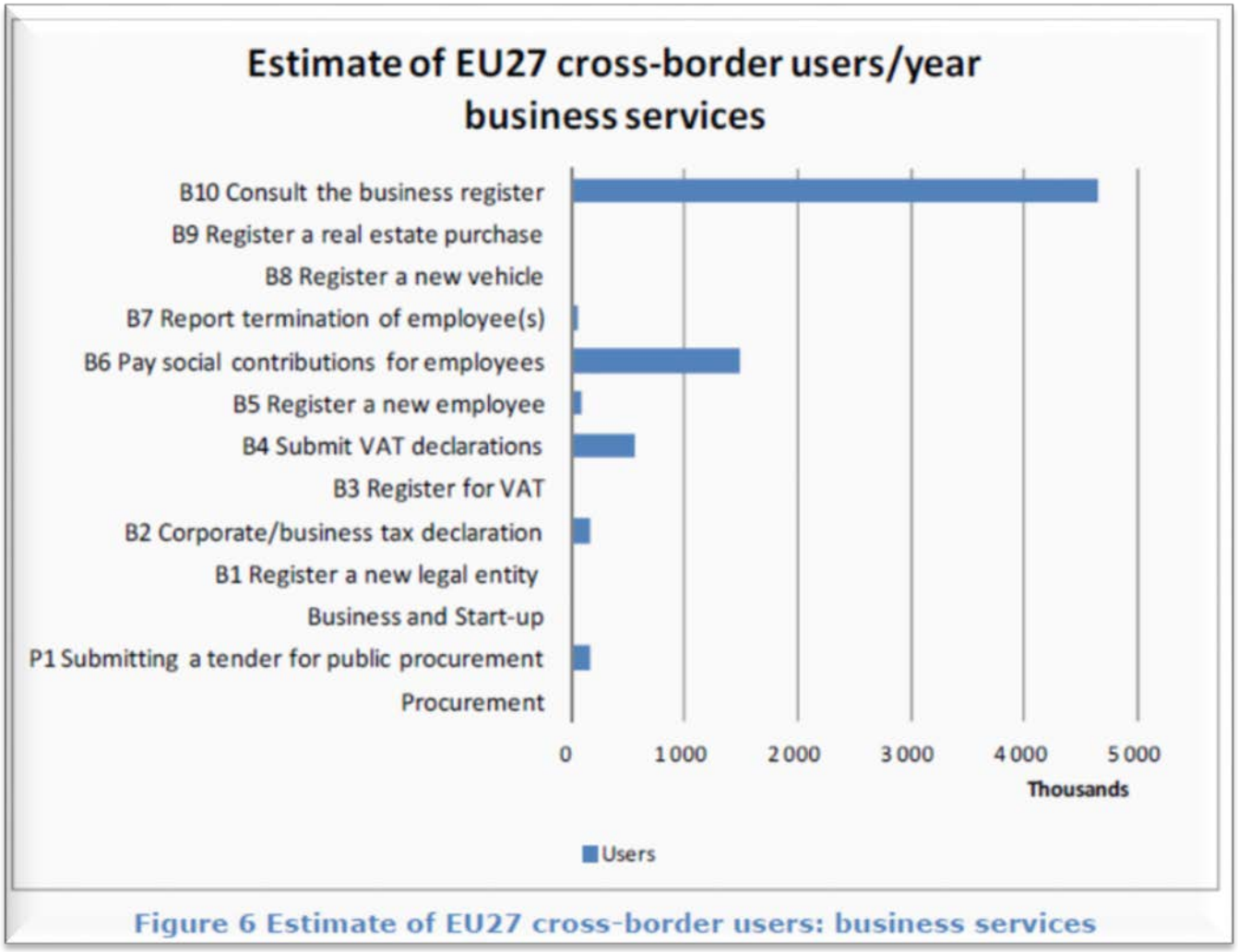
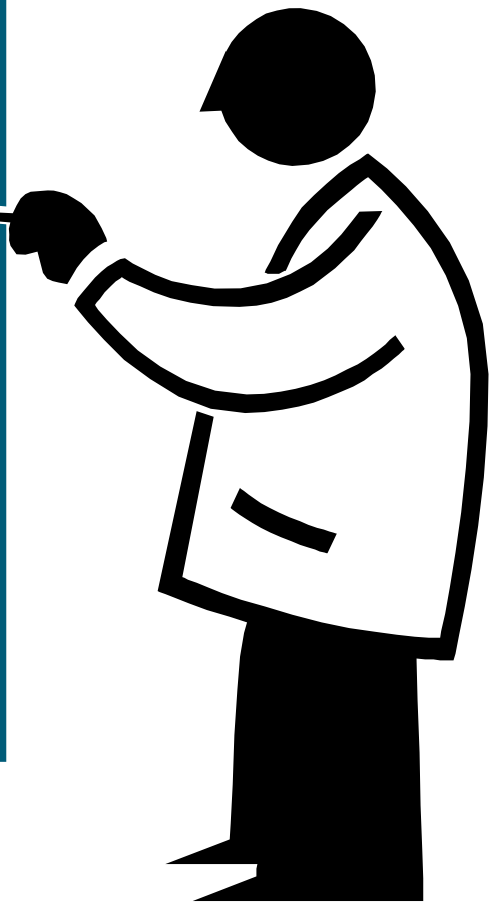


Figure 6 Estimate of EU27 cross-border users: business services

Quelle: EC Study on Analysis of the Needs for Cross-Border Services … (2013)

Inhalte

- Hintergrund und Historie
- **Vertrauensdienste**
  - Grundlagen
  - Umsetzung in Österreich
- Elektronische Identität
  - Grundlagen
  - Umsetzung in Österreich



Vertrauensdienste

- Abgeschlossene Liste
  - Elektronische Signatur (*natürliche Person*)
  - Elektronische Siegel (*jur. Person, weiter Begriff*)
  - Elektronische Bewahrungsdienste
  - Elektronische Validierungsdienste
  - Elektronische Zeitstempeldienste
  - Dienste für die Zustellung elektronischer Einschreiben
  - Website Authentifizierung

Gemeinsamkeiten Vertrauensdiensteanbieter (VDA)

- Qualifizierte / Nicht-qualifizierte VDA
- Haftung: Beweislastumkehr bei QVDA
- Aufsicht QVDA, reaktive (ex post) Maßnahmen VDA
- Sicherheitsanforderungen an VDA mit Notifikationspflichten bei Kompromittierungen
- Vorabgenehmigungsverfahren für QVDA mit Konformitätsprüfungen
- Vertrauensliste (TL) mit konstitutiver Wirkung
- „EU-Vertrauenssiegel“ für qual. Vertrauensdienste
- Anerkennung von qual. VDA aus Drittstaaten nur bei Abkommen mit EU

Folie mit Dank vom BMDW

Gemeinsamkeiten Vertrauensdiensteanbieter (cntd.)

- Anforderungen an QVDA betreffend
  - Identifikationsmechanismen bei Ausgabe von qual. Zertifikaten
  - Verlässlichkeit der MitarbeiterInnen
  - Finanzielle Ressourcen/ Versicherung
  - Informationspflichten
  - Sicherheitsanforderungen an die Systeme und Produkte
  - Dokumentationspflichten
  - Verzeichnis- und Widerrufsdienste etc.
  - „Notfall-(Einstellungs)pläne“ zur Sicherstellung der Kontinuität

- Allgemeine Bestimmungen zu Datenschutz, Accessibility, Strafbestimmungen

Folie mit Dank vom BMDW

Vertrauenslisten (TL)

- Jeder MS führt Vertrauensliste (TL) seiner Q(VDA)
- EK führt Liste der MS-TLs
- Aktuell (26.9.18): 238 VDAs EWR-weit, 214 QVDA
  - Q-Zert Signatur: 193 in 27 MS *(inkl. IS, NO, LI)*
  - Q-Zert Siegel: 82 in 22 MS
  - Q-Bewahrung. (Sig/Siegel): 9 in 7 MS
  - Q-Validierung (Sig/Siegel): 9 in 9 MS
  - Q-Zeitstempel: 94 in 21 MS
  - Q-Zustellung: 9 in 5 MS
  - Q-Zert Webserver (TLS): 35 in 16 MS

Siehe TL Browser https://webgate.ec.europa.eu/tl-browser/#/

Durchführungsrechtsakte

- Vertrauenssiegel *(EU) 2015/806*
- Vertrauenslisten *(EU) 2015/1505*
  - Format (ETSI TS 119 612 v2.1.1) und Notifizierung
- QSCD-Zertifizierung *(EU) 2016/650*
  - Smartcard-artig: Common Criteria verpflichtend
  - Fernsignatur: notifizierte, alternative Verfahren der MS
- Signaturformate *(EU) 2016/650*
  - Anerkennung XAdES, PAdES, CAdES, ASiC (-B, -T, -LT; nicht -LTA)
  - Prüfdienst für alternative Formate
    - www.signaturpruefung.gv.at
- *Weitere DRA möglich (>20), jedoch noch nicht diskutiert*

Qualifizierte Signatur

- In Substanz zur Signatur-RL gleich, einige neue Punkte:
  - Klärung Fernsignatur
    - Betrieb QSCD durch QVDA
  - QSCD Zertifizierungspflicht
    - nach gemein. Standards, wenn in DRA (dzt. Smartcard-artige)
  - Verpflichtende Konformitäts-bewertung QVDA alle 2 J.
  - Formate in öffentl. Diensten

aus https://www.eid.as/tsp-map/#/
© emsec

Qualifizierte Siegel

- Signatur der jur. Person
  - Rechtswirkung qual. Siegel national beschränkt (in Ö)
    - Kein Äquivalent zu „gleicher Wirkung wie Schriftlichkeit“
  - Amtssignatur (nicht qual.)
- Technisch kein wesentlicher Unterschied zur Signatur
  - ggf. Schutz Verwendung QSCD durch Dritte anders

aus https://www.eid.as/tsp-map/#/
© emsec

Qualifizierte Bewahrungsdienste

- Verlängerung Vertrauens-würdigkeit qual. Signatur oder qual. Siegel über technische Gültigkeit hinaus
- Noch keine Durchführungs-rechtsakte, damit keine gemeinsamen Norm(en)

aus https://www.eid.as/tsp-map/#/
© emsec

Qualifizierte Validierungsdienste

- Prüfung von qual. Signatur, oder qual. Siegel
- Allg. Anforderungen, wie bisher in Anhang IV Sig-RL
  - z.B. Prüfung zum Zeitpunkt des Signierens
- Noch keine Durchführungs-rechtsakte, damit keine gemeinsamen Norm(en)

aus https://www.eid.as/tsp-map/#/
© emsec

Elektronische Zeitstempeldienste

- Vermutung der Richtigkeit von Datum/Zeit und Unversehrtheit verbundene Daten
  - Verknüpft Daten mit Zeit
  - Benötigt korrekte Zeitquelle, die mit Weltzeit verknüpft ist
- Noch keine Durchführungsrechtsakte, damit keine gemeinsamen Norm(en)

aus https://www.eid.as/tsp-map/#/
© emsec

Zustellung elektronischer Einschreiben

- Identifizierung von
  - Absender „hohes Maß an Vertrauenswürdigkeit“
  - Empfänger „sicher gestellt“
- Ausschließen Veränderung von Daten (und Anzeige, falls doch)
- Sende-/Empfangszeit mit qualifizierten Zeitstempeln
- Noch keine Durchführungs-rechtsakte, damit keine gemeinsamen Norm(en)

aus https://www.eid.as/tsp-map/#/
© emsec

Webseiten Authentifizierung

- Noch keine Durchführungs-rechtsakte, damit keine gemeinsamen Norm(en)
- Frage der Integration und Erkennbarkeit im Browser

aus https://www.eid.as/tsp-map/#/
© emsec

Umsetzung in Österreich rechtlich (I/II)

- Signatur- u. Vertrauensdienstegesetz (SVG)
  - Schriftlichkeit bis auf
    - Letztwillige Verfügungen
    - Familien-/Erbrecht und Bürgschaft Privater (außer Belehrung durch Notar oder Rechtsanwalt zu Rechtsfolgen)
  - Kein Ausschluss Signatur in AGB (für Verbraucher)
  - Klärung Zertifikats-Aussetzung (in eIDAS ermöglicht)
  - Weiterführung durch Bund, wenn öffentliches Interesse
  - Aufsicht Telekom-Control-Kommission + RTR
  - Kostenloser Validierungsdienst durch RTR
    - www.signaturpruefung.gv.at

Umsetzung in Österreich rechtlich (II/II)

- Signatur- u. Vertrauensdiensteverordnung (SVV)
  - Gebühren Aufsicht
  - Anforderungen an VDA und Personal
  - Identifikation Unterzeichner über Lichtbildausweis oder Verlässlichkeit wie Zustellung zu eigenen Handen
  - Regelungen Neuausstellung eines Zertifikats mit selben Inhalten (nur andere Serien-Nr., außer bei Übernahme)
  - Anforderung Zertifikatsdatenbank (zB Übernahme-fähig) und Zugänglichkeit Widerruf
  - Eignung A-SIT als Bestätigungsstelle

Umsetzung Österreich technisch

- Relevant sind v.a. Signaturformate
  - Prüfung X-/P-/CAdES und ASiC
    - mit MOA-SP ab v3.1.*x* (seit 06/2017), aktuell ist v3.1.1
    - Allgemein verfügbarer Prüfdienst
      - Von A-SIT erstellt, Betrieb RTR auf www.signaturpuefung.gv.at
      - Manuell oder Webschnittstelle (registrierte Anwendungen)
  - Erstellung der Signaturen
    - XAdES/CAdES mit MOA-SS (keine qual. Signatur)
    - PAdES mit PDF-AS (seit v4 2014) oder zB PDF-OVER
    - So noch PDF-AS „binär“ oder „text“ verwendet: **Umstellen!**
  - Jeweils OpenSource auf JoinUp.eu
- Auch: CEF Building Block DSS der EU

Inhalte

- Hintergrund und Historie
- Vertrauensdienste
  - Grundlagen
  - Umsetzung in Österreich
- **Elektronische Identität**
  - Grundlagen
  - Umsetzung in Österreich

Erste europ. Projekte v.a. eID Karten

Frühe (Karten)Projekte späte 90er frühe 2000er

– Finnische eID: Dezember 1999

– Estnische eID: seit Jänner 2002

– Bürgerkarte: OCG 2003; Bankomat/e-card/A1Sig. 2005

– Italien CIE/CNS: Pilot ab 2003 (CIE)

– Belgische eID: seit 2.HJ 2003

Ein paar aktuelle Beispiele

AT: Bürgerkarte/Handy-Signatur wird „E-ID“

- Ähnliches wie Handy-Signatur auch in IT, PT, SI

DE: Neuer Personalausweis (seit 2010)

- eID am Personalausweis auch in BE, EE, LU, PT, …

IT: Statt CIE/CNS nun SPID

- 8 Anbieter, 3 LoAs mit Karten und Server-Lösungen

UK: GOV.UK verify

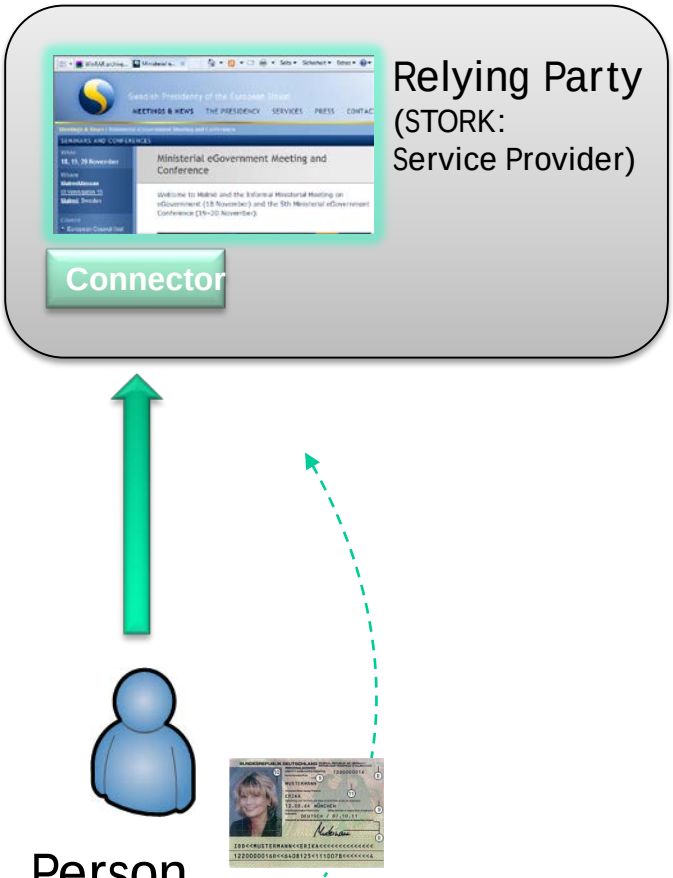
- 7 privatwirtschaftliche IdPs

EE: ID-kaart, Mobiil-ID, eResidency, …

DK: NemID, und in weiteren MS viel mehr …

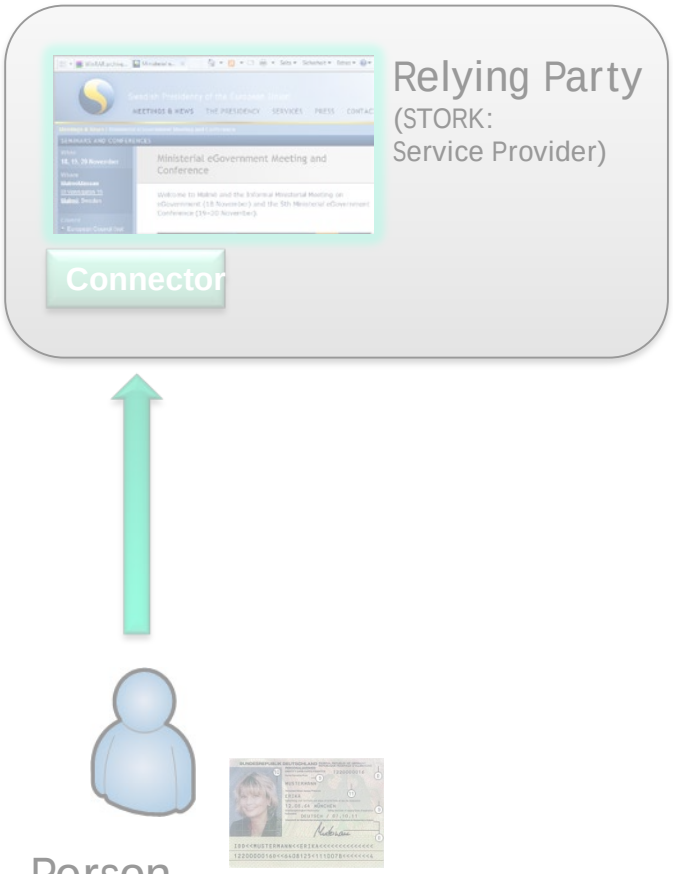
Vorgriff auf Architektur:
Direkte vs. indirekte Authentifizierung

Direct Authentication

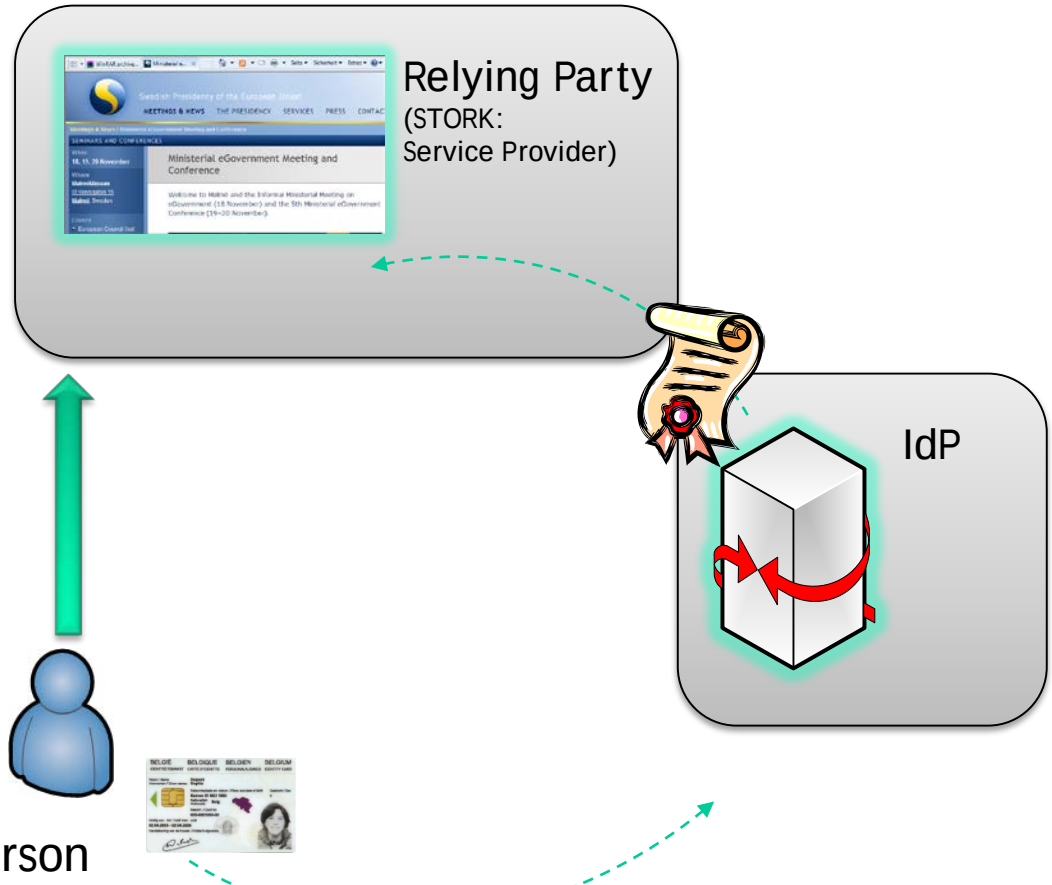


Vorgriff auf Architektur:
Direkte vs. indirekte Authentifizierung

Direct Authentication



Indirect (IdP-based) Authentication



Direkt / indirekt – Proxy / middleware

- Direct authentication:
  - AT urspr. mit MOA-ID, DE mit „eID Server“
  - AT Handy-Signatur bereits *IdP-artiges* Element
- Grenzüberschreitend war im STORK-Pilot
  - AT und DE „middleware“ (direkt)
  - Alle anderen MS „Proxy“ (indirekt)
- Mit eIDAS (dzt. Stand)
  - DE „Middleware“, alle anderen „Proxy“

eIDAS eID Kernelemente

- MS können ihre eIDs notifizieren
  - Natürliche Person, juristische Person, Vertretung
  - 3 Level of Assurance: low, substantial, high
  - Peer-Review anderer MS (ohne formelle Konsequenz)
  - Haftung für:
    - Identitätsdaten (minimum/optional data): MS haftet
    - elektronisches Identifizierungsmittel: Aussteller haftet
    - Authentifizierungsverfahren (Proxy): Betreiber haftet, (Middleware?)
  - notif. MS kann Bedingungen für privatwirtschaftliche RPs stellen
- Alle MS müssen
  - notif. eID LoA high und LoA substantial in öffentlichen Anwendungen akzeptieren, unabhängig davon, ob sie eigene eIDs notifizieren
    - Frist: 1 Jahr ab EK-Veröff. Notifizierung (18-20 Monate ab Prä-Notifiz.)
    - in Ö 6 Monate nach technischer Möglichkeit

Durchführungsrechtsakte

- Notifizierung *(EU) 2015/1984*
  - Vorgang, Formular
- Interoperabilität *(EU) 2015/1501*
  - Führt eIDAS Nodes (Knoten) ein
  - Ermächtigung Kooperationsnetzwerk für technische Spezifikationen
  - Sicherheit, Logging, Datenschutz
  - Minimum Data Set, optionale Daten als „Matching Data“
- LoA Anforderungen *(EU) 2015/1502*
  - Anmeldung
  - Verwaltung eID
  - Authentifizierung
  - Management und Organisation

Minimum Data Set

- Nat. Person zumindest
  - dzt. Familienname(n)
  - dzt. Vorname(n)
  - Geburtsdatum
  - eindeutige Kennung „*möglichst dauerhaft*“

Optional:

  - *derzeitige Anschrift*
  - *Vor-/Familienname bei Geburt*
  - *Geburtsort*
  - *Geschlecht*

- Jur. Person zumindest
  - dzt. amtliche Bezeichnung
  - eindeutige Kennung „*möglichst dauerhaft*“

Optional:

  - *derzeitige Anschrift*
  - *Umsatzsteuer-Identifikationsn.*
  - *Steuerregisternummer*
  - *2009/101/EG 3.1 (Firmenbuch)*
  - *LEI*
  - *EORI-Nr.*
  - *Verbrauchsteuernummer*

Über MDS hinausgehende Attribute

- Nat. Person zumindest
  - dzt. Familienname(n)
  - dzt. Vorname(n)
  - Geburtsdatum
  - eindeutige Kennung *„möglichst dauerhaft“*

Optional:

  - *derzeitige Anschrift*
  - *Vor-Familienname bei Geburt*
  - *Geburtsort*
  - *Geschlecht*

- Jur. Person zumindest
  - dzt. amtliche Bezeichnung
  - eindeutige Kennung *„möglichst dauerhaft“*

Optional:

  - *derzeitige Anschrift*
  - *Umsatzsteuer-Identifikationsn.*
  - *Steuerregisternummer*
  - *2009/101/EG 3.1 (Firmenbuch)*
  - *LEI*
  - *EORI-Nr.*
  - *Verbrauchsteuernummer*

Spezifikationen erlauben Transport weiterer Attribute, sog. „domain specific attributes“

Herausforderung „unique identifier“

- Nicht alle MS haben persistente Identifikatoren bzw. Abbildung nicht immer ein-eindeutig
  - z.B. DE: Identifikator an Karte gebunden
    - Person hat mit neuem Personalausweis neuen Identifikator
  - z.B. UK: Identifikator je IdP eindeutig
    - Person kann mehrere Identifikatoren parallel haben
- Ö erstellt auf Basis eIDAS Stammzahl im ERnP
  - Matching bei erstem Zugang: Person im ERnP bekannt?
  - Matching bei Wechsel des Identifikators
- Für Matching optionale Attribute wesentlich
  - z.B. bei DE Name bei Geburt und Ort der Geburt

Architektur: eIDAS Knoten (Nodes)

Ausgehende eID

- Jeder MS betreibt einen Node „*eIDAS Service*“, InhaberInnen der eigenen eIDs authentifiziert
- Auch als „Proxy Service“ bezeichnet
- Ausnahme Middleware: Node (eIDAS Service) vom empfangenden MS betrieben (dzt. nur DE)

Einkommende eID

- Jeder MS betreibt einen *oder mehrere* „eIDAS Connector“ der für eigene Anwendungen (Relying Parties) InhaberInnen ausl. eIDs an deren eIDAS Node leitet
- ad „mehrere“: eIDAS Connectoren können sektorell sein
  - z.B. Banken, Gesundheit, ..

Architektur: eIDAS Knoten (Nodes)

Ausgehende eID

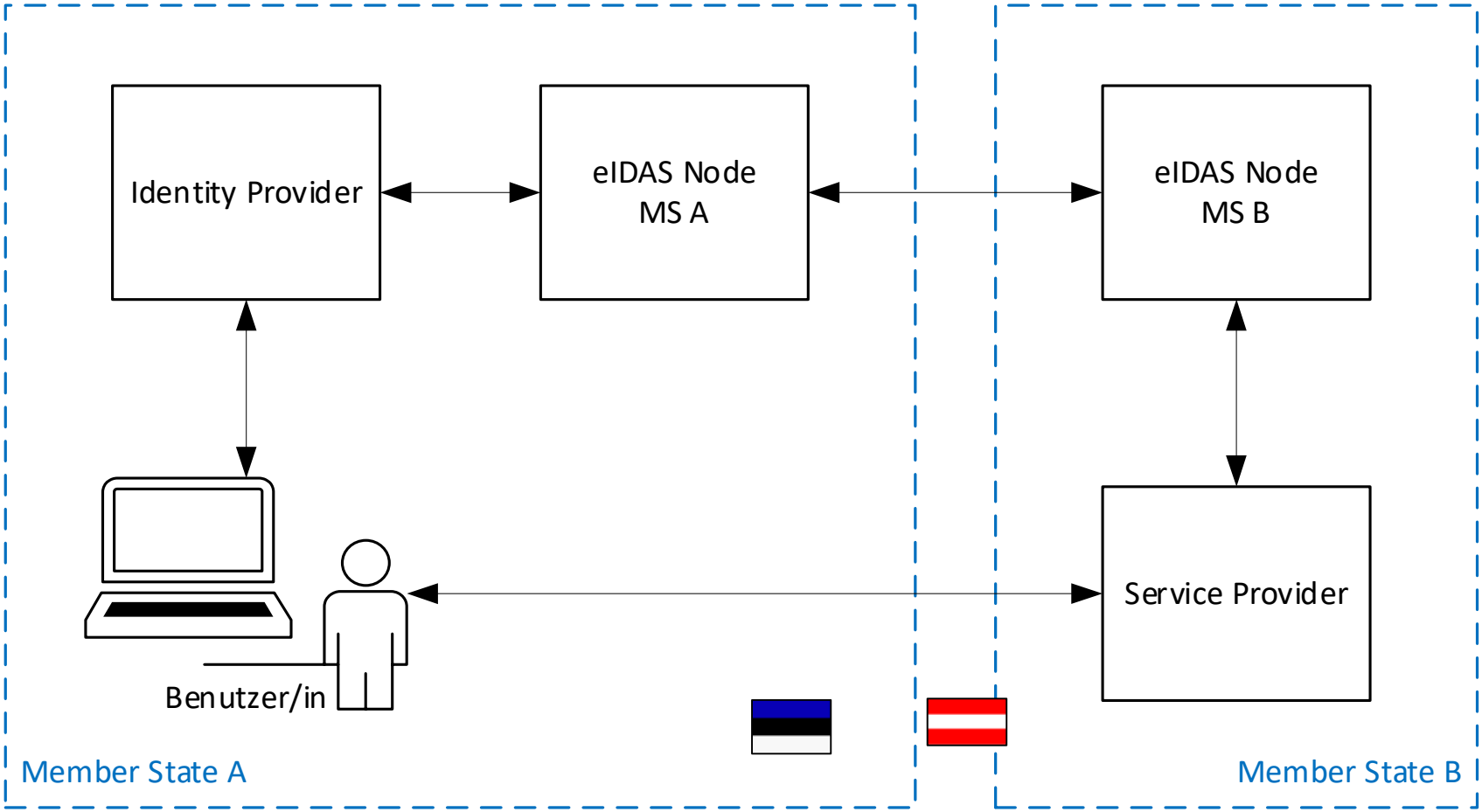
- Jeder MS betreibt einen Node „*eIDAS Service*“, InhaberInnen der eigenen eID's authentifiziert
- Auch als „Proxy Service“ bezeichnet
- Ausnahme Middleware: Nodt (eIDAS Service) vom empfangenden MS betrieben (dzt. nur DE)

Einkommende eID

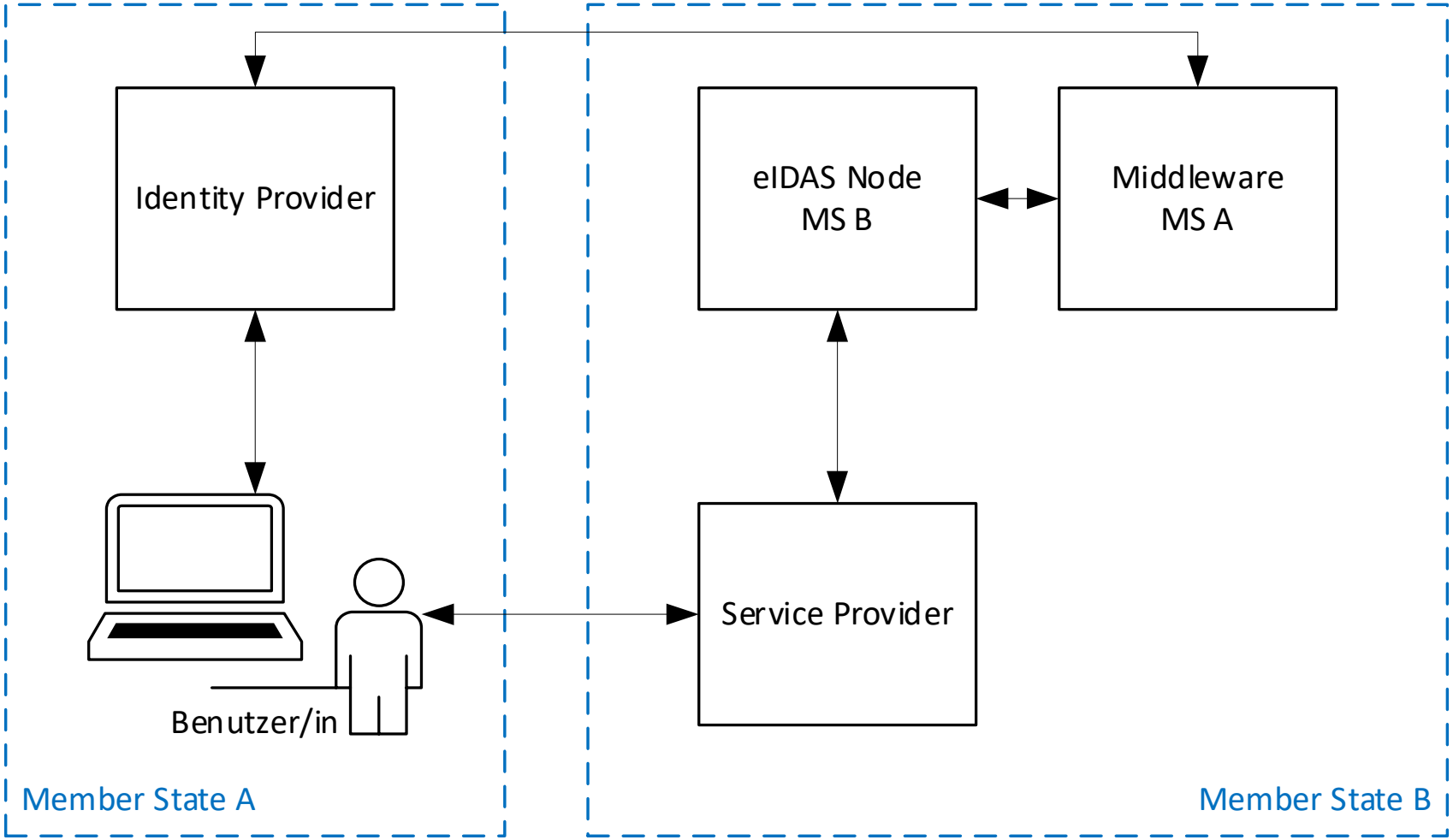
- Jeder MS betreibt einen *oder mehrere* „eIDAS Connector“ der für eigene Anwendungen (Relying parties) InhaberInnen ausl. eIDs akzeptieren
- eIDAS Node leitet ad „mehrere“: eIDAS Connectoren können sektorell sein
  - z.B. Banken, Gesundheit, ..

Technisch eine SAML 2.0 Identity Federation (mit zum „Dreieck“ SP-Person-IdP zusätzlichen Indirektionen)

eIDAS eID Federation: Proxy Service



eIDAS eID Federation: Middleware



Technische Eckdaten

- eIDAS SAML 2.0 Profil
  - Nahe an Kantara eGov / PVP 2.1
  - Web SSO
  - Post oder Redirect Binding (kein Artefact-B.)
  - Attribute von ISA Core Vocabulary abgeleitet
  - Request/Response signiert, verschl. Assertion
  - Vertrauensmodell über MS Metadata Signer
- In MOA-ID integriert, auch EK Referenzimpl.

Notifizierte/peer-reviewed/pre-notif. eIDs

Land	eID Schemen	LoA	Status *)	Anerk. bis **)
DE	nPA	High	notifiziert	09/2018
IT	SPID (9 IdPs)	(High) / Subst. / Low	notifiziert	09/2019
ES	DNIe	High	peer-reviewed	ca. 10/2019
EE	5 (ID) Cards, mobiil ID	High	peer-reviewed	ca. 10/2019
HR	ID Card	High	peer-reviewed	ca. 10/2019
LU	ID Card	High	peer-reviewed	ca. 10/2019
BE	ID Card, FAS		Im Peer-Review	ca. 12/2019
PT	ID Card, Mobile ID, SCAP		Im Peer-Review	ca. 12/2019
UK	UK GOV.Verify		Vor Peer-Review	ca. 03/2020

*) Stand 09/2018

**) Frist lt. eIDAS; lt. ö. E-GovG nach Maßgabe techn. Möglichkeit 6 Monate früher

UMSETZUNG IN ÖSTERREICH RECHTLICH

E-GovG Novelle: Wesentliche Änderungen

- Aus „Bürgerkarte“ wird „E-ID“
  - Behördliche Registrierung
    - Im Zuge Passantrag
  - Zentrale Infrastruktur im BM.I
    - Technisch/organisatorische Verfügbarkeit bestimmt Anwendungsbeginn; Pilot mit in Kraft Treten
  - Online-Personenbindung
    - Inhalt von Verwendung bestimmt (behördlich/privat)
    - Registrierung Anwendungen (auch aus eIDAS notw.)
  - Weitere Attribute aus Registern möglich

Weiterentwicklung zur eID

Novelle E-GovG – 2017:

- Notifizierung/Anerkennung gemäß eIDAS-VO
- Weiterentwicklung des österreichischen elektronischen Identifizierungssystems (eID) – Bürgerkarte „neu“

Folie mit Dank vom BMDW

Bürgerkarte „neu“ durch E-GovG-Novelle

- Schaffung der Voraussetzungen für die **Notifizierung des österreichischen elektronischen Identifizierungssystems** (bislang Bürgerkarte)
- und für die **innerstaatliche Verwendbarkeit notifizierter elektronischer Identifizierungsmittel anderer MS** im Sinne der eIDAS-VO
  - insb. Erstellung einer umfassend prüfbaren Personenbindung bei einer zentralen Stelle bei jeder Verwendung des E-ID
  - insb. Eintragung der Personenidentifikationsdaten des verwendeten elektr. Identifizierungsmittels des anderen MS in das ERnP (sofern keine Zuordnung zu bestehendem Eintrag ZMR/ ERnP möglich)

Folie mit Dank vom BMDW

Bürgerkarte „neu“ durch E-GovG-Novelle

- Änderung von Begrifflichkeiten
  - „**Elektronischer Identitätsnachweis (E-ID)**“ statt „Bürgerkarte“
- **Weiterentwicklung** des österreichischen elektronischen Identifizierungssystems (bislang Bürgerkarte)
  - Schaffung eines behördlichen Prozesses für die Registrierung eines E-ID
  - Erweiterung des Funktionsumfangs des E-ID, insbesondere durch die Einfügung weiterer Merkmale in die Personenbindung (variabel je nach Anwendungsfall)

Folie mit Dank vom BMDW

Online-Personenbindung *(§ 4 Abs. 5)*

- Wird bei jeder Verwendung des E-ID „neu“ gebildet und von der Stammzahlenregisterbehörde signiert/besiegelt
- Unterschiedlicher Inhalt je nach Art der Verwendung:
  - öffentlicher Bereich § 4 Abs. 5: ein/mehrere bPK, Mindestdatensatz (MDS=Vorname, Nachname, Geburtsdatum), optional: weitere Merkmale
  - privater Bereich § 14 Abs. 3: ein bPK
    optional: MDS, weitere Merkmale
  - Ausland § 14a Abs. 2: ein bPK, MDS
    optional: weitere Merkmale
- Prüfbarkeit im eIDAS Kontext damit sichergestellt, da auch Anwendungen im privaten Bereich und im Ausland eine behördlich signierte/besiegelte Personenbindung erhalten

Folie mit Dank vom BMDW

Neuer Registrierungsprozess *(§§ 4a, 4b)*

- Bisher: Registration-Officers (RO)
- In Zukunft: Registrierungsbehörde
- Registrierung eines E-ID (Identitätsfeststellung) im Rahmen der Beantragung eines Reisepasses bei der **Passbehörde**
  - Im Einvernehmen mit BMI können auch andere Behörden Registrierung vornehmen
  - Für Fremde ist Landespolizeidirektion sachlich zuständig
  - Von Amts wegen
  - Umfassende Identitätsprüfung (Registerabfragen, EKIS, etc.)
  - Wird der Behörde keine Telefonnummer bekannt gegeben, kann E-ID-Registrierung nicht abgeschlossen werden. Passantrag scheitert dadurch aber nicht.

Folie mit Dank vom BMDW

Weitere Merkmale

- Nachweis von Daten aus Registern von Auftraggebern des öffentlichen Bereichs (etwa Personenstands-, Melde- oder Staatsbürgerschaftsdaten)
- Werden nach Maßgabe der technischen Möglichkeit (etwa Anbindung des jeweiligen Registers) bei Verwendung des E-ID in die Personenbindung eingefügt und behördlich signiert/ besiegelt
  - Zugriff auf derartige Merkmale nur mit Zustimmung und Wissen des Betroffenen
  - Im privaten Bereich hätte der Betroffene die Möglichkeit, bloß Informationen über das Alter oder das Geburtsdatum, jedoch nicht seine Identität preiszugeben (vgl. § 14 Abs. 3)

Folie mit Dank vom BMDW

Innerstaatl. Verwendbarkeit eID *(§ 6 Abs. 5)*

- Elektronische Identifizierungsmittel eines anderen EU-MS die nach der eIDAS-VO notifiziert wurden, können wie ein E-ID im öffentlichen Bereich verwendet werden
  - Im privaten Bereich nur, wenn es vom Betreiber der Anwendung zugelassen wird
- Die Daten der Betroffenen werden ins ERnP oder zu einem bereits bestehenden Eintrag im ZMR/ERnP eingetragen
- Auf Grundlage dieses Eintrags wird im Rahmen der Verwendung der ausländischen eID eine Personenbindung wie für E-ID-Inhaber erstellt

Folie mit Dank vom BMDW

Inkrafttreten, Übergangsbestimmungen

- Inkrafttreten und Anwendungsbeginn fallen auseinander
  - Anwendungsbeginn erst wenn technisch/organisatorische Voraussetzungen für Echtbetrieb E-ID vorliegen
- Ab Inkrafttreten soll ein Pilotbetrieb durchgeführt werden
  - Dient der Gewährleistung eines sicheren Betriebs für die vollumfängliche Nutzung des E-ID
- Übergangsregelung für bestehende Bürgerkarten
  - Bis zum Anwendungsbeginn („Echtbetrieb E-ID“) bleibt bestehendes Bürgerkartensystem anwendbar
  - Ab Anwendungsbeginn werden bestehende Bürgerkarten bis zum Ablauf des Zertifikats zu einem E-ID umgewandelt (vereinfachter Prozess für Umstieg)

Folie mit Dank vom BMDW

Elektronischer Identitätsnachweis (E-ID)

- Fokus der Weiterentwicklung des Bürgerkartenkonzeptes…
  - Grenzüberschreitender Einsatz der österreichischen Lösung
  - Attraktivierung für Verwendung im privatwirtschaftlichen Bereich
  - Weiterentwicklung in puncto Sicherheit
  - Verbesserung der Transparenz

Folie mit Dank vom BMDW

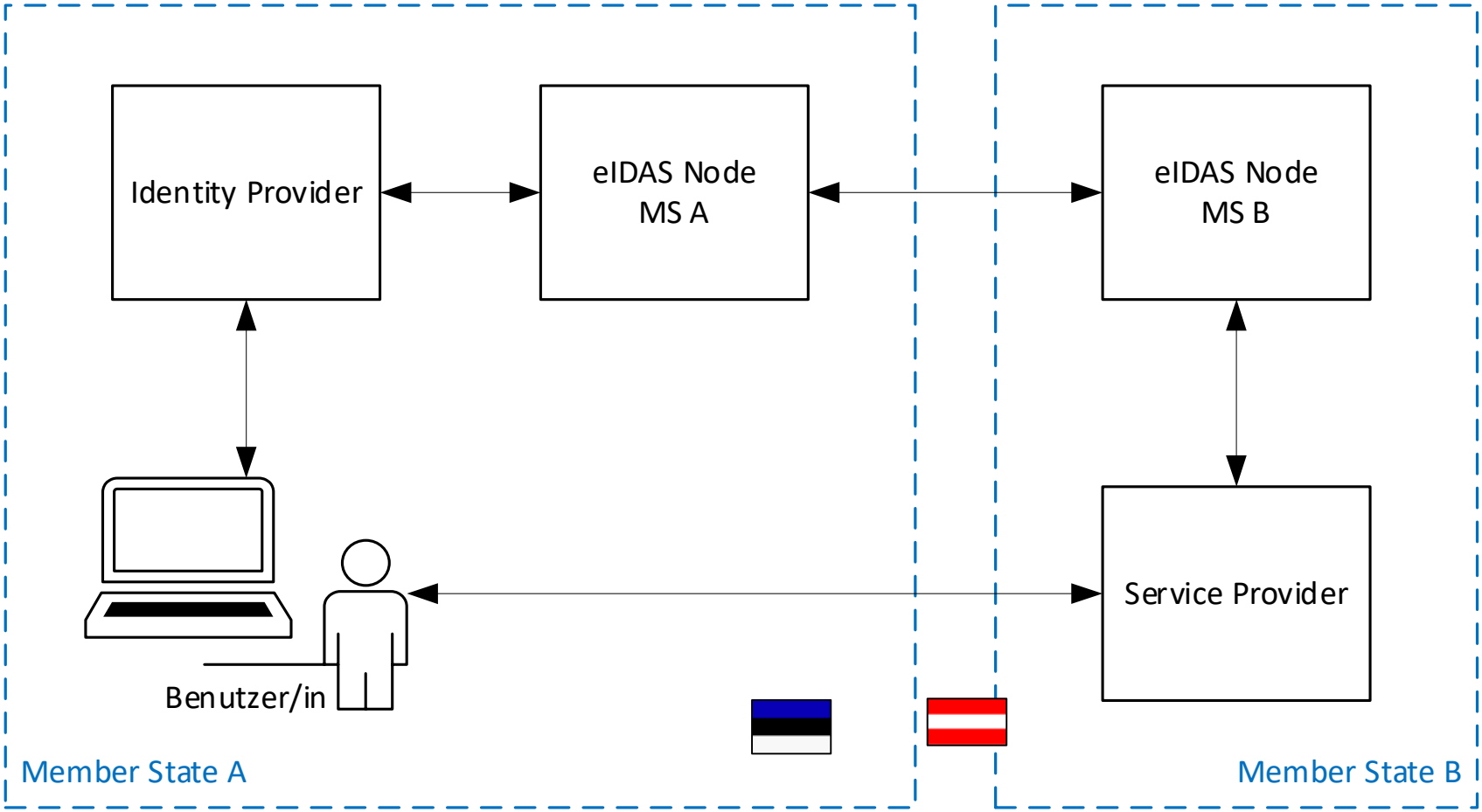
Elektronischer Identitätsnachweis (E-ID)

- Anforderungen an die Technik
  - Zentrale Erstellung der bPK (dzt.: dezentral)
  - Erweiterte Prüfmöglichkeiten der Personenbindung (Signatur durch SZB)
  - Sichere Bereitstellung von Merkmalen aus Verwaltungsregistern
  - Weiterentwicklung in puncto Sicherheit
  - Erweiterte Kontrollmöglichkeiten im Zuge der Datenfreigabe sowie Einsichtnahme in Protokolldaten
  - „Data Protection by Design“

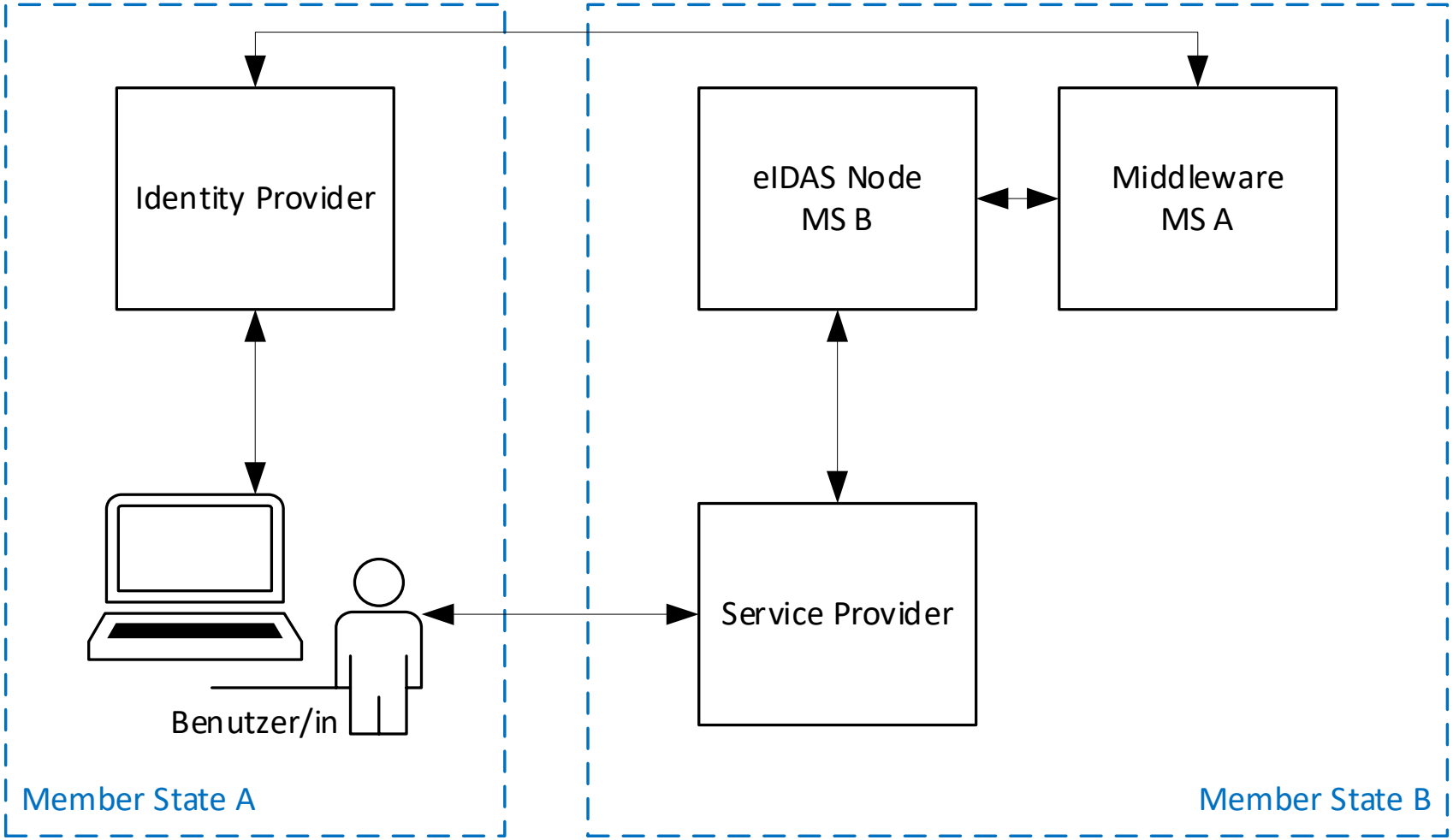
Folie mit Dank vom BMDW

UMSETZUNG IN ÖSTERREICH TECHNISCH (EINGEHENDE EID)

Wiederholung: eIDAS Proxy Service



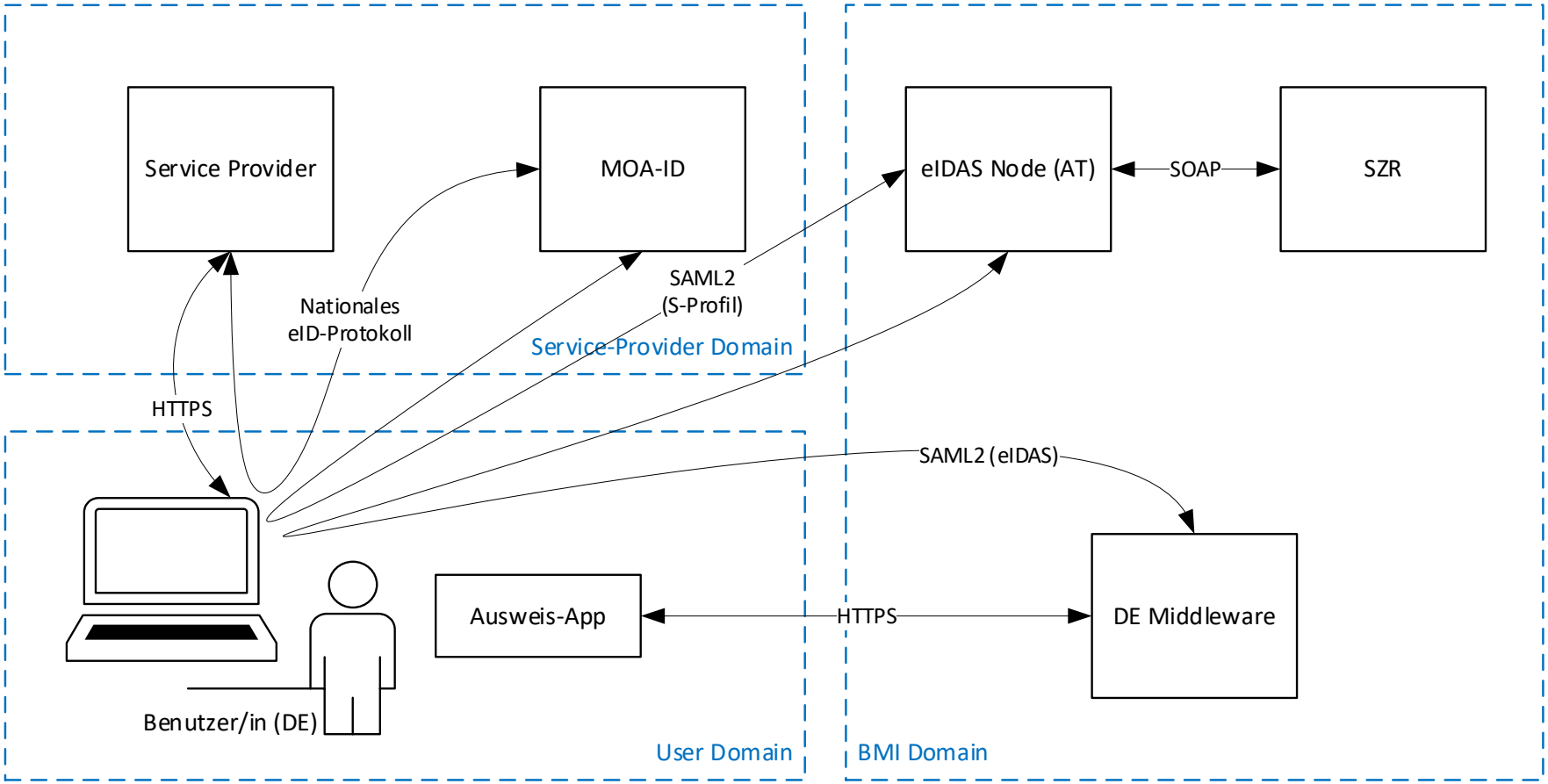
Wiederholung: eIDAS Middleware



Anbindung notifizierter eIDs an österr. SPs

- Österreichische eIDAS-Node wird durch das BM.I betrieben werden
- Anmeldeprozess wird für den Service Provider wie bisher über MOA-ID gekapselt sein
- MOA-ID leitet zur Authentifizierung an die österreichische eIDAS-Node statt an die BKU/Handy-Signatur weiter, falls BenutzerIn eIDAS-Login triggert
- Für Service Provider ist der Authentifizierungsprozess über eine notifizierte ausländische eID damit weitgehend transparent

Architektur (Anbindung deutsche eID)



Sicht der Anwenderin

- Wechsel zu eIDAS in BKU-Auswahl

bisher

neu

AKTIONSPUNKTE FÜR SERVICE PROVIDER

Aktionspunkte für Service Provider

- Aktualisierung von MOA-ID zumindest auf Version 3.4.0
- Anbindung der MOA-ID-Instanz an die eIDAS-Node des BM.I
- Überprüfung der Kompatibilität eigener Services mit eIDAS-basierten eIDs
- Freischalten eIDAS-basierter Authentifizierungsprozesse („Erweiterung der BKU-Auswahl“) in MOA-ID

Einschränkungen

- Derzeit noch keine Unterstützung für privatwirtschaftliche Anwendungen
- Keine Unterstützung für qualifizierte Signaturen
- Derzeit noch keine Unterstützung elektr. Vollmachten
- Limitierungen in von MOA-ID bereitgestellten Identity-Assertions
  - Assertion enthält keinen signierten Auth.-Block
  - Assertion enthält kein qualifiziertes Signaturzertifikat der BenutzerIn

Wir danken für die Zeit und Aufmerksamkeit

Wien, 1.10.2018

Herbert.Leitold@a-sit.at

Thomas.Zefferer@a-sit.at