Elektronische Signatur

Wahlfachkorb Computer und Recht

SoSe 2024

Mag. Peter Kustor
Bundeskanzleramt
Abt. VII/2 - Legistik und Stammzahlenregisterbehörde, E-Government-Strategie sowie EU und Internationales

peter.kustor@bka.gv.at

Agenda

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens:
   EU (eIDAS-VO) und national (SVG/SVV)
5. Verfahrensrechtliche Anforderungen, Amtssignatur
6. Weitere „Vertrauensdienste“ – insbes. nach der „neuen“ eIDAS-VO
7. Elektronische Signatur und Identitätsmanagement
8. Von der „Bürgerkarte“ und der „Handy-Signatur“ zur „Identity Austria“
9. EU-eID – „Wallet“ und aktuelle Entwicklungen

Form von Rechtsgeschäften

- Grundsatz der Formfreiheit - schriftlich, mündlich (auch telefonisch) oder sogar durch schlüssiges Verhalten
- Ausnahmen durch Gesetz oder Vereinbarung
  - Schriftform
  - Notariatsakt
  - Beglaubigung (Notar/ Gericht)
  - Realverträge
  - Vereinbarte Formvorschiften (Grenzen bei Verbraucherverträgen)

„Schriftlichkeit“ - § 886 ABGB

„Ein Vertrag, für den Gesetz oder Parteiwille **Schriftlichkeit** bestimmt, kommt durch die **Unterschrift** der Parteien oder, falls sie des Schreibens unkundig oder wegen Gebrechens unfähig sind, durch Beisetzung ihres gerichtlich oder notariell beglaubigten Handzeichens oder Beisetzung des Handzeichens vor zwei Zeugen, deren einer den Namen der Partei unterfertigt, zustande. Der schriftliche Abschluß des Vertrages wird durch gerichtliche oder notarielle Beurkundung ersetzt. **Eine Nachbildung der eigenhändigen Unterschrift auf mechanischem Wege ist nur da genügend, wo sie im Geschäftsverkehr üblich ist**.“

„Unterschrift“ - Wikipedia

„**Unterschrift** (auch **Signatur**, von lateinisch *signare* „bezeichnen“ zu *signum* „Zeichen“) ist die handschriftliche, eigenhändige Namenszeichnung auf Schriftstücken durch eine natürliche Person mit mindestens dem Familiennamen. Die Unterschriftsleistung ist zur Gültigkeit von Rechtsgeschäften, die mindestens der Schriftform bedürfen, erforderlich.“

„Unterschrift“ - OGH

„Das Gebot der Schriftlichkeit bedeutet im allgemeinen "**Unterschriftlichkeit**", es sei denn, das Gesetz sieht ausdrücklich eine Ausnahme vor. Das Erfordernis der Schriftform soll gewährleisten, dass aus dem Schriftstück der Inhalt der Erklärung, die abgegeben werden soll, und die Person, von der sie ausgeht, hinreichend zuverlässig entnommen werden können.“

(zB 1Ob525/93 vom 2.7.1993)

„Unterschrift“ - VwGH

„Eine "Unterschrift" ist dabei ein Gebilde aus Buchstaben einer üblichen Schrift, aus der ein Dritter, der den Namen des Unterzeichneten kennt, diesen Namen aus dem Schriftbild noch herauslesen kann; eine Unterschrift muss nicht lesbar, aber ein "**individueller Schriftzug**" sein, der entsprechend charakteristische Merkmale aufweist. Die Anzahl der Schriftzeichen muss der Anzahl der Buchstaben des Namens nicht entsprechen. Eine Paraphe ist keine Unterschrift“

(Erkenntnis vom 4.9.2000 Zl. 98/10/0013 mit Hinweis auf Walter/Mayer, Grundriss des österreichischen Verwaltungsverfahrensrechts, 7. Auflage, Rz 190 ff, mit Judikaturhinweisen)

Wirkung der Unterschrift: § 294 ZPO

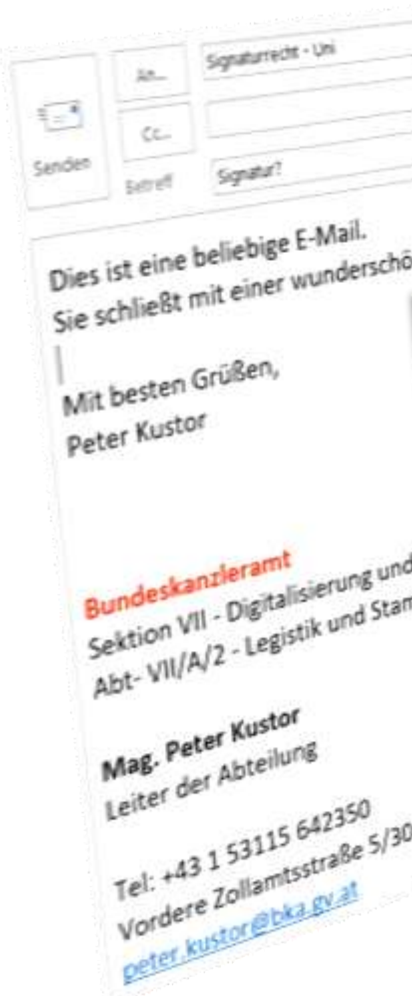
„Auf Papier oder elektronisch errichtete Privaturkunden begründen, sofern sie von den Ausstellern **unterschrieben** oder mit ihrem gerichtlich oder notariell beglaubigten Handzeichen versehen sind, **vollen Beweis** dafür, **dass die** in denselben **enthaltenen Erklärungen von den Ausstellern herrühren**.“

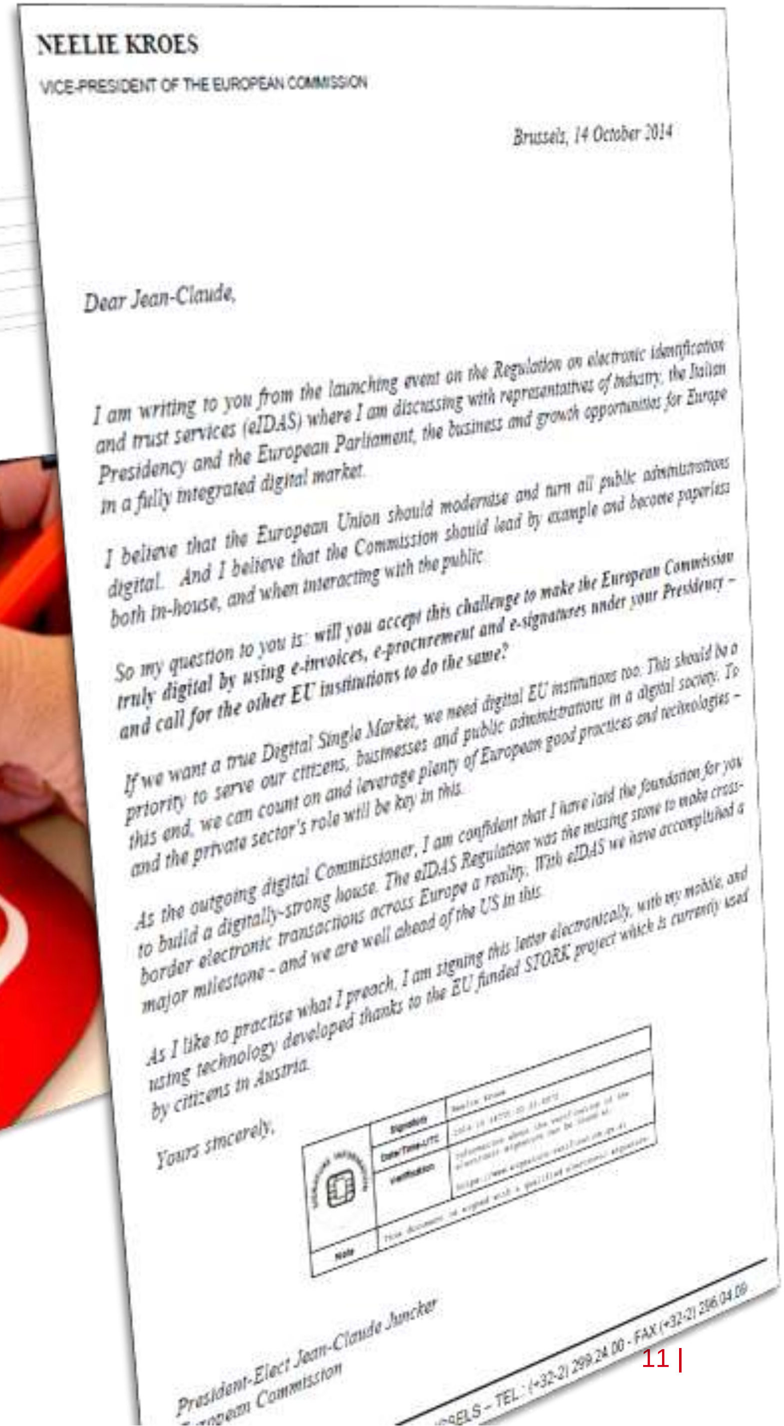
- *„Qualifizierte Echtheitsvermutung“*
- *Bezieht sich auf die äußere Beweiskraft der Urkunde*

Funktionen einer Unterschrift

- **Identitätsfunktion**: Der Aussteller der Urkunde wird erkennbar
- **Echtheitsfunktion**: Gewähr, dass die Willenserklärung vom Aussteller stammt
- **Beweisfunktion**: Beweisführung wird durch die Urkunde erheblich vereinfacht
- **Abschlussfunktion**: Bringt zum Ausdruck, dass die Willenserklärung abgeschlossen/vollendet ist
- **Warnfunktion**: Schützt den Unterzeichner vor Übereilung

Elektronische Signatur?





NEELIE KROES

VICE-PRESIDENT OF THE EUROPEAN COMMISSION

Brussels, 14 October 2014

Dear Jean-Claude,

I am writing to you from the launching event on the Regulation on electronic identification and trust services (eIDAS) where I am discussing with representatives of industry, the Italian Presidency and the European Parliament, the business and growth opportunities for Europe in a fully integrated digital market.

I believe that the European Union should modernise and turn all public administrations digital. And I believe that the Commission should lead by example and become paperless both in-house, and when interacting with the public.

So my question to you is: **will you accept this challenge to make the European Commission truly digital by using e-invoices, e-procurement and e-signatures under your Presidency – and call for the other EU institutions to do the same?**

If we want a true Digital Single Market, we need digital EU institutions too. This should be a priority to serve our citizens, businesses and public administrations in a digital society. To this end, we can count on and leverage plenty of European good practices and technologies – and the private sector's role will be key in this.

As the outgoing digital Commissioner, I am confident that I have laid the foundation for you to build a digitally-strong house. The eIDAS Regulation was the missing stone to make cross-border electronic transactions across Europe a reality. With eIDAS we have accomplished a major milestone - and we are well ahead of the US in this.

As I like to practise what I preach, I am signing this letter electronically, with my mobile, and using technology developed thanks to the EU funded STORK project which is currently used by citizens in Austria.

Yours sincerely,

Signatory	
Date/Time-UTC	
Verification	
Note	

President-Elect Jean-Claude Juncker
European Commission

E-Kommunikation

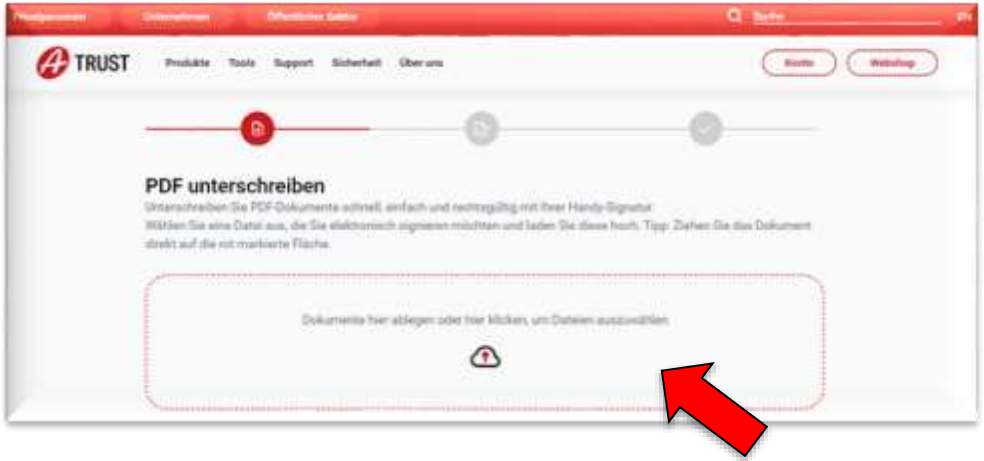
- Vergleichbar mit einer Postkarte, kann am Postweg **gelesen** und **verändert** werden
  - Postkarte: Postmitarbeiter, …
  - E-Mail: Systemadministratoren, Hacker, …
- Ungewissheit des Gegenübers

Authentizität von Urheber & Daten

- Zuordnung der Daten zum Unterzeichner
- Schutz vor Abstreiten durch Unterzeichner
- Sicherung der signierten Daten vor Manipulation
  - am Übertragungsweg
  - durch den Empfänger

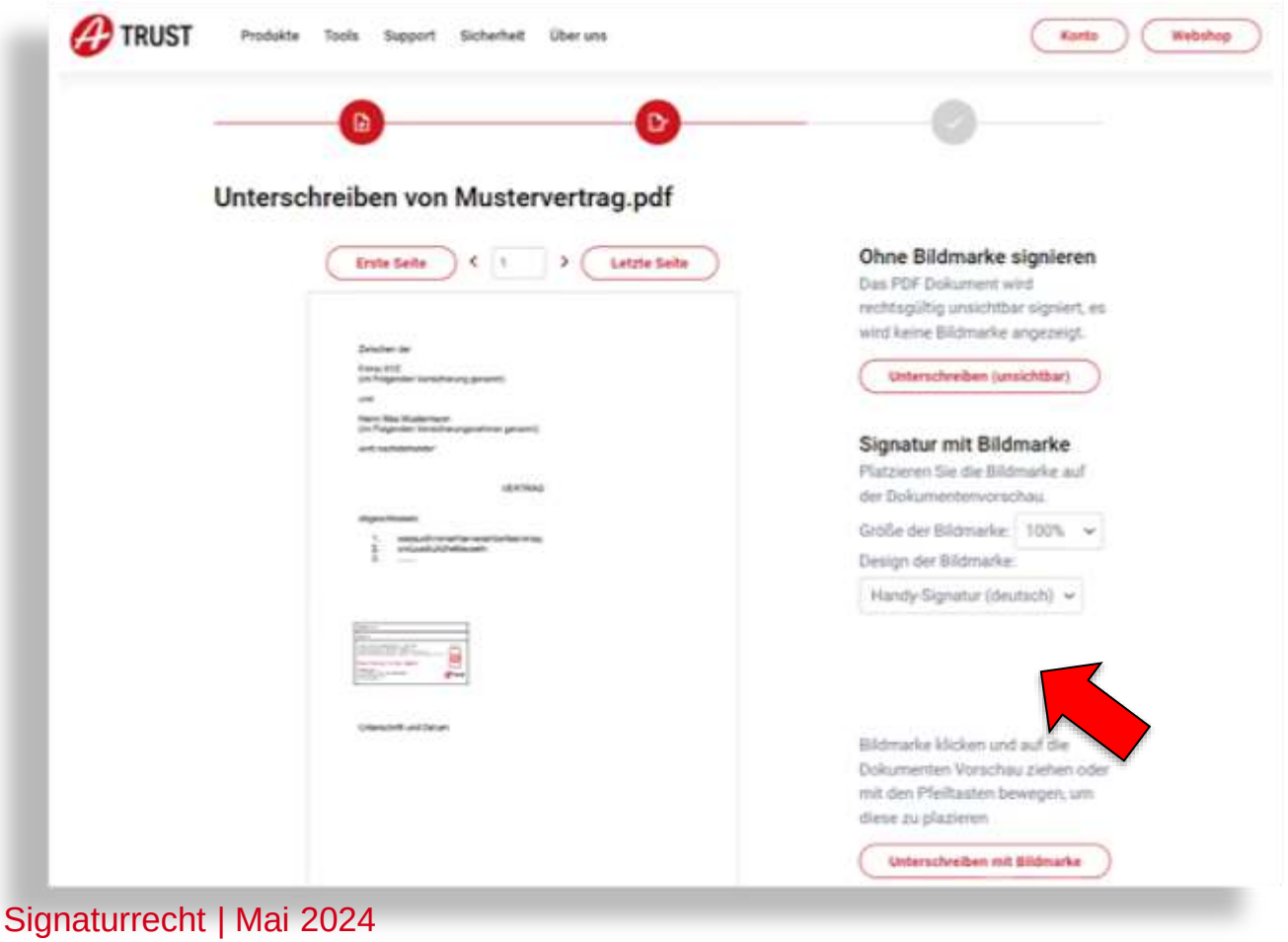
Dokumente elektronisch unterschreiben (Kaufverträge, etc.)

- „herkömmlich“ mehrere aufwändige Schritte nach Erhalt des zu unterschreibenden Dokuments per E-Mail
  - ausdrucken
  - händisch unterschreiben
  - kuvertieren und Versand mittels Brief (inkl. Gang zur Post)
    - Oder: einscannen und rücksenden per E-Mail (Frage: liegt hier eine „Unterschrift“ vor?)
- das geht auch schneller, komfortabler und sicherer (zB ID Austria…)
  - auf https://www.oesterreich.gv.at/landingpages/pdf_signatur_services.html finden Sie verschiedene Anbieter. Hier am Beispiel von https://www.a-trust.de/pdfsign/:
  - wird das zu unterschreibende Dokument hochgeladen und gleich elektronisch unterschrieben



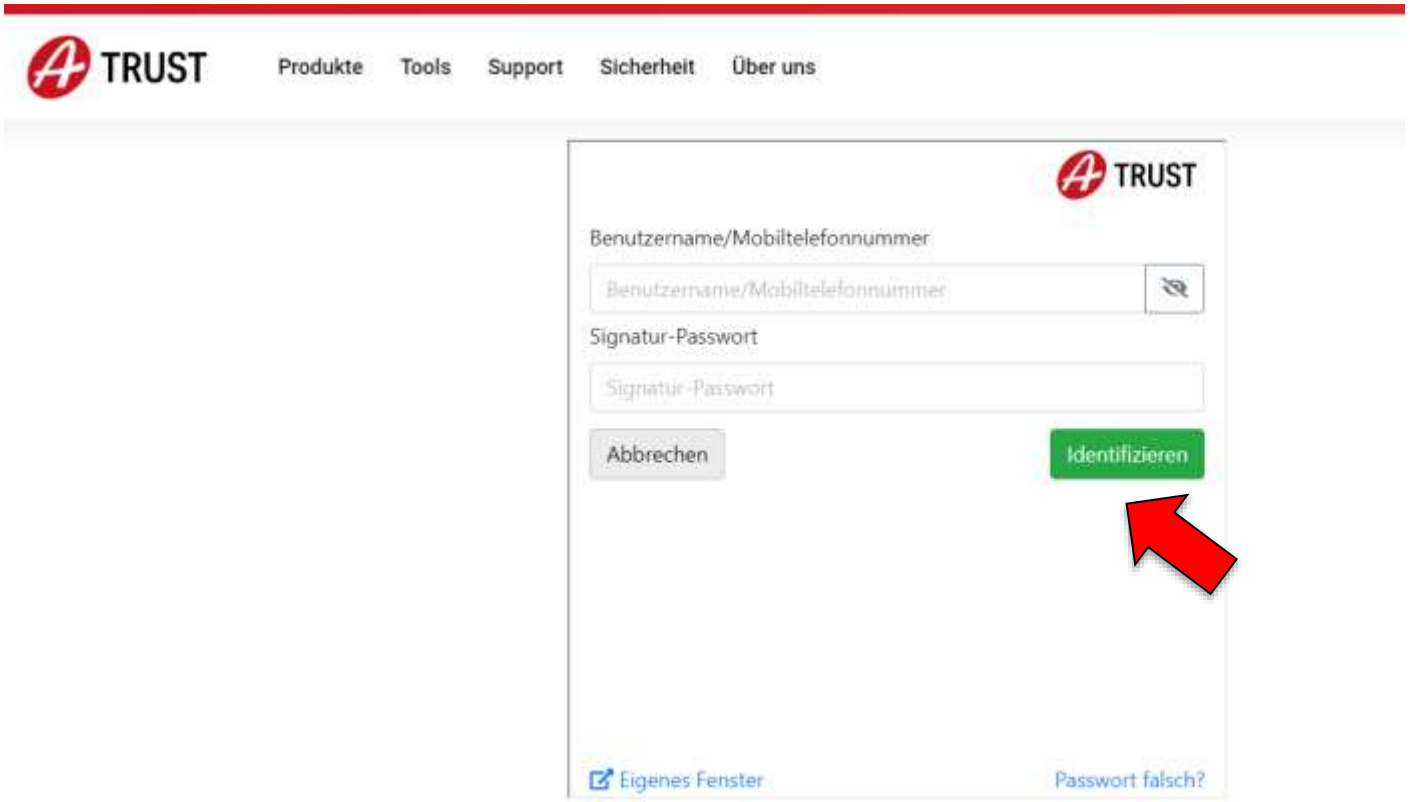
Dokumente elektronisch unterschreiben

Nach Hochladen des Dokuments positionieren Sie den „Signaturbock“ („Bildmarke“)



Dokumente elektronisch unterschreiben

Zum Unterschreiben geben Sie Ihre User-ID/ Mobiltelefonnummer und das von Ihnen definierte Passwort ein und klicken auf „identifizieren“.

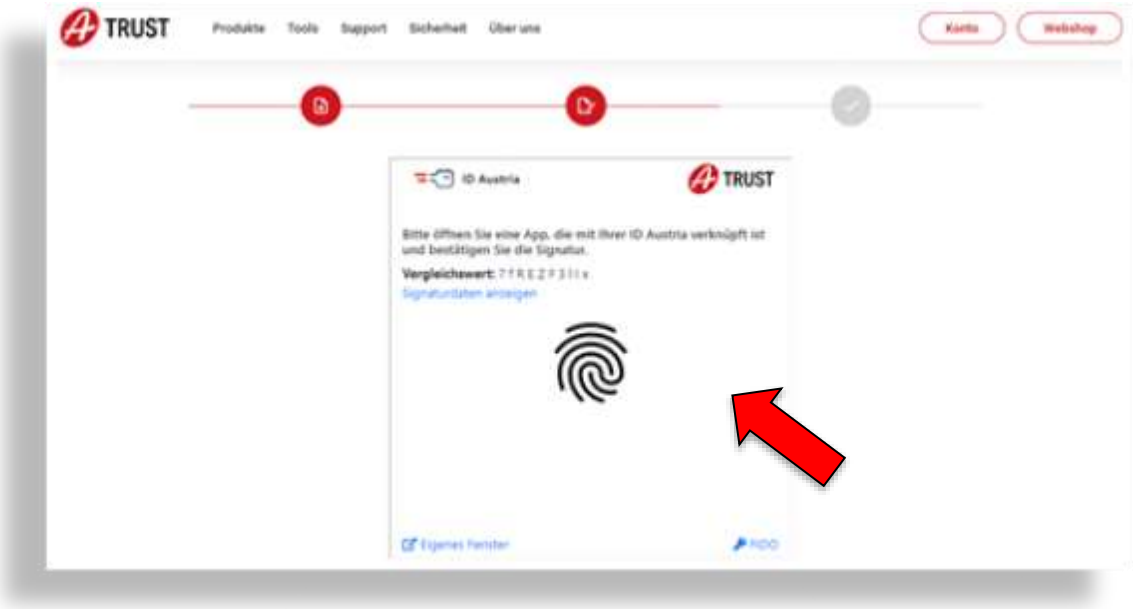


Dokumente elektronisch unterschreiben

Hier Signaturauslösung mit Biometrie in der App (Digitales Amt-App):

Damit bestätigen Sie, dass Sie nicht nur UID und das Passwort wissen, sondern auch das Mobiltelefon gerade in Ihrem Besitz haben und auch die Bindung an Ihrer Person mit dem Sicherheitselement des Handies besteht.

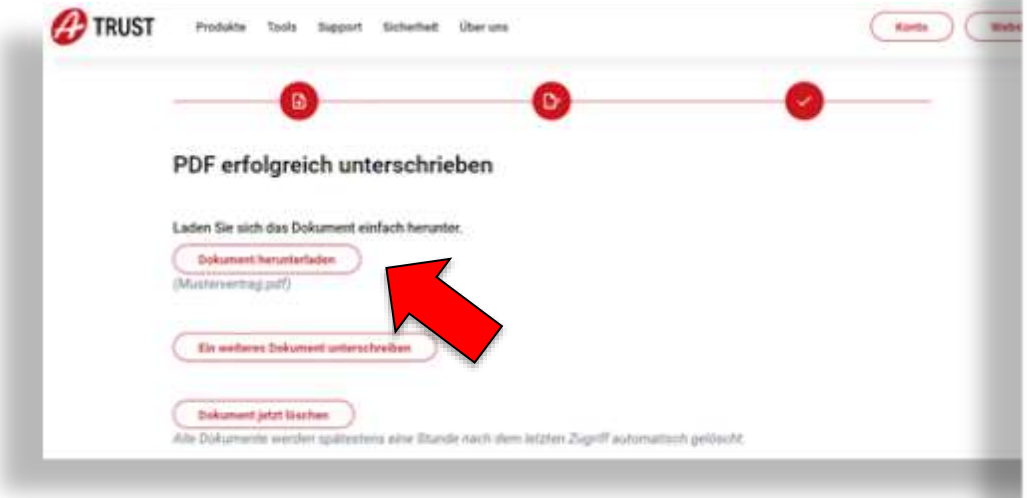
Davor können Sie in der App auch nochmals das zu signierende Dok. ansehen und den Vergleichswert checken.



Dokumente elektronisch unterschreiben

Fertig.

Download/ speichern/ versenden…




Zwischen der

Firma XYZ
(im Folgenden Versicherung genannt)

und

Herrn Max Mustermann
(im Folgenden Versicherungsnehmer genannt)

wird nachstehender

VERTRAG

abgeschlossen:

1. wasauchimmerhiervereinbartseinmag
2. undzusätzlicheklauseln
3. .....

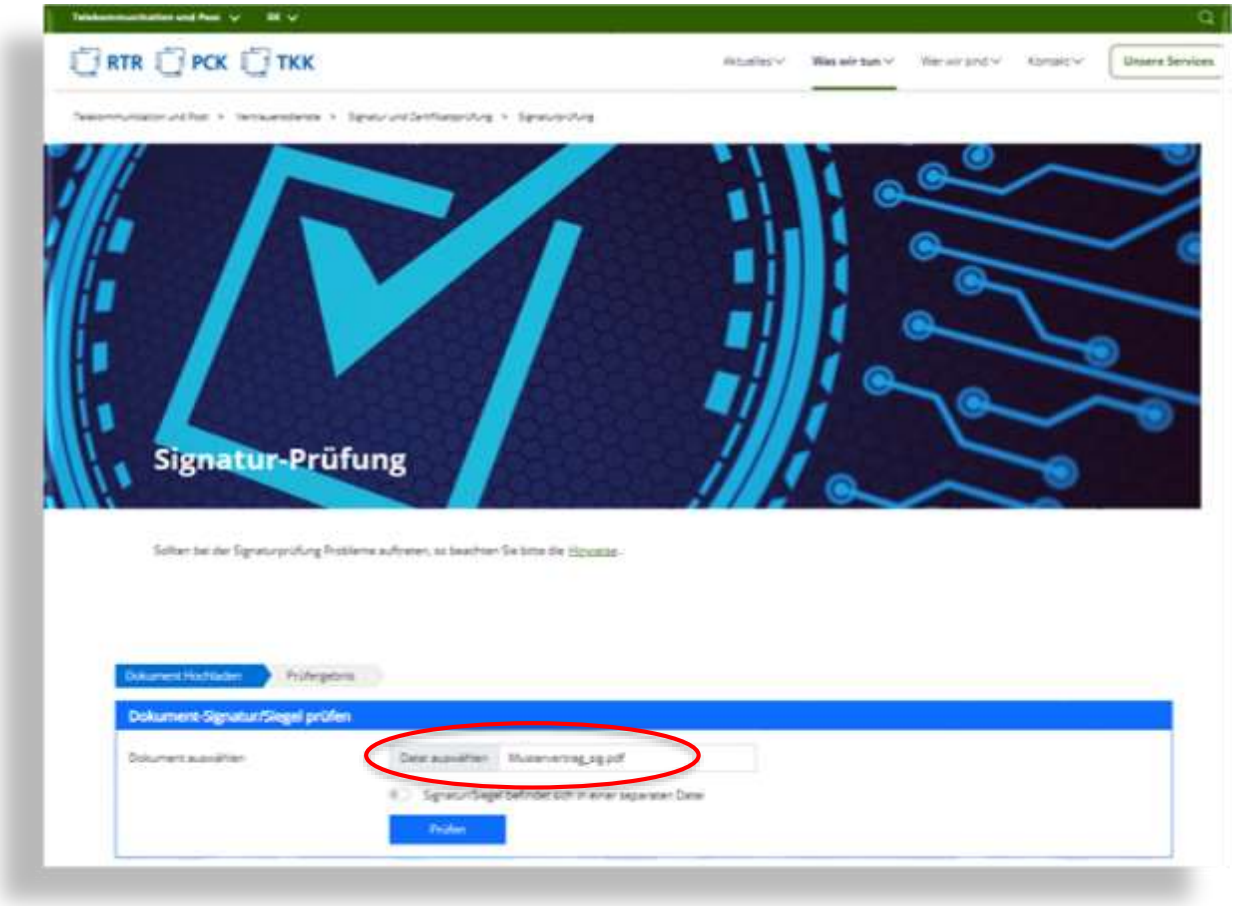
Unterschrift und Datum

Dokumente elektronisch unterschreiben

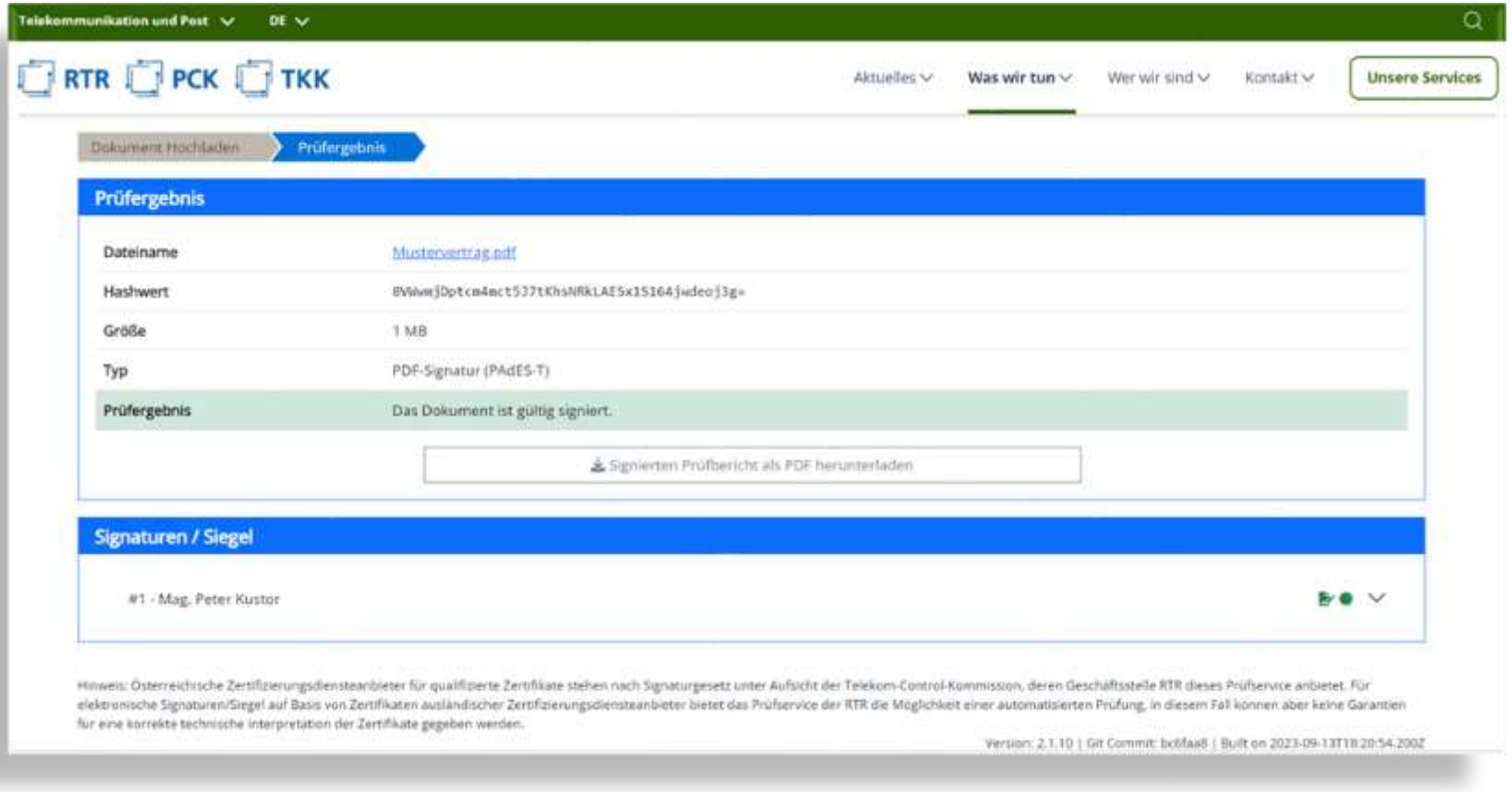
Was in der Papierwelt die sichtbare Unterschrift ist, ist in der elektronischen Welt der „Signaturblock“, welcher Informationen enthält, um die Unterzeichnerin bzw. den Unterzeichner zu identifizieren.

Signaturprüfung ganz einfach über www.signaturpruefung.gv.at

Upload des Dokuments und Anzeige des Prüfergebnisses



Anzeige des Prüfergebnisses (1/2)



Anzeige des Prüfergebnisses (2/2)

Signaturen / Siegel

#1 - Mag. Peter Kustor

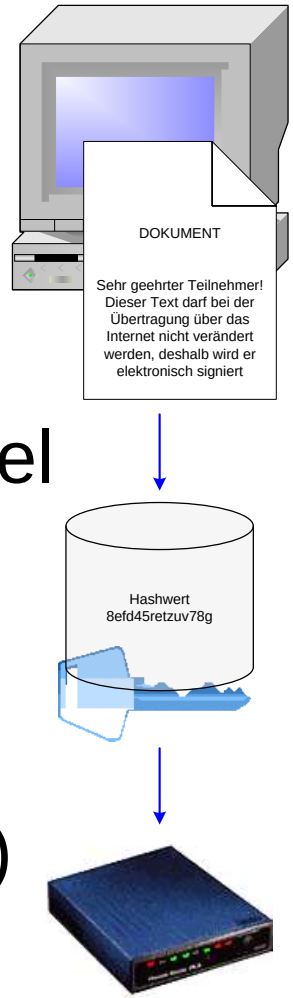
Signatur/Siegel- bzw. Prüfzeitpunkt (UTC)	2024-05-09T09:58:26Z
Signatur/Siegel	Die Überprüfung des Werts der Signatur bzw. des Siegels konnte erfolgreich durchgeführt werden.
Zertifikat	Eine formal korrekte Zertifikatskette vom Signatur/Siegel-Zertifikat zu einem vertrauenswürdigen Wurzelzertifikat konnte konstruiert werden. Jedes Zertifikat dieser Kette ist zum in der Anfrage angegebenen Prüfzeitpunkt gültig.
Zusatzinformationen	
Signaturtyp/Siegeltyp	PAdES-T
Die Signatur deckt den/die folgende/n Bereich/e an Bytes ab	0,1487500,1506446,56516
Signaturalgorithmus	SHA256withECDSA
	Signierte Daten herunterladen
Unterzeichner/Siegelersteller	
Name	Peter Kustor
Titel	Mag.
Staat	AT
Seriennummer	dez.: 726887618829, hex.: a9:3d:e0:d9:0d
Aussteller	
Name	a-sign-premium-mobile-05
Organisationseinheit	a-sign-premium-mobile-05
Organisation	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Staat	AT
Informationen zum Zertifikat	
Seriennummer	dez.: 1994748980, hex.: 76:e5:74:34
Qualität	Qualifiziertes Zertifikat (Quelle: TSL), sichere Signaturerstellungseinheit (Quelle: Zertifikat)
Zeitliche Gültigkeit	Gültig von 2022-07-15T13:35:04Z bis 2026-09-10T12:16:56Z. Der Prüfzeitpunkt liegt innerhalb des Gültigkeitszeitraumes.
Key Usage	Digital Signature, Non Repudiation
Zertifizierungsstatement	http://www.a-trust.at/docs/cp/a-sign-premium-mobile
	Zertifikat Herunterladen
Informationen zum Vertrauensdienst	
Herausgeberland	AT
ServiceTypeStatus	http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted
ServiceTypeIdentifier	http://uri.etsi.org/TrstSvc/Svctype/CA/QC
Zusätzliche Service Informationen	• http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures • http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures

Signaturvorgang im Überblick (Sender)

- Erstellen eines Dokuments
- Hashwert („Fingerabdruck“ des Dok.) wird gebildet
- Hashwert wird mit dem privaten Schlüssel verschlüsselt

  Signatur

✓ z.B.: Versand der signierten Nachricht (mit dem eigenen öffentlichen Schlüssel)



„Hash“

- Wird aus dem Gesamttext errechnet.
- Vergleichsbeispiel einer – primitiven – Hash-Funktion: Jeder Buchstabe wird durch seine Position im Alphabet ersetzt, am Schluss werden diese Zahlen zusammengezählt:

Buchstabe	S	C	H	M	E	T	T	E	R	L	I	N	G	Summe
Position im Alphabet	19	3	8	13	5	20	20	5	18	12	9	14	7	**153**

- Natürlich kommen wesentlich komplexere Verfahren zum Einsatz. ZB SHA-256, womit Hash-Werte mit einer Länge von 256 Bit erzeugt werden - üblicherweise als 64-stellige Hexadezimal-Zahl ausgedrückt werden. Der Hash-Wert für das Wort „Schmetterling“ zB lautet dann:
- d7e3dabc2c95c4c440ee57fb2883188e7f46a9cf51e94674f0e80f7d6db092c4

Anforderungen an die Hash-Funktion

- Kann auf eine Datei beliebiger Länge angewandt werden
- Erzeugt immer Ausgabe einer fixen Länge
- Für den Hashwert darf kein anderer Ausgangstext gefunden werden, als der gehashte.
- Es dürfen nicht mehrere verschiedene Ausgangstexte gefunden werden, die denselben Hashwert erzeugen.
- Auch geringe Änderungen im Ausgangstext müssen signifikante Änderungen im Hashwert erzeugen.
- Hashwert kann für beliebige Ausgangsdatei einfach und schnell errechnet werden

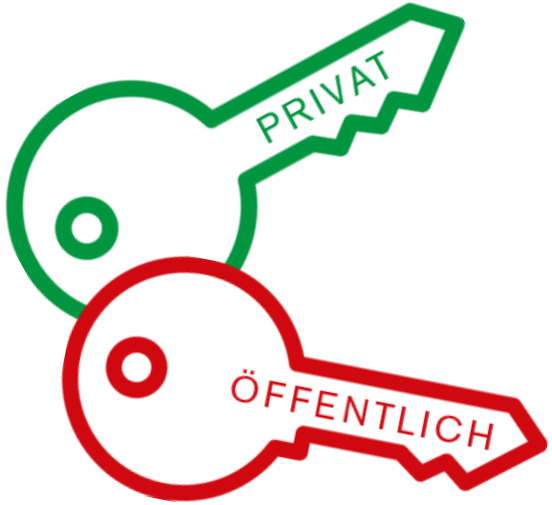
Verschlüsselung

- Symmetrische versus asymmetrische Verschlüsselung
- Komplexität:
  - Schlüsselverwaltung und Schlüsselaustausch bei symmetrischer Verschlüsselung…

Asymmetrische Verschlüsselung – „PKI“

Zwei Schlüssel Prinzip

- Privater Schlüssel (Private Key)
  - „Signaturerstellungsdaten“
  - Zugangsberechtigung (PIN)
  - nur dem Signator bekannt
- Öffentlicher Schlüssel (Public Key)
  - „Signaturprüfdaten“/ „Signaturvalidierungsdaten“
  - öffentlich zugänglich und abrufbar

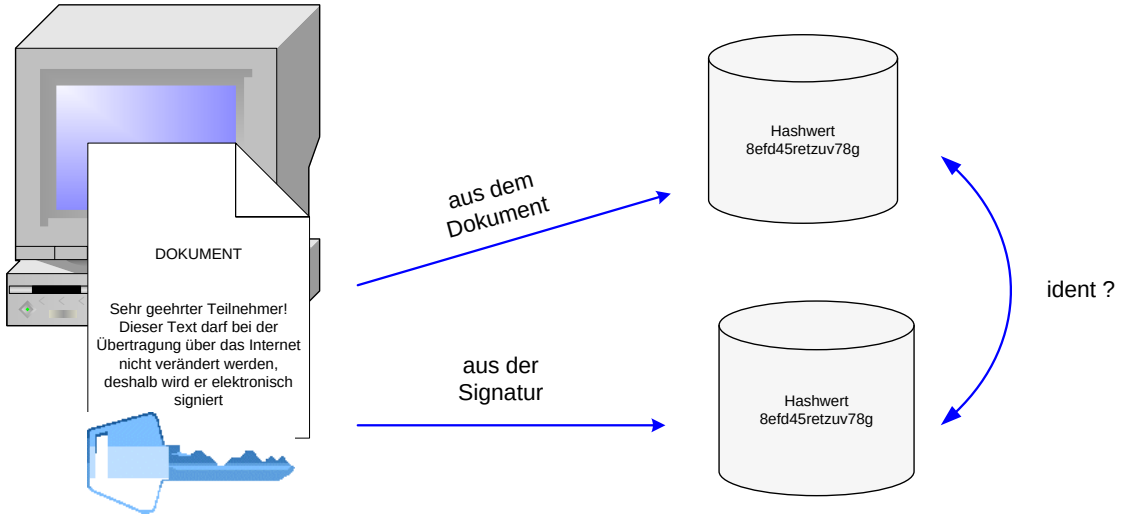


Verschlüsselung vs Signatur

- Es geht bei der Signatur nicht um Verschlüsselung des Inhalts!
- Es wird der Inhalt im Klartext belassen
- Es wird lediglich der Hashwert verschlüsselt!

Überprüfung der Signatur im Überblick (Empfänger)

- Aus dem empfangenen Dokument wird der Hashwert erneut gebildet
- Mit dem öffentlichen Schlüssel des Senders wird die Signatur entschlüsselt, der ursprüngliche Hashwert wird bekannt
- Vergleich beider Hashwerte
- ✓ Hashwerte ident ⇨ Nachricht vom Sender und unverfälscht



Worum geht es also?

- Es werden Daten (der Inhalt, der signiert wird) so gesichert, dass eine nachträgliche Änderung sofort erkannt wird.

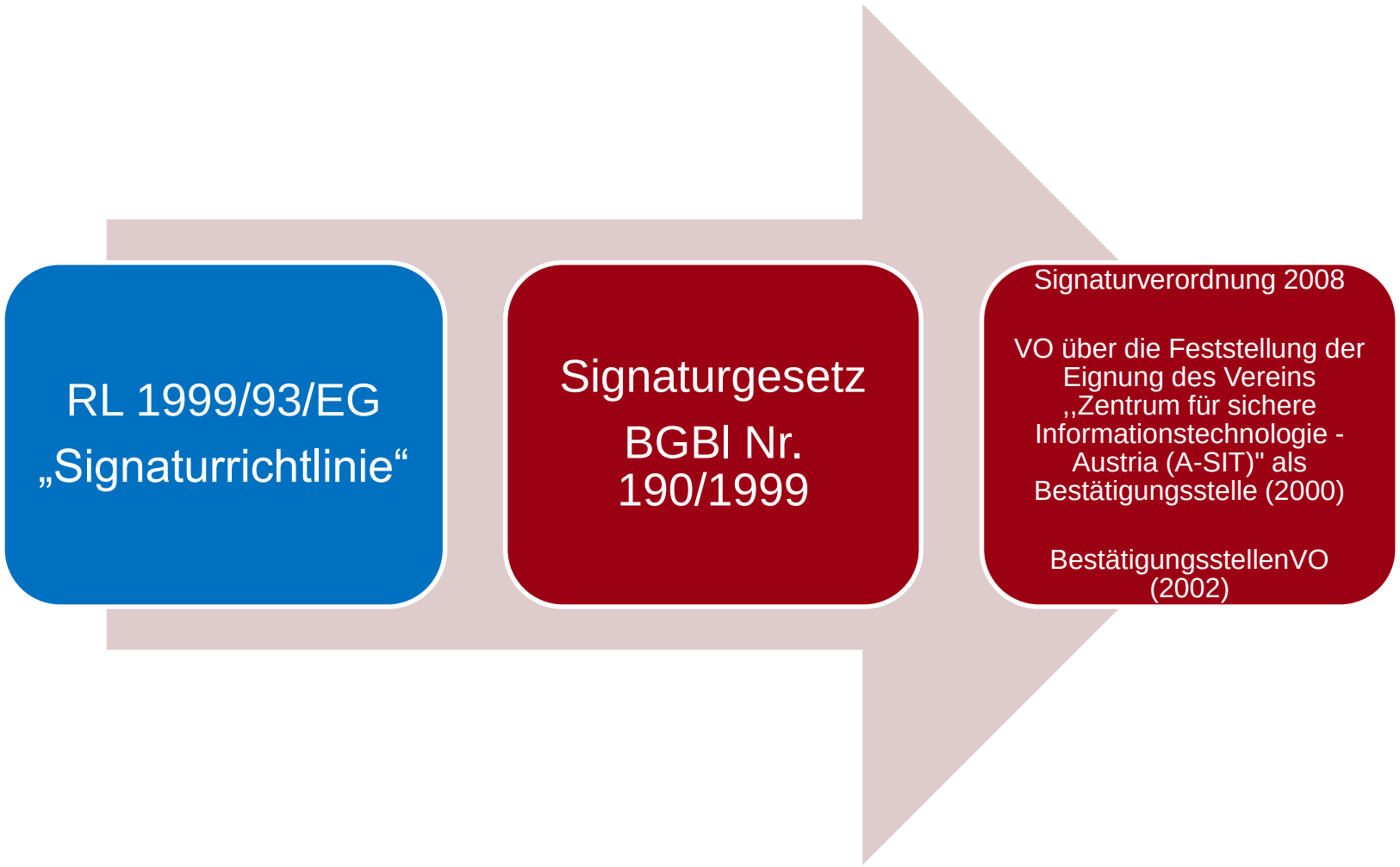
- „Integrität“

- Es werden Daten einer bestimmten Person zugeordnet (dem „Signator“, denn nur er hat den privaten Schlüssel)

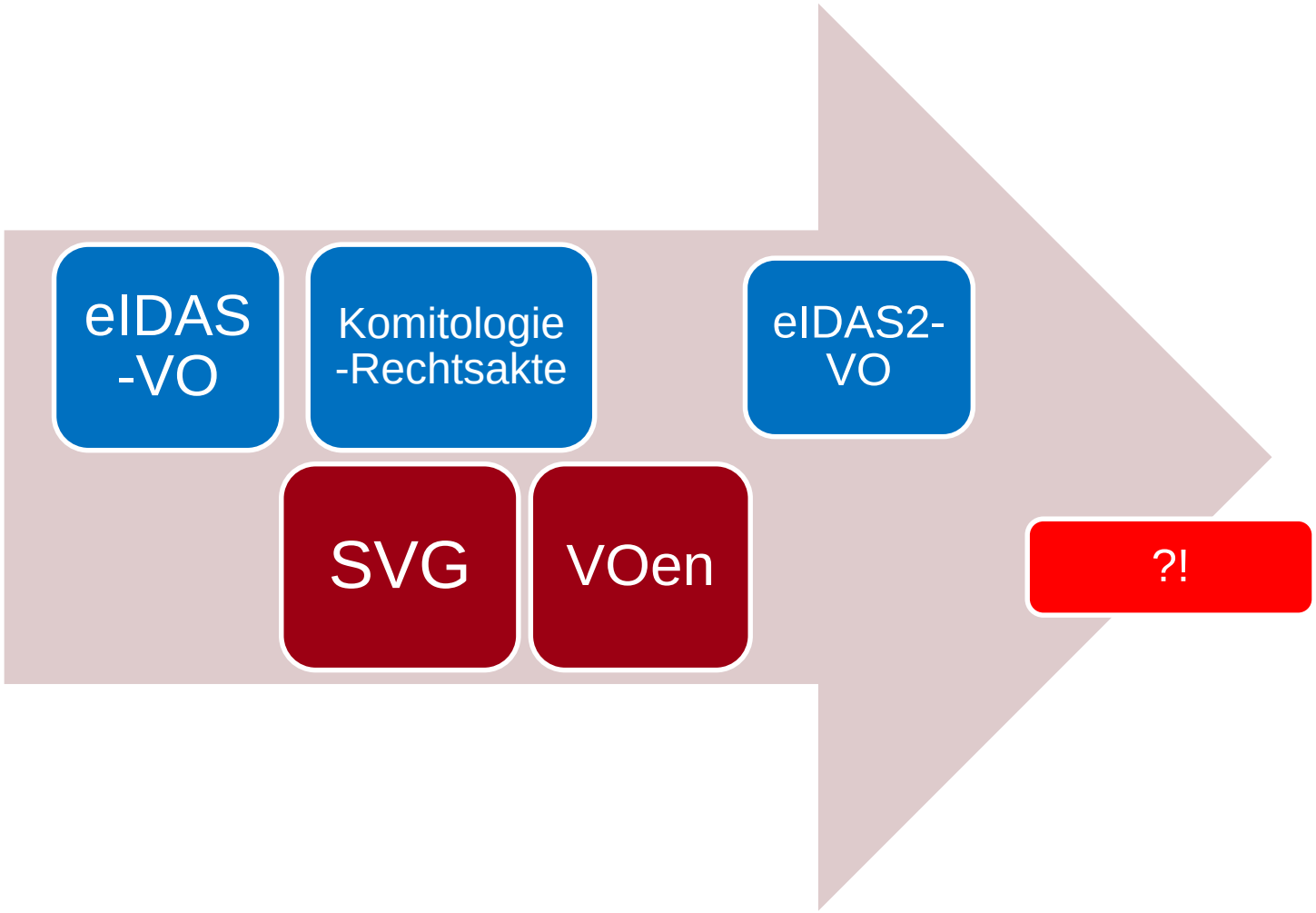
- „Authentizität“

- Die Daten des Signators werden mit einem „Zertifikat“ dokumentiert, das von einer vertrauenswürdigen Stelle ausgestellt wird.

Rechtsquellen bis 30.6.2016



Rechtsquellen ab 1.7.2016



eIDAS-VO – Hintergrund (2014)

- 13 Mio EU BürgerInnen arbeiten in einem anderen EU MS
- 21 Mio KMU – ein signifikanter Teil davon arbeitet international
- 150 Mio EU BürgerInnen shoppen Online; nur 20% davon kaufen aus einem anderen EU MGS

Ergo:

- Elektronischen Zugang erleichtern und Hürden bei der Nutzung der „eigenen“ Methoden beseitigen
- Grenzüberschreitende el. Nutzung ermöglichen
- Vertrauen und Sicherheit heben
- Elektronischen „Vertrauensdiensten“ den selben Wert verleihen wie in der „Papierwelt“

Politisches Committment auf EU-Ebene

- Die **Digitale Agenda** und der **E-Government Aktionsplan** enthielten wesentliche Maßnahmen:
  - 2011: EK-Vorschlag zur Überprüfung der *e*Signatur-Richtlinie, um einen Rechtsrahmen für die grenzübergreifende Anerkennung und Interoperabilität gesicherter elektronischer Authentifizierungssysteme zu schaffen
  - 2012: EK-Vorschlag für einen Beschluss zur EU-weiten gegenseitigen Anerkennung der elektronischen Identität und Authentifizierung.
  - 2012-2014: Einführung und Anwendung von eID-Systemen in den MGS - gestützt auf die Ergebnisse des Projektes STORK.
- Zahlreiche weitere polit. Dok. - **Binnen-marktakte**; **SF des ER; Rats-SF; EP-Resolutionen; Ministerial Declarations; DSM; Digitale Dekade**

Der EU-Rechtsrahmen seit 2016: die eIDAS-VO

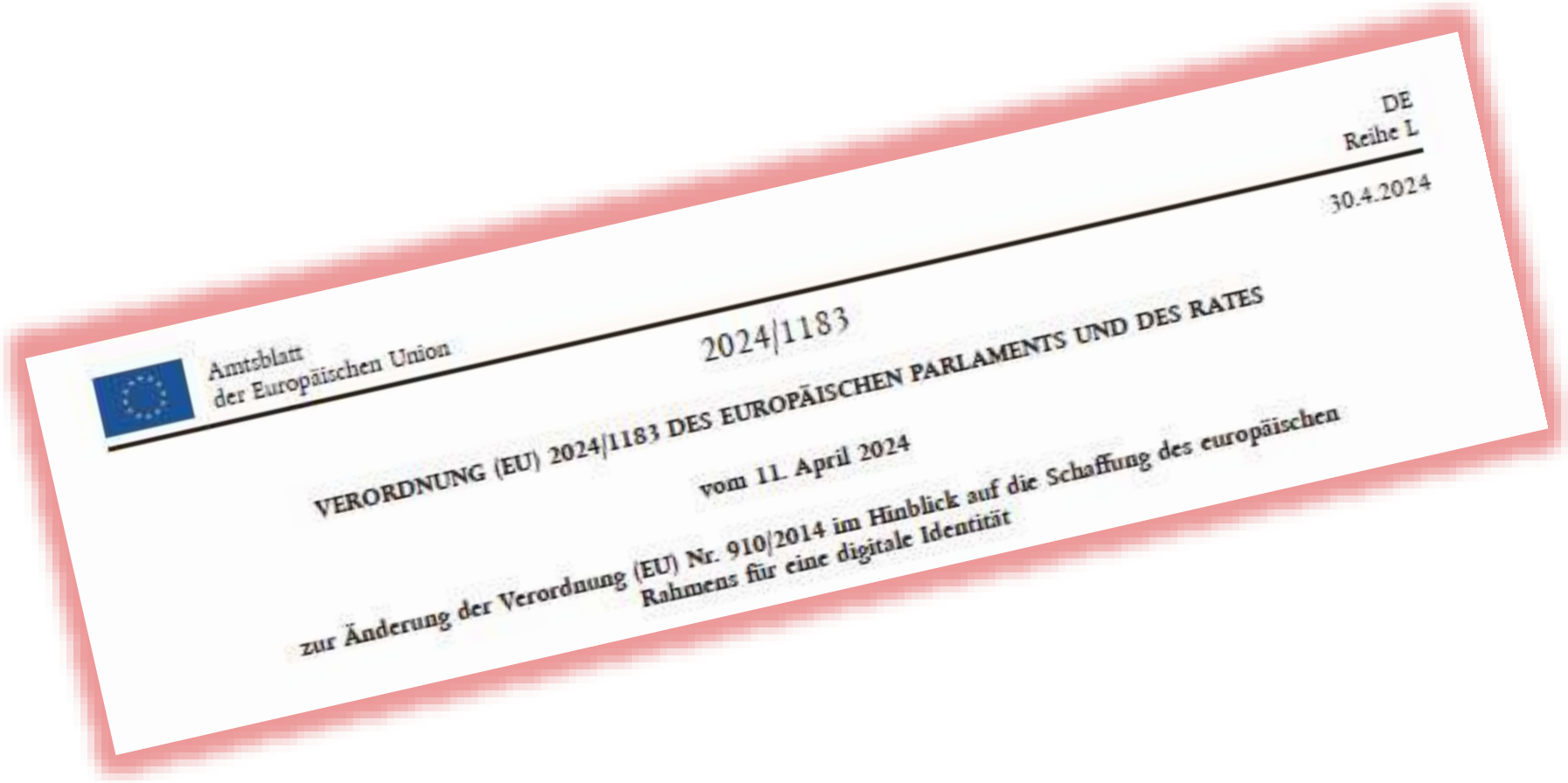
28.8.2014 DE Amtsblatt der Europäischen Union L 257/73

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Seit 2024: Ergänzt durch die „eIDAS2“-VO



Amtsblatt
der Europäischen Union

DE
Reihe L

30.4.2024

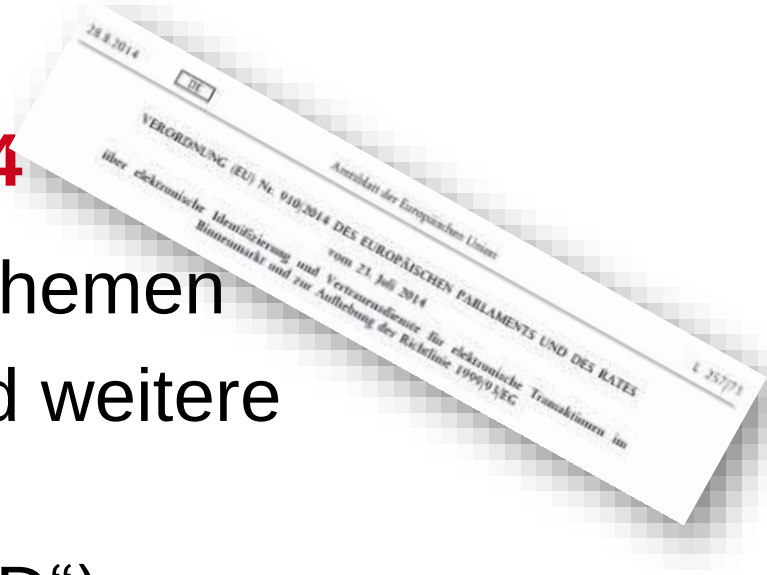
2024/1183

VERORDNUNG (EU) 2024/1183 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 11. April 2024

zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität

Eckpunkte eIDAS1-VO - 2014


28.8.2014 DE Amtsblatt der Europäischen Union L 257/73

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 23. Juli 2014

über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Ein Rechtsakt für die beiden Themen

- **elektronische Signatur** und weitere „Vertrauensdienste“ und
- **elektronische Identität** („eID“)

Die SigRL (im damaligen SigG innerstaatlich umgesetzt) wurde komplett ersetzt

- Typ des Rechtsakts: Verordnung
  - VO ist unmittelbar anzuwenden;
  - bestehende Umsetzungsvorschriften (SigG/ SigV etc.) waren zu bereinigen;
  - Umsetzungen und flankierende Regelungen waren aber notwendig - SVG

„eIDAS1-VO“ 2014: 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)

Vertrauensdienste 2014 (1/2)

- Elektronische Signatur – nat. Person

- Elektronische Siegel – jur. Person (weiter Begriff)

Weitere Vertrauensdienste 2014 (2/2)

- Elektronische Bewahrungsdienste
- Elektronische Validierungsdienste
- Elektronische Zeitstempeldienste
- Elektronische Zustelldienste – „Dienste für die Zustellung elektronischer Einschreiben “
- Website Authentifizierung

Zu diesen fehlen bislang tw. noch relevante internationale Standards und damit die Durchführungsrechtsakte

Durchführungsrechtsakte - Vertrauensdienste

- EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter:
  - Durchführungsverordnung (EU) 2015/806, ABl. Nr. L 128 vom 23.5.2015

- Vertrauensliste
  - Durchführungsbeschluss (EU) 2015/1505, Abl. Nr. L 235 vom 9.9.2015
- Signaturformate
  - Durchführungsbeschluss (EU) 2015/1506, Abl. Nr. L 235 vom 9.9.2015
- Sicherheitsbewertung von QSCD
  - Durchführungsbeschluss (EU) 2016/650, Abl. Nr. L 109 vom 26.4.2016

Legistische Umsetzung in Österreich 1

- nur jene Bereiche geregelt, in denen die unmittelbar anwendbare eIDAS-Verordnung den Mitgliedstaaten die Möglichkeit überlässt (oder die MS dazu verpflichtet – „**hinkende VO**“), nationale Vorschriften zu erlassen.
- Dies betrifft im Bereich der Vertrauensdiensteanbieter insbes.: Aufsicht, Formvorschriften, Haftung und Sanktionen bei Nichteinhaltung der Vorgaben der Verordnung.
- Kern: Elektronische Signaturen (auch Regelungen des aufgehobenen SigG sind enthalten)

Legistische Umsetzung 2 - Bundesgesetze

- Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (**Signatur- und Vertrauensdienstegesetz – SVG**)
- Aufhebung Signaturgesetz
- Novelle E-Government-Gesetz
- Legistische Anpassungen 22 weiterer Bundesgesetze

- Inkrafttreten: **1. Juli 2016**

Legistische Umsetzung 3 - Verordnung

- Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (**Signatur- und Vertrauensdiensteverordnung – SVV**)
- Aufhebung Signaturverordnung

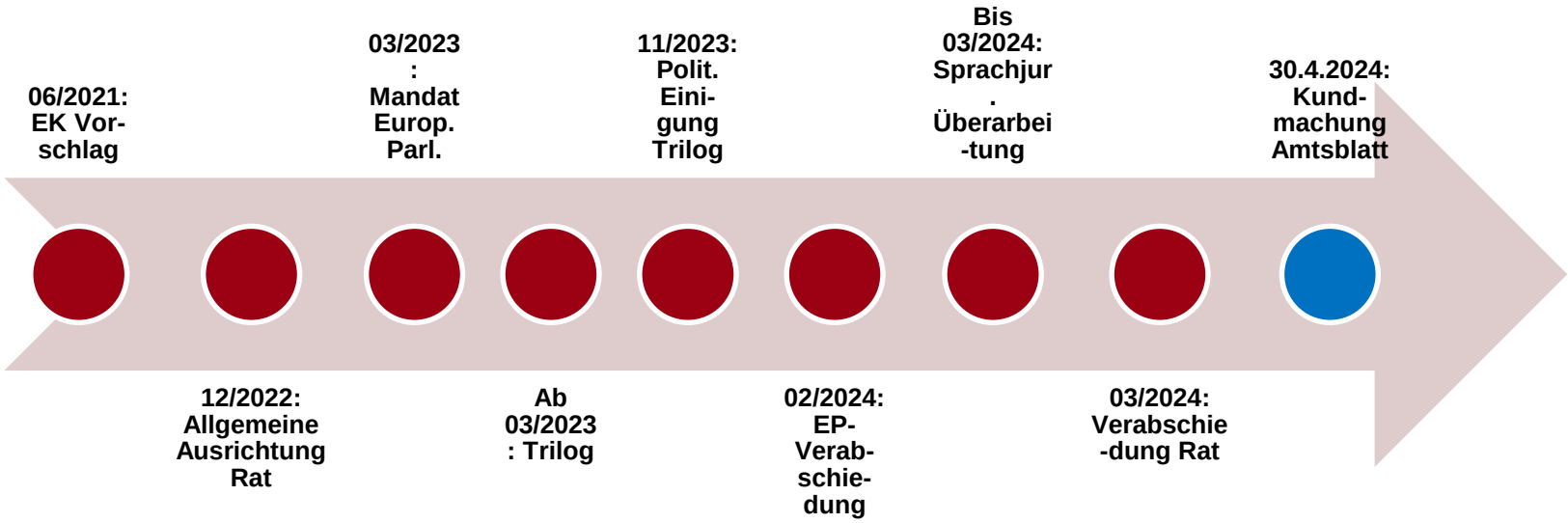
- Verordnung über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)

- Inkrafttreten: **02. August 2016**

VO 2014 vs. VO 2024

- Eckpunkte 2014:
- **Harmonisierung** im Bereich **Vertrauensdienste**. EU-weit: Qu elektronische Signatur einer nat. Person „der handschriftlichen Unterschrift gleichgestellt“
- eID-Kapitel hingegen:
  - Keine Harmonisierung; keine „EU-eID“ - aber freiwillige Notifikation des eID-Systems durch die MS
  - Verpflichtende gegenseitige Anerkennung der von den anderen MS notifizierten eIDs für **E-Government Services**
  - Keine verpflichtende Anerkennung im Privatsektor (sondern „Ermutigung“)

Prozess eIDAS Revision



Wesentliche Neuerungen auf einen Blick:

Vertrauensdienste

- **Einführung neuer Vertrauensdienste**
  - **elektronische Attributsbescheinigungen** (El. attestations of attributes/ „EAA“)
  - **elektronische Journale** (Electronic ledgers)
  - **Verwaltung elektronischer Fernsignatur- und Fernsiegelerstellungseinheiten**
  - **elektronische Archivierungsdienste**
- Neue Regeln für **Website-Authentifizierung**
- Angleichung an **NIS 2 -Regime**

eID

- **Verpflichtung** für alle MS, eine **eID auszustellen**
- **„Europäische Brieftasche für die Digitale Identität“ („Wallet“)** als neuer zwingender Bestandteil in allen MS
- Obligatorische gegenseitige Anerkennung dieser eIDs in allen Mitgliedstaaten – **Anerkennungsverpflichtungen auch** für (große) Player im **Wirtschaftssektor** (Zwei-Faktor-Auth. KYC/ Online Plattformen)

Art. 1 eIDAS-VO - Gegenstand

VO dient

- dem **ordnungsgemäßen Funktionieren des Binnenmarkts** und
- gleichzeitig der Gewährleistung eines **angemessenen Sicherheitsniveaus**

bei elektronischen Identifizierungsmitteln und Vertrauensdiensten.

Zweck:

- um natürlichen und juristischen Personen
- die Ausübung des Rechts auf sichere Teilhabe an der digitalen Gesellschaft und
- auf Zugang zu
  - öffentlichen und
  - privaten Online-Diensten

  in der gesamten Union zu ermöglichen und zu erleichtern.

Art. 1 eIDAS-VO - Gegenstand

Deshalb legt die VO fest:

a) die **Bedingungen**, unter denen die Mitgliedstaaten **elektronische Identifizierungsmittel** für natürliche und juristische Personen, die einem notifizierten elektronischen Identifizierungssystem eines anderen Mitgliedstaats unterliegen **anerkennen**, sowie **europäische Brieftaschen für die Digitale Identität** bereitstellen und anerkennen müssen;

b) **Vorschriften für Vertrauensdienste** und insbesondere für elektronische Transaktionen;

c) **Rechtsrahmen für elektronische Signaturen**, elektronische **Siegel**, elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben, Zertifizierungsdienste für die Website-Authentifizierung, die elektronische Archivierung, die elektronische Attributsbescheinigung, elektronische Signaturerstellungseinheiten, elektronische Siegelerstellungseinheiten und elektronische Journale.“

Art. 2 eIDAS-VO - Anwendungsbereich

(1) Diese Verordnung gilt für von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme, für von einem Mitgliedstaat bereitgestellte europäische Brieftaschen für die Digitale Identität und für in der Union niedergelassene Vertrauensdiensteanbieter.

(2) Diese Verordnung findet **keine Anwendung** auf die Erbringung von Vertrauensdiensten, die **ausschließlich innerhalb geschlossener Systeme** aufgrund von nationalem Recht oder von Vereinbarungen **zwischen einem bestimmten Kreis von Beteiligten** verwendet werden.

(3) Diese Verordnung **berührt nicht** das Unionsrecht oder das nationale Recht in Bezug auf den **Abschluss und die Gültigkeit von Verträgen** oder andere rechtliche oder verfahrensmäßige **Formvorschriften** oder sektorspezifische Formvorschriften.

(4) …. Lässt DSGVO unberührt

Art. 4 eIDAS-VO - Binnenmarktgrundsatz

(1) Die Erbringung von Vertrauensdiensten im Gebiet eines Mitgliedstaats durch einen in einem anderen Mitgliedstaat niedergelassenen Vertrauensdiensteanbieter unterliegt keinen Beschränkungen aus Gründen, die in den Anwendungsbereich dieser Verordnung fallen.

(2) Produkte und Vertrauensdienste, die dieser Verordnung entsprechen, dürfen im Binnenmarkt frei verkehren.

Art. 5 - Pseudonyme bei elektronischen Transaktionen

- Unbeschadet spezifischer Vorschriften des Unionsrechts oder des nationalen Rechts,
- wonach die Nutzer sich identifizieren müssen,
- oder der Rechtswirkungen, die Pseudonyme nach nationalem Recht haben,
- darf die Benutzung von vom Nutzer gewählten Pseudonymen nicht untersagt werden.

Art. 15 eIDAS-VO - Zugänglichkeit

Elektronische Identifizierungsmittel, Vertrauensdienste und zur Erbringung solcher Dienste verwendete Endnutzerprodukte werden

- in einfacher und verständlicher Sprache gemäß dem Übereinkommen über die Rechte von Menschen mit Behinderungen und den Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 zugänglich gemacht,
- wodurch sie auch Personen mit funktionellen Einschränkungen, wie z. B. ältere Personen, und Personen mit eingeschränktem Zugang zu digitalen Technologien zugutekommen.

Art. 16 eIDAS-VO - Sanktionen

Die Mitgliedstaaten legen Regeln für Sanktionen bei Verstößen gegen diese Verordnung fest. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Umsetzung in Ö: siehe bislang § 16 SVG – Verwaltungsstrafbestimmungen

Massive Verschärfung 2024: Mindesthöchststrafen bei Vertrauensdiensteanbietern: 5 Mio € bzw. 1% weltweiter Jahresumsatz

Art. 3 eIDAS-VO - Begriffsbestimmungen

9. „**Unterzeichner**“ ist eine **natürliche** Person, die eine elektronische Signatur erstellt.

10. „**Elektronische Signatur**“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

Somit:
Elektronische Signatur?

Art. 3 eIDAS-VO - Begriffsbestimmungen

9. „**Unterzeichner**“ ist eine **natürliche** Person, die eine elektronische Signatur erstellt.

10. „**Elektronische Signatur**“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.

11. „**Fortgeschrittene elektronische Signatur**“ ist eine elektronische Signatur, die die Anforderungen des Artikels 26 erfüllt.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine **fortgeschrittene** elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.

b) Sie **ermöglicht die Identifizierung** des Unterzeichners.

c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.

- Das Schlüsselpaar darf bei dem Aussteller nur ein einziges Mal existieren und ist der einen Person zugeordnet…

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

b) Sie **ermöglicht die Identifizierung** des Unterzeichners.

- Die Signatur, die mit einem bestimmten öff. Schlüssel geprüft wird, kann nur mit dem korrespondierenden privaten Schlüssel erstellt worden sein.
- Es muss praktisch ausgeschlossen sein, dass der private Schlüssel aus dem öffentlichen Schlüssel errechnet werden kann.

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.

- Signaturerstellung nur durch eine bestimmte dazu berechtigte Person
- Berechtigung durch PIN/ Passwort etc. bzw. zwei-Faktoren-System zur Sicherstellung (Wissen+Besitz)

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.

- „Integrität“
- Unterschiedliche Daten müssen zu unterschiedlichen Hashwerten führen

Art. 26 eIDAS-VO - Anforderungen an fortgeschrittene elektronische Signaturen

Eine **fortgeschrittene** elektronische Signatur erfüllt alle folgenden Anforderungen:

a) Sie ist **eindeutig** dem Unterzeichner zugeordnet.

b) Sie **ermöglicht die Identifizierung** des Unterzeichners.

c) Sie wird unter Verwendung elektronischer **Signaturerstellungsdaten** erstellt, die der Unterzeichner mit einem **hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann**.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung der Daten erkannt werden kann**.

Art. 3 eIDAS-VO – Begriffsbestimmungen…

12. „**Qualifizierte elektronische Signatur**“ ist

- eine fortgeschrittene elektronische Signatur, die
- von einer **qualifizierten elektronischen Signaturerstellungseinheit** erstellt wurde **und**
- auf einem **qualifizierten Zertifikat** für elektronische Signaturen beruht.

13. „**Elektronische Signaturerstellungsdaten**“ sind eindeutige Daten, die vom Unterzeichner zum Erstellen einer elektronischen Signatur verwendet werden.

EU-weite Anerkennung – Art. 24a eIDAS-VO

- Abs. 1: Qualifizierte elektronische Signaturen, die auf einem von einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, und qualifizierte elektronische Siegel, die auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, werden in allen anderen Mitgliedstaaten als qualifizierte elektronische Signaturen bzw. qualifizierte elektronische Siegel anerkannt.
- Die weiteren Absätze enthalten spiegelgleiche Regelungen für alle anderen Vertrauensdienste.

Art. 25 eIDAS-VO - Rechtswirkung elektronischer Signaturen

(1) Einer **elektronischen Signatur** darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.

(2) Eine **qualifizierte elektronische Signatur** hat die **gleiche Rechtswirkung wie eine handschriftliche Unterschrift**.

§ 4 SVG – Rechtswirkungen (1/2)

(1) Eine qualifizierte elektronische Signatur erfüllt das **rechtliche Erfordernis der Schriftlichkeit im Sinne des § 886 ABGB**.

Andere **gesetzliche Formerfordernisse**, insbesondere solche, die die Beiziehung eines Notars oder eines Rechtsanwalts vorsehen, sowie vertragliche Vereinbarungen über die Form **bleiben unberührt**.

Hintergrund: Rechtsvorschriften verlangen häufig Schriftform, zB Abschluss eines befristeten Mietvertrags gem. §29 Abs. 1 Z 3 MRG; Schenkung ohne wirkliche Übergabe gem. 943 ABGB…!

§ 4 SVG – Rechtswirkungen (2/2)

(2) **Letztwillige Verfügungen** können in elektronischer Form **nicht** wirksam errichtet werden. **Folgende** Willenserklärungen können nur **dann** in elektronischer Form wirksam abgefasst werden, **wenn** das Dokument über die Erklärung die Bestätigung eines **Notars** oder eines **Rechtsanwalts** enthält, dass er den **Signator über die Rechtsfolgen seiner Signatur aufgeklärt** hat:

1. Willenserklärungen des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind;
2. eine Bürgschaftserklärung (§ 1346 Abs. 2 ABGB), die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben wird.

§1a Notariatsordnung

Sämtliche bei den Amtsgeschäften nach § 1 entsprechend den Bestimmungen dieses Bundesgesetzes **von dem Notar oder vor dem Notar gesetzten oder bekräftigten elektronischen Signaturen** entfalten auch die Rechtswirkungen der Schriftlichkeit im Sinne des § 886 ABGB; § 4 Abs. 2 SVG ist insoweit nicht anzuwenden.

Qualifizierte Signatur - Konsumentenschutz

Stärkung des Vertrauens in die Akzeptanz qualifiziert signierter Dokumente – Beseitigung der „versteckten“ Klauseln in AGBs (vgl. die Beschwerdefälle von Konsumenten bei Vertragskündigungen)

§ 4 Abs. 3 SVG: Bei Rechtsgeschäften zwischen Unternehmern und Verbrauchern sind Vertragsbestimmungen, nach denen eine qualifizierte elektronische Signatur nicht das rechtliche Erfordernis der Schriftlichkeit erfüllt, für Anzeigen oder Erklärungen, die vom Verbraucher dem Unternehmer oder einem Dritten abgegeben werden, nicht verbindlich, es sei denn, der Unternehmer beweist, dass die Vertragsbestimmungen **im Einzelnen ausgehandelt** worden sind oder mit dem Verbraucher eine andere vergleichbar einfach verwendbare Art der elektronischen Authentifizierung vereinbart wurde .

Art. 3 eIDAS-VO – Begriffsbestimmungen…

14. „**Zertifikat für elektronische Signaturen**“ ist eine elektronische Bescheinigung, die elektronische Signaturvalidierungsdaten mit einer natürlichen Person verknüpft und die mindestens den Namen oder das Pseudonym dieser Person bestätigt.

15. „**Qualifiziertes Zertifikat für elektronische Signaturen**“ ist ein von einem qualifizierten Vertrauensdiensteanbieter ausgestelltes Zertifikat für elektronische Signaturen, das die Anforderungen des Anhangs I erfüllt.

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (1/3)

Qualifizierte Zertifikate für elektronische Signaturen enthalten Folgendes:

a) eine Angabe, dass das Zertifikat als qualifiziertes Zertifikat für elektronische Signaturen ausgestellt wurde, zumindest in einer zur automatischen Verarbeitung geeigneten Form;

b) einen Datensatz, der den **qualifizierten Vertrauensdiensteanbieter**, der die qualifizierten Zertifikate ausstellt, eindeutig repräsentiert und zumindest die Angabe des **Mitgliedstaats** enthält, in dem der Anbieter niedergelassen ist, sowie

— bei einer juristischen Person: den Namen und gegebenenfalls die Registriernummer gemäß der amtlichen Eintragung;

— bei einer natürlichen Person: den Namen der Person;

c) mindestens den **Namen des Unterzeichners** oder ein **Pseudonym**; wird ein Pseudonym verwendet, ist dies eindeutig anzugeben;

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (2/3)

d) elektronische **Signaturvalidierungsdaten**, die den elektronischen Signaturerstellungsdaten entsprechen;

e) Angaben zu **Beginn und Ende der Gültigkeitsdauer** des Zertifikats;

f) den **Identitätscode** des Zertifikats, der für den qualifizierten Vertrauensdiensteanbieter eindeutig sein muss;

g) die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des ausstellenden qualifizierten Vertrauensdiensteanbieters;

Anhang I – Anforderungen an qualifizierte Zertifikate für elektronische Signaturen (3/3)

h) den Ort, an dem das Zertifikat, das der fortgeschrittenen elektronischen Signatur oder dem fortgeschrittenen elektronischen Siegel gemäß Buchstabe g zugrunde liegt, kostenlos zur Verfügung steht;

i) die Angabe des Gültigkeitsstatus des qualifizierten Zertifikats oder den **Ort** der Dienste, die genutzt werden können, um den **Status zu überprüfen**;

j) falls sich die elektronischen Signaturerstellungsdaten, die den elektronischen Signaturvalidierungsdaten entsprechen, in einer **qualifizierten elektronischen Signaturerstellungseinheit** befinden — eine geeignete Angabe dieses Umstands, zumindest in einer zur automatischen Verarbeitung geeigneten Form.

Art. 28 eIDAS-VO – Qualifizierte Zertifikate für elektronische Signaturen

(2) Für qualifizierte Zertifikate für elektronische Signaturen dürfen keine obligatorischen Anforderungen gelten, die über die in Anhang I festgelegten hinausgehen.

(3) Qualifizierte Zertifikate für elektronische Signaturen können zusätzliche **fakultative spezifische Attribute** enthalten. Diese Attribute dürfen die Interoperabilität und Anerkennung qualifizierter elektronischer Signaturen nicht berühren.

Attribute in Ö. zB für Anwälte, Notare, Ziviltechniker!

Berufsspezifische Ausprägungen der elektr. Signaturen („Attribute“ im Zert.)

- Für Berufsgruppen
  - Elektronische Beurkundungssignatur der Notare
  - El. Notarsignatur
  - El. Anwaltssignatur
  - El. Beurkundungssignatur der Ziviltechniker
  - El. Ziviltechnikersignatur

- Für Behörden
  - Elektronische Signatur der Justiz
  - Amtssignatur

Seit 1.7.2016 eigentlich „Siegel“!

§ 13 Abs. 1 Notariatsordnung (1/2)

Zum Zweck der elektronischen Unterfertigung bei den Amtsgeschäften nach § 1 ist der Notar verpflichtet, sich einer qualifizierten elektronischen Signatur zu bedienen, die der Errichtung öffentlicher Urkunden vorbehalten ist (**elektronische Beurkundungssignatur**). Der Notar ist berechtigt, sich bei der Besorgung der Amtsgeschäfte nach § 5 einer qualifizierten elektronischen Signatur als Notar zu bedienen (**elektronische Notarsignatur**). Das Verlangen auf Ausstellung der qualifizierten Zertifikate und der Ausweiskarten für die elektronische Beurkundungssignatur und die elektronische Notarsignatur ist gemäß § 8 Abs. 1 SVG bei der zuständigen Notariatskammer einzubringen.

§ 13 Abs. 1 Notariatsordnung (2/2)

Die **Eigenschaft** als Notar ist in das qualifizierte Zertifikat aufzunehmen (Art. 28 Abs. 3 eIDAS-VO), wenn diese zuverlässig nachgewiesen ist. Der Inhalt der qualifizierten Zertifikate des Notars ist vom VDA im Internet gesichert abfragbar zu machen. Mit dem Erlöschen des Amtes (§ 19 Abs. 1) oder der Suspension (§§ 32 Abs. 2 lit. c, 158, 180) erlischt auch die Befugnis zur Verwendung der elektronischen Beurkundungssignatur und der elektronischen Notarsignatur. Der Notar hat die Ausweiskarten umgehend der Notariatskammer zurückzustellen und beim Vertrauensdiensteanbieter um den Widerruf der Zertifikate zu ersuchen (Art. 24 Abs. 3 eIDAS-VO).

Art. 3 eIDAS-VO – Begriffsbestimmungen…

22. „**Elektronische Signaturerstellungseinheit**“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

23. „**Qualifizierte elektronische Signaturerstellungseinheit**“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des **Anhangs II** erfüllt.

Anhang II – Anforderungen an qualifizierte Signaturerstellungseiheiten (1/2)

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen durch geeignete Technik und Verfahren zumindest gewährleisten, dass

a) die **Vertraulichkeit** der zum Erstellen der elektronischen Signatur verwendeten elektronischen **Signaturerstellungsdaten** angemessen sichergestellt ist, (=kein „Auslesen“)

b) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten **praktisch nur einmal vorkommen** können,

c) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten mit hinreichender Sicherheit **nicht abgeleitet** werden können und die elektronische Signatur bei Verwendung der jeweils verfügbaren Technik **verlässlich gegen Fälschung geschützt** ist, (=nicht „kompromittiert“)

Anhang II – Anforderungen an qualifizierte Signaturerstellungseiheiten (2/2)

d) die zum Erstellen der elektronischen Signatur verwendeten elektronischen Signaturerstellungsdaten vom rechtmäßigen Unterzeichner **gegen eine Verwendung durch andere verlässlich geschützt** werden können. (=PIN/ Passwort neben dem Besitz bzw. der „Kontrolle“)

(2) Qualifizierte elektronische Signaturerstellungseinheiten dürfen die zu unterzeichnenden Daten nicht verändern und nicht verhindern, dass dem Unterzeichner diese **Daten vor dem Unterzeichnen angezeigt** werden. (= „Viewer“)

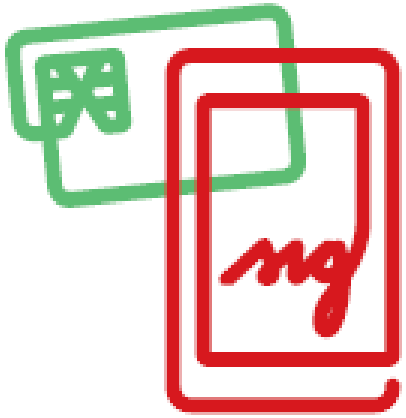
Art. 29 eIDAS-VO – Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

(2) Die Kommission kann im Wege von Durchführungsrechtsakten Kennnummern für Normen für qualifizierte elektronische Signaturerstellungseinheiten festlegen. Bei qualifizierten elektronischen Signaturerstellungseinheiten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs II erfüllen.

eIDAS1-VO: „Verwalten im Namen…“ (1/2)

(Erwägungsgrund 52)

Die Erstellung elektronischer **Fernsignaturen** in einer von einem Vertrauensdiensteanbieter im Namen des Unterzeichners geführten Umgebung soll aufgrund der vielfältigen damit verbundenen wirtschaftlichen Vorteile ausgebaut werden.



eIDAS1-VO: „Verwalten im Namen…“ (2/2)

…Damit **elektronische Fernsignaturen** tatsächlich rechtlich in gleicher Weise anerkannt werden können wie elektronische Signaturen, die vollständig in der Umgebung des Nutzers erstellt werden, sollten die Anbieter von elektronischen Fernsignaturdiensten jedoch spezielle Verfahren für die Handhabung und Sicherheitsverwaltung mit vertrauenswürdigen Systemen und Produkten anwenden, u. a. durch abgesicherte elektronische Kommunikationskanäle, um für eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen zu sorgen und zu gewährleisten, dass diese Umgebung unter alleiniger Kontrolle des Unterzeichners genutzt worden ist.

Nun: explizit geregelter neuer Vertrauensdienst - Art. 3 eIDAS-VO

23a. ‚Qualifizierte elektronische **Fern**signaturerstellungseinheit‘ ist eine qualifizierte elektronische Signaturerstellungseinheit, die von einem qualifizierten Vertrauensdiensteanbieter gemäß Artikel 29a im Namen eines Unterzeichners verwaltet wird.

Und neuer Art. 29a zu den „Anforderungen an einen **qualifizierten Dienst zur Verwaltung** qualifizierter elektronischer Fernsignaturerstellungseinheiten“

Art. 30 eIDAS-VO – Zertifizierung qualifizierter elektronischer Signaturerstellungseinheiten

(1) Die **Konformität** qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II wird von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen **zertifiziert**.

Gültigkeitsdauer der Zertifizierung 5 Jahre und Schwachstellenbeurteilung alle zwei Jahre.

§ 7 SVG - Bestätigungsstelle

(1) Die Konformität qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten mit den Anforderungen des Anhangs II der eIDAS-VO wird durch eine Bestätigungsstelle oder eine in einem anderen Mitgliedstaat der Europäischen Union gemäß Art. 30 Abs. 1 eIDAS-VO benannte Stelle zertifiziert.

…. Anforderungen an die Bestätigungsstelle

(3) Der Bundeskanzler hat mit Verordnung festzustellen, dass eine Einrichtung als Bestätigungsstelle geeignet ist.

Verordnung BGBl. II Nr. 208/2016

„Die Eignung des Vereins **„Zentrum für sichere Informationstechnologie – Austria (A-SIT)“**, die Aufgaben einer Bestätigungsstelle nach dem Signatur- und Vertrauensdienstegesetz (SVG) und den auf seiner Grundlage ergangenen Verordnungen wahrzunehmen, wird festgestellt.“

Erwägungsgrund 56 - QSCD-Zertifizierung

… Diese Verordnung sollte **nicht die gesamte Systemumgebung** abdecken, in der die Einheit betrieben wird. Daher sollte sich der Anwendungsbereich der Zertifizierung qualifizierter Signaturerstellungseinheiten nur auf die Hardware und die Systemsoftware erstrecken, die verwendet werden, um die in der Signaturerstellungseinheit erstellten, gespeicherten oder verarbeiteten Signaturerstellungsdaten zu verwalten und zu schützen. Wie in den einschlägigen Normen angegeben, sollte der Anwendungsbereich der Zertifizierungspflicht **Signaturerstellungs-anwendungen ausschließen**.

Art. 31 eIDAS-VO – Liste der QSCDs

(1) Die MS **notifizieren** der EK Informationen über qualifizierte elektronische Signaturerstellungseinheiten, die von den in Artikel 30 Absatz 1 genannten Stellen zertifiziert worden sind.

(2) Auf der Grundlage der erhaltenen Informationen sorgt die Kommission für die Aufstellung, Veröffentlichung und Führung einer Liste zertifizierter qualifizierter elektronischer Signaturerstellungseinheiten.

Art. 3 eIDAS-VO – Begriffsbestimmungen…

16. „**Vertrauensdienst**“ ist ein elektronischer Dienst, der **in der Regel gegen Entgelt** erbracht wird und aus irgendeiner der folgenden Tätigkeiten besteht:

a) **Ausstellung** von Zertifikaten für elektronische **Signaturen**, von Zertifikaten für elektronische **Siegel**, von Zertifikaten für die **Website-Authentifizierung** oder von Zertifikaten für die Erbringung anderer Vertrauensdienste;

b) **Validierung** von Zertifikaten für elektronische Signaturen, Zertifikaten für elektronische Siegel, Zertifikaten für die Website-Authentifizierung oder Zertifikaten für die Erbringung anderer Vertrauensdienste;

c) Erstellung elektronischer Signaturen oder elektronischer Siegel;

d) …..

„in der Regel gegen Entgelt“

Art. 57 AEUV: Dienstleistungen im Sinne der Verträge sind Leistungen, die **in der Regel gegen Entgelt** erbracht werden, soweit sie nicht den Vorschriften über den freien Waren- und Kapitalverkehr und über die Freizügigkeit der Personen unterliegen.

Als Dienstleistungen gelten insbesondere:

a) gewerbliche Tätigkeiten,

b) kaufmännische Tätigkeiten,

c) handwerkliche Tätigkeiten,

d) freiberufliche Tätigkeiten.

- „**in der Regel gegen Entgelt**“: wirtschaftlicher Charakter, Erwerbszweck

Art. 3 eIDAS-VO – Begriffsbestimmungen…

17. „**Qualifizierter Vertrauensdienst**“ ist ein Vertrauensdienst, der die einschlägigen Anforderungen dieser Verordnung erfüllt.

19. „**Vertrauensdiensteanbieter**“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.

20. „**Qualifizierter Vertrauensdiensteanbieter**“ ist ein Vertrauensdiensteanbieter, der einen oder mehrere qualifizierte Vertrauensdienste erbringt und dem von der Aufsichtsstelle der **Status** eines qualifizierten Anbieters **verliehen** wurde.

Art. 19 eIDAS-VO – Sicherheitsanforderungen an Vertrauensdiensteanbieter

Diese Regelung wurde durch die RL (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („NIS2-RL“) aufgehoben.

Art. 24 eIDAS-VO – Sicherheitsanforderungen an Vertrauensdiensteanbieter

… beschäftigen Personal das über das erforderliche **Fachwissen**, die erforderliche **Zuverlässigkeit**, die erforderliche Erfahrung und die erforderlichen **Qualifikationen** verfügt, in Bezug auf die Vorschriften für die **Sicherheit** und den **Schutz personenbezogener Daten** angemessen geschult worden ist und Verwaltungs- und Managementverfahren anwendet, die den anerkannten europäischen oder internationalen Normen entsprechen.

Art. 24 eIDAS-VO – weitere Anforderungen

- Ausreichende Finanzmittel, Haftpflichtversicherung
- Sie **informieren Personen**, die einen qualifizierten Vertrauensdienst nutzen wollen, in klarer, umfassender und leicht zugänglicher Weise in einem öffentlich zugänglichen Raum und individuell über die genauen Bedingungen für die Nutzung des Dienstes, einschließlich Nutzungsbeschränkungen, bevor sie vertragliche Beziehungen zu dieser Person eingehen..
- Vertrauenswürdige Systeme, Sicherheit, Aufzeichnungspflichten…
- **Zertifikatsdatenbank**…

§ 2 SVV – Konkretisierungen zu qual. VDA-Zuverlässigkeit

- Zutrittssicherung
- Zuverlässiges Personal
- Ausbildung und Fachwissen
- …

Art. 21 eIDAS-VO – Beginn der Erbringung qualifizierter Vertrauensdienste

(1) **Zulassungsverfahren** durch Aufsichtsstelle. Vorlage eines Konformitätsbewertungsberichts einer Konformitätsbewertungsstelle.

(2) **Verleihung des Qualifikationsstatus** und **Veröffentlichung** auf der Vertrauensliste.

(3) Qualif. VDA können mit der Erbringung des qualif. Vertrauensdienstes beginnen, nachdem der qualifizierte Status in den Vertrauenslisten ausgewiesen wurde.

Art. 22 eIDAS-VO – Vertrauenslisten

(1) Jeder MS sorgt für die Aufstellung, Führung und Veröffentlichung von Vertrauenslisten, die Angaben zu den qualifizierten VDA, für die er verantwortlich ist, und den von ihnen erbrachten qualifizierten Vertrauensdiensten, umfassen.

(2) Die MS erstellen, führen und veröffentlichen auf **gesicherte Weise** el. unterzeichnete oder besiegelte Vertrauenslisten in einer für eine **automatisierte Verarbeitung geeigneten Form.**

§14 SVG – Vertrauenslisten

(1) Die **RTR-GmbH** erstellt, führt und veröffentlicht für die Aufsichtsstelle auf gesicherte Weise eine von der RTR-GmbH elektronisch unterzeichnete oder besiegelte Vertrauensliste gemäß Art. 22 eIDAS-VO. Nichtqualifizierte VDA und die von ihnen erbrachten Vertrauensdienste sind auf Antrag in die Vertrauensliste aufzunehmen

„EU-Vertrauensliste“

– Tool: https://eidas.ec.europa.eu/efda/home bzw. direkt https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

Art. 23 eIDAS-VO – EU-Vertrauenssiegel für qualifizierte Vertrauensdiensteanbieter

(1) Nachdem der Qualifikationsstatus in der Vertrauensliste ausgewiesen wurde, können qualif. VDA das EU-Vertrauenssiegel verwenden, um in einfacher, wiedererkennbarer und klarer Weise die von ihnen erbrachten qualifizierten Vertrauensdienste zu kennzeichnen.

(3) Durchführungsrechtsakt für Spezifikationen zur Form und Aufmachung, Zusammensetzung, Größe und Gestaltung des EU-Vertrauenssiegels.

Durchführungsverordnung (EU) 2015/806, ABl. Nr. L 128 vom 23.5.2015

Art. 20 eIDAS-VO – Beaufsichtigung qualifizierter Vertrauensdiensteanbieter

(1) Mind. alle 2 Jahre Prüfung durch Konformitätsbewertungsstelle und Vorlage an Aufsichtsstelle

(2) Jederzeitige Prüfung durch Aufsichtsstelle

„Konformitätsbewertungsstelle“

- Verordnung (EG) Nr. 765/2008 über die Vorschriften für die Akkreditierung von Konformitätsbewertungsstellen und Marktüberwachung von Produkten
- Bundesgesetz über die Akkreditierung von Konformitätsbewertungsstellen (Akkreditierungsgesetz 2012 – AkkG 2012), BGBl. I Nr. 28/2012 - „Akkreditierung Austria“, strenge Akkreditierungsverfahren

- https://eidas.ec.europa.eu/efda/browse/notification/cab-nab

Beaufsichtigung von Vertrauensdiensten

- Art. 46b der neuen eIDAS2-VO:

Die Mitgliedstaaten benennen eine Aufsichtsstelle, die in ihrem Hoheitsgebiet niedergelassen ist, oder sie benennen, aufgrund einer gegenseitigen Vereinbarung mit einem anderen Mitgliedstaat, eine in diesem anderen Mitgliedstaat niedergelassene Aufsichtsstelle.

Diese Aufsichtsstelle ist für die Wahrnehmung der Aufsichtsaufgaben im benennenden Mitgliedstaat im Hinblick auf Vertrauensdienste verantwortlich

§ 12 SVG – Aufsichtsstelle

(1) Aufsichtsstelle gemäß Art. 17 eIDAS1-VO (bzw. dem neuen Art. 46b) ist die **Telekom-Control-Kommission** (§ 116 TKG 2003).

(3) Die Aufsichtsstelle kann sich zur Beratung geeigneter Personen oder Einrichtungen wie etwa einer Bestätigungsstelle bedienen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 7) oder einer in einem anderen Mitgliedstaat der Europäischen Union gemäß Art. 30 Abs. 1 eIDAS-VO benannten Stelle zu erfolgen.

§ 12 SVG – Aufsichtsstelle

(4) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden.

§ 13 SVG: Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der **RTR-GmbH** (§ 16 KOG) bedienen.

§ 15 SVG – Durchführung der Aufsicht

(1) Die VDA haben das Betreten der Geschäfts- und Betriebsräume zu gestatten, Aufzeichnungen oder Unterlagen vorzulegen.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.

(3) …unter möglichster Schonung der Betroffenen und ohne unnötiges Aufsehen so durchzuführen, dass dadurch die Sicherheit der Vertrauensdienste nicht verletzt wird.

§ 10 SVG – Zugangsrechte (1/2)

(1) Auf Ersuchen von Gerichten oder anderen Behörden hat ein qualifizierter VDA **Zugang zur Dokumentation** nach Art. 24 Abs. 2 lit. h eIDAS-VO und seiner Zertifikatsdatenbank zu gewähren.

(2) Bei Verwendung eines **Pseudonyms** in einem Zertifikat hat der VDA die Daten über die Identität des Signators an einen Dritten zu übermitteln, sofern von diesem an der Feststellung der Identität ein **überwiegendes berechtigtes Interesse** glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

§ 10 SVG – Zugangsrechte (2/2)

(3) Die **Dokumentation** ist vom qualifizierten VDA **30 Jahre**, gerechnet ab dem im qualifizierten Zertifikat eingetragenen Ende der Gültigkeit oder, mangels eines solchen, 30 Jahre ab dem Zeitpunkt des Anfallens von einschlägigen Informationen über die von dem qualifizierten VDA im Rahmen seiner Tätigkeit ausgegebenen und empfangenen Daten, **aufzubewahren**.

Art. 3 eIDAS-VO – Begriffsbestimmungen…

40. „**Validierungsdaten**“ sind Daten, die zur Validierung einer elektronischen Signatur oder eines elektronischen Siegels verwendet werden.

41. „**Validierung**“ ist der Prozess der Überprüfung und Bestätigung der Gültigkeit von Daten in elektronischer Form gemäß den Anforderungen dieser Verordnung.

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (1/3)

(1) Mit dem Verfahren für die Validierung einer qualifizierten elektronischen Signatur wird die Gültigkeit einer qualifizierten elektronischen Signatur bestätigt, wenn

a) das der Signatur zugrunde liegende Zertifikat **zum Zeitpunkt des Signierens** ein qualifiziertes Zertifikat für elektronische Signaturen war, das die Anforderungen des Anhangs I erfüllt,

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (2/3)

b) das qualifizierte Zertifikat von einem qualifizierten Vertrauensdiensteanbieter ausgestellt wurde und **zum Zeitpunkt des Signierens gültig** war,

c) die **Signaturvalidierungsdaten** den Daten entsprechen, die dem vertrauenden Beteiligten bereitgestellt werden,

d) der eindeutige Datensatz, der den **Unterzeichner** im Zertifikat repräsentiert, dem vertrauenden Beteiligten korrekt bereitgestellt wird,

e) die etwaige Benutzung eines **Pseudonyms** dem vertrauenden Beteiligten eindeutig angegeben wird,

Art. 32 eIDAS-VO – Anforderungen an die Validierung qualifizierter elektronischer Signaturen (3/3)

f) die elektronische Signatur von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde,

g) die Unversehrtheit der unterzeichneten Daten nicht beeinträchtigt ist,

h) die Anforderungen des Artikels 26 zum Zeitpunkt des Signierens erfüllt waren.

Art. 33 eIDAS-VO – Qualifizierter Validierungsdienst für qualifizierte elektronische Signaturen (3/3)

(1) Qualif. Validierungsdienste für qu. el. Sig. können nur von qualifizierten VDA erbracht werden, die

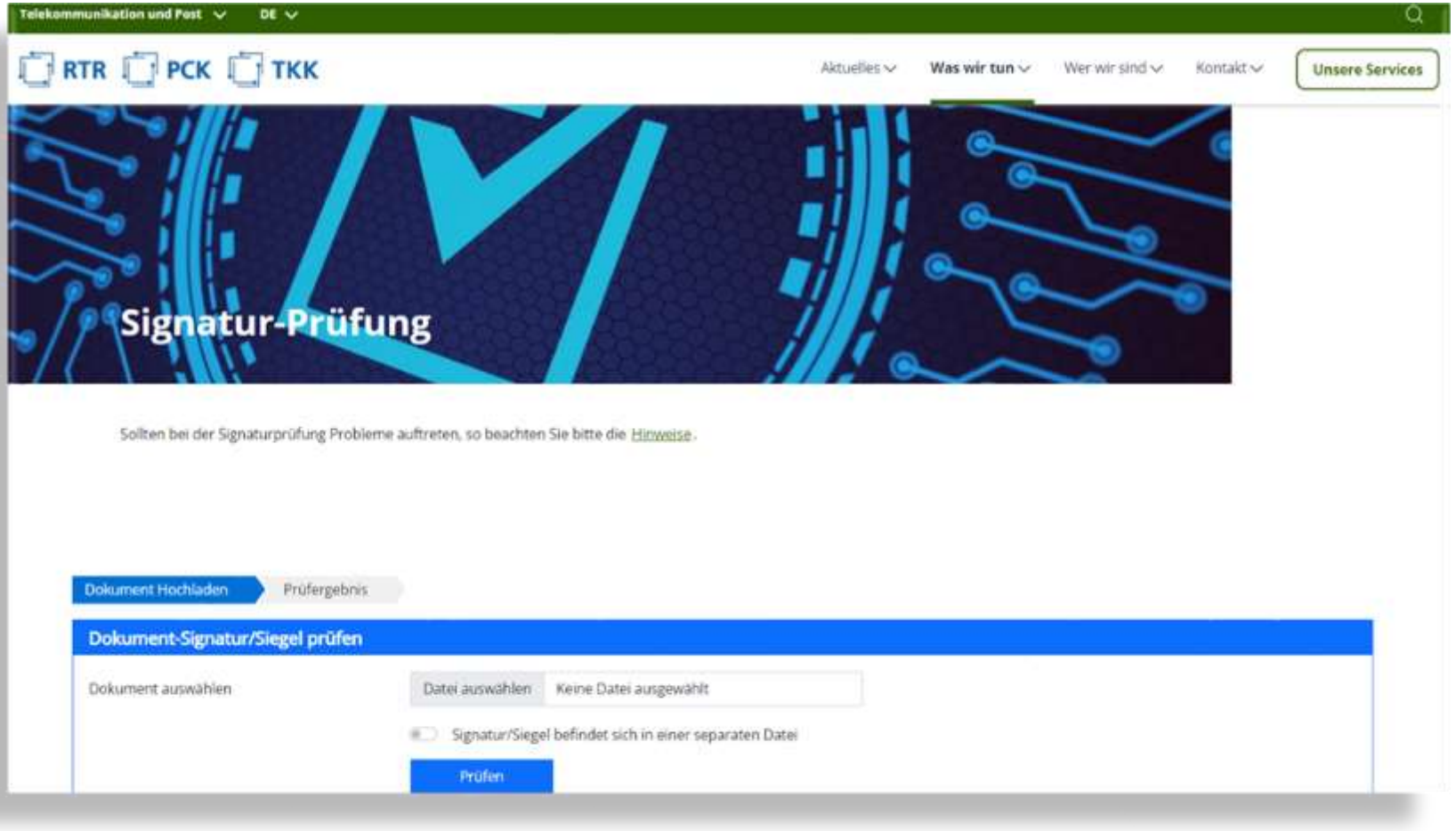
a) eine Validierung gemäß Art. 32 Abs 1 durchführen und

b) es vertrauenden Beteiligten ermöglichen, das Ergebnis automatisch in zuverlässiger und effizienter Weise mit Bestätigung durch die fortgeschrittene elektronische Signatur oder das fortgeschrittene elektronische Siegel des Anbieters des qualif. VDA zu erhalten.

§ 14 SVG - Validierungsservice

(2) Die RTR-GmbH hat für die Aufsichtsstelle **im öffentlichen Interesse kostenfrei** im Internet ein **technisches Service** zur Verfügung zu stellen, **mit dem qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel validiert werden können**. Nach Maßgabe der technischen Möglichkeiten ist eine Schnittstelle für die automatische Verarbeitung anzubieten. …Das Service hat …die Anforderungen des Art. 32 Abs. 1 eIDAS-VO zu erfüllen.

www.signaturpruefung.gv.at



Ist somit die RTR-GmbH ein qualifizierter VDA (der „sich selbst beaufsichtigt“)?

Nein – siehe oben: Art. 3 eIDAS-VO – Begriffsbestimmungen…

16. „**Vertrauensdienst**“ ist ein elektronischer Dienst, der **in der Regel gegen Entgelt** erbracht wird und ….

Art. 24 eIDAS-VO – Ausstellung qual. Zert. (1/2)

(1) Bei der Ausstellung eines qualifizierten Zertifikats oder einer qualifizierten elektronischen Attributsbescheinigung **überprüft** der qualifizierte VDA die **Identität** und gegebenenfalls **spezifische Attribute** der natürlichen oder juristischen Person, der das qualifizierte Zertifikat oder die qualifizierte elektronische Attributsbescheinigung ausgestellt werden soll.

(1a) Überprüfung anhand geeigneter Mittel durch den qVDA direkt oder über einen Dritten:

a) Mit der europ. Brieftasche für die Digitale Identität oder notif. eID (Sicherheitsniveau hoch)

Art. 24 eIDAS-VO – Ausstellung qual. Zert. (2/2)

b) Qual. Zertifikat/ quali. Siegel

c) „mit anderen Identifizierungsmethoden, die die Identifizierung der Person mit einem hohen Maß an Vertrauen gewährleisten und deren Konformität von einer Konformitätsbewertungsstelle bestätigt wird“

d) physische Anwesenheit der natürlichen Person oder eines bevollmächtigten Vertreters der juristischen Person nach geeigneten Nachweisen und Verfahren im Einklang mit dem nationalen Recht.

§ 8 SVG – Ausstellung qual. Zert. (1/2)

1) Ein qualifizierter VDA oder eine in seinem Auftrag tätige Stelle hat die Identität von **persönlich anwesenden** natürlichen Personen oder Vertretern einer juristischen Person, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines **amtlichen Lichtbildausweises oder durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis festzustellen** (Art. 24 Abs. 1 lit. a eIDAS-VO). Vertreter von juristischen Personen haben darüber hinaus einen Nachweis über das Bestehen der Vertretungsbefugnis vorzulegen.

§ 3 SVV - Konkretisierung

Zur Feststellung der Identität von **persönlich anwesenden** natürlichen Personen oder Vertretern einer juristischen Person, denen ein qualifiziertes Zertifikat ausgestellt werden soll (§ 8 Abs. 1 SVG), geeignet sind ein

1. amtlicher Lichtbildausweis oder
2. ein Nachweis, der bescheinigt, dass die Identität zumindest mit jener Verlässlichkeit geprüft wurde, wie sie bei der Zustellung zu eigenen Handen (§ 21 ZustG) einzuhalten ist.

Die Daten des Lichtbildausweises oder des anderen Nachweises (§ 8 Abs. 1 erster Satz SVG) sind zu erfassen und mit dem Antrag zu dokumentieren, sofern sie nicht schon dokumentiert wurden. Die Erfassung und Dokumentation kann auch in ausschließlich elektronischer Form erfolgen.

§ 8 SVG – Ausstellung qual. Zert. (2/2)

2) Erfolgt die Ausstellung **nicht in persönlicher Anwesenheit**, können auch **sonstige Identifizierungsmethoden**, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, angewendet werden (**Art. 24 Abs. 1 lit. d eIDAS1-VO**). Dabei ist insbesondere **auf eine erfolgte Identifizierung anhand eines Nachweises iSd Abs. 1, die von einer vertrauenswürdigen Stelle durchgeführt wurde, zurückzugreifen**.

§ 5 SVG – Pflichten der Signatoren

Signatoren haben ihre elektronischen **Signaturerstellungsdaten sorgfältig zu verwahren**, soweit zumutbar **Zugriffe** von Dritten auf ihre elektronischen Signaturerstellungsdaten **zu verhindern** und deren Weitergabe an Dritte zu unterlassen… Signatoren haben den **Widerruf** des qualifizierten Zertifikats **zu verlangen**, wenn die elektronischen Signaturerstellungsdaten **abhandenkommen**, wenn Anhaltspunkte für deren **Kompromittierung** bestehen oder wenn **sich die im qualifizierten Zertifikat bescheinigten Umstände geändert** haben.

Art. 24 eIDAS-VO – Widerruf

(3) Bei Widerruf: VDA **registriert den Widerruf in seiner Zertifikatsdatenbank** und veröffentlicht den Widerrufsstatus des Zertifikats zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens. Der Widerruf wird sofort nach seiner Veröffentlichung wirksam.

(4) …Informationen über den Gültigkeits- oder **Widerrufsstatus** der ausgestellten qualifizierten Zertifikate. … **jederzeit** und **über die Gültigkeitsdauer des Zertifikats hinaus automatisch**, zuverlässig, kostenlos..

Art. 28 eIDAS-VO – Aussetzung

(5) MS können vorbehaltlich der folgenden Bedingungen **nationale Vorschriften zur vorläufigen Aussetzung** eines qual. Zertifikats für eine elektronische Signatur erlassen:

a) Ist ein qualifiziertes Zertifikat für elektronische Signaturen vorläufig ausgesetzt worden, so **verliert dieses Zertifikat für die Dauer der Aussetzung seine Gültigkeit.**

b) Die Dauer der Aussetzung wird in der Zertifikatsdatenbank deutlich angegeben und der Status der Aussetzung ist während der Dauer der Aussetzung ersichtlich.

§ 6 SVG – Aussetzung (1/3)

(1) Sofern ein qual. VDA ein qual. Zertifikat nicht widerruft, hat er dieses vorläufig auszusetzen, wenn

1. der Signator, der Siegelersteller oder ein sonstiger dazu Berechtigter dies **verlangt**,
2. die **Aufsichtsstelle** (§ 12) die Aussetzung des Zertifikats **anordnet**,
3. der qualifizierte VDA Kenntnis vom **Ableben** des Signators, der Beendigung des Bestehens des Siegelerstellers oder sonst von der **Änderung im Zertifikat bescheinigter Umstände** erlangt,

§ 6 SVG – Aussetzung (2/3)

4. das Zertifikat auf Grund **unrichtiger Angaben** erwirkt wurde oder
5. die **Gefahr einer missbräuchlichen Verwendung** des Zertifikats besteht.

(2) Ein qualifizierter VDA hat bei Vorliegen der in Abs. 1 genannten Umstände die Aussetzung zeitnah und in jedem Fall innerhalb von 24 Stunden nach Erhalt des Ersuchens vorzunehmen.

§ 6 SVG – Aussetzung (3/3)

(3) Ist ein qualifiziertes Zertifikat für elektronische Signaturen oder elektronische Siegel vorläufig ausgesetzt worden, so **verliert dieses Zertifikat**, **solange der Status der Aussetzung gemäß Abs. 4 veröffentlicht ist, seine Gültigkeit**. Dieser Zeitraum **darf zwei Wochen nicht überschreiten**.

(4) Ein qual. VDA hat die Dauer der Aussetzung in seiner Zertifikatsdatenbank zu registrieren und den Status der Aussetzung **während der Dauer der Aussetzung** elektronisch jederzeit allgemein zugänglich zu veröffentlichen.

§ 5 SVV – Aussetzung

(7) Im Fall einer Aussetzung eines qualifizierten Zertifikats **ist der Signator oder der Siegelersteller unverzüglich zu verständigen**. Die **Aussetzung kann aufgehoben werden**. Eine aufgehobene Aussetzung hat auf die Gültigkeit des Zertifikats keinen Einfluss. **Wird eine Aussetzung nicht aufgehoben, so ist das Zertifikat zu widerrufen**. **Erfolgt auf Grund einer Aussetzung der Widerruf eines Zertifikats, so gilt bereits die Aussetzung als Widerruf**.

Art. 13 eIDAS-VO – Haftung des VDA (1/2)

(1) …haften VDA für alle natürlichen oder juristischen Personen **vorsätzlich oder fahrlässig** zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind. …

Die **Beweislast** für den Nachweis des Vorsatzes oder der Fahrlässigkeit seitens eines **nichtqualifizierten** VDA liegt **bei** der natürlichen oder juristischen **Person**, die den in Unterabsatz 1 genannten **Schaden geltend macht**.

Art. 13 eIDAS-VO – Haftung des VDA (2/2)

Bei einem **qualifizierten** VDA **wird von Vorsatz oder Fahrlässigkeit ausgegangen**, **es sei denn**, der qualifizierte **VDA weist nach**, dass der in Unterabsatz 1 genannte Schaden entstanden ist, ohne dass er vorsätzlich oder fahrlässig gehandelt hat.

(2) Beschränkungen möglich, wenn informiert und ersichtlich – Haftung nicht bei einer über diese Beschränkungen hinausgehenden Verwendung

(3) Anwendung „im Einklang mit den nationalen Vorschriften über die Haftung“

§ 11 SVG - Haftung

(1) Abgesehen von Art. 13 Abs. 2 eIDAS-VO kann die Haftung eines VDA nach Art. 13 Abs. 1 eIDAS-VO im Vorhinein weder ausgeschlossen noch beschränkt werden.

(2) Umfang und Ausmaß des nach Art. 13 eIDAS-VO zu ersetzenden Schadens sowie allfällige Rückgriffsrechte gegenüber anderen Personen richten sich nach den auf den Schadensfall sonst anwendbaren Bestimmungen.

(3) Ersatzansprüche gegenüber anderen Personen oder aus einem anderen Rechtsgrund bleiben unberührt

Art. 24 eIDAS-VO - Beendigungsplan

(2) lit. i) VDA verfügen über einen fortlaufend aktualisierten **Beendigungsplan**, um die **Kontinuität** des Dienstes nach den von der Aufsichtsstelle gemäß Artikel 46b Absatz 4 Buchstabe i geprüften Vorgaben sicherzustellen

Dort ist als **Aufsichtsaufgabe** vorgesehen: Überprüfung des Vorliegens und der ordnungsgemäßen Anwendung von Vorschriften über Beendigungspläne für den Fall, dass der Vertrauensdiensteanbieter seine Tätigkeit einstellt, wobei auch die Frage, wie die Informationen (Dokumentationen…) weiter zugänglich gehalten werden, geprüft wird;

§ 9 SVG - Beendigungsplan und Vertrauensinfrastruktur (1/2)

(1) Ein qualifizierter VDA hat der Aufsichtsstelle zumindest drei Wochen im Vorhinein die geplante Einstellung seiner Tätigkeit anzuzeigen.

(2) Widerruf der gültigen qualifizierten Zertifikate oder dafür Sorge zu tragen, dass zumindest seine Zertifikatsdatenbank von einem anderen qualifizierten VDA übernommen wird. Auch im Fall des Widerrufs der qualifizierten Zertifikate hat der qualifizierte VDA sicherzustellen, dass die Zertifikatsdatenbank weitergeführt wird;

§ 9 SVG - Beendigungsplan und Vertrauensinfrastruktur (2/2)

(2) kommt er dieser Verpflichtung nicht nach, so hat die **Aufsichtsstelle** als Teil ihrer Vertrauensinfrastruktur für die **Weiterführung der Zertifikatsdatenbank** auf Kosten des qualifizierten VDA Sorge zu tragen.

(3) Ein **Widerruf** der gültigen qualifizierten Zertifikate gemäß Abs. 2 ist nur dann zulässig, **wenn** die Aufsichtsstelle auf Antrag des BMF feststellt, dass deren **Weiterführung nicht im öffentlichen Interesse gelegen** ist. Ist der Widerruf unzulässig, hat der Bund für deren Weiterführung Sorge zu tragen.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (1/3)

(1) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine **fortgeschrittene** elektronische Signatur, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen, und qualifizierte elektronische Signaturen zumindest in den **Formaten** oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (2/3)

(2) Verlangt ein Mitgliedstaat für die Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle oder im Namen einer öffentlichen Stelle angeboten wird, eine **fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht**, so erkennt dieser Mitgliedstaat fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat beruhen, und qualifizierte elektronische Signaturen zumindest in den **Formaten** oder unter Verwendung der Verfahren an, die in den Durchführungsrechtsakten nach Absatz 5 festgelegt sind.

Art. 27 eIDAS-VO - Elektronische Signaturen in öffentlichen Diensten (3/3)

(3) Die Mitgliedstaaten **verlangen** für die grenzüberschreitende Verwendung in einem Online-Dienst, der von einer öffentlichen Stelle angeboten wird, **keine elektronische Signatur mit einem höheren Sicherheitsniveau als dem der qualifizierten elektronischen Signatur**.

(5)…Komitologiebeschlüsse für Normen und Referenzformate…

„Signaturformate“

Siehe den **Durchführungsbeschluss (EU) 2015/1506** zur Festlegung von Spezifikationen für Formate fortgeschrittener elektronischer Signaturen und fortgeschrittener Siegel, die von öffentlichen Stellen gemäß Artikel 27 Absatz 5 und Artikel 37 Absatz 5 der Verordnung (EU) Nr. 910/2014.

- MS erkennen fortgeschrittene elektronische **XML-, CMS- und PDF-Signaturen** der Konformitätsstufen **B, T oder LT** und Signaturen mit zugehörigen Containern an, wenn diese Signaturen die technischen Spezifikationen des Anhangs erfüllen…
- Bei **anderen Formaten: Validierungsservice** muss angeboten werden (kostenlos, online, verständlich…)

Elektronisches Siegel

- „Signatur“ der **juristischen** Person
- Art. 3 Z 25 eIDAS-VO: „Elektronisches Siegel“ sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, **um deren Ursprung und Unversehrtheit sicherzustellen**.
- Begrifflichkeiten angepasst:
  - Signator – Siegelersteller
  - Signaturerstellungsdaten – Siegelerstellungsdaten
  - Signaturerstellungseinheit – Siegelerstellungseinheit

Art. 35 eIDAS-VO – Rechtswirkungen el. Siegel

(1) Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.

(2) Für ein **qualifiziertes elektronisches Siegel** gilt die **Vermutung der Unversehrtheit der Daten** und der **Richtigkeit der Herkunftsangabe** der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

Art. 14 eIDAS-VO – Internationale Aspekte

(1) Vertrauensdienste, die von in einem Drittland niedergelassenen VDA oder von einer internationalen Organisation bereitgestellt werden, werden als rechtlich gleichwertig mit den Vertrauensdiensten anerkannt, die von in der Union niedergelassenen qualifizierten VDA bereitgestellt werden, sofern die aus dem Drittland oder von einer internationalen Organisation stammenden Vertrauensdienste **im Wege von Durchführungsrechtsakten oder** einer **gemäß Artikel 218 AEUV geschlossenen Vereinbarung** zwischen der Union und dem betreffenden Drittland oder der internationalen Organisation anerkannt sind..

Relevante Entwicklungen auf internationaler Ebene dazu

UNCITRAL – WG IV (Electronic Commerce) hat ein Model Law zur Nutzung und grenzüberschreitenden Anerkennung von eIDs und Vertrauensdiensten erarbeitet und 2022 abgeschlossen:

https://uncitral.un.org/en/mlit

Zusammenfassung

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens: EU (eIDAS-VO) und national (SVG/SVV)

Überblick

- E-Kommunikation birgt Risken in sich
  - Wer ist mein Gegenüber?
  - Wurde etwas verändert?

- Lösung dazu elektronische Signatur/Siegel
  - Elektronisch signierte Texte können nicht unbemerkt verändert werden (weder am Übertragungsweg noch vom Empfänger)
  - Absender kann Text nicht abstreiten (z.B. verbindliches Angebot)

- Elektronische Signaturen/Siegel gibt es in unterschiedlichen Qualitäten
  - Einfache Signaturen/Siegel (geringere technische und organisatorische Anforderungen)
  - Qualifizierte Signatur/Siegel (hohe technische und organisatorische Anforderungen)

Elektronische Signatur

- **„Einfache“ elektronische Signatur**
  - Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet
- **„fortgeschrittene“ elektronische Signatur**
  - elektronische Signatur, die die Anforderungen des Artikels 26 der eIDAS-VO erfüllt:
    - a) ist eindeutig dem Unterzeichner zugeordnet.
    - b) ermöglicht die Identifizierung des Unterzeichners.
    - c) wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
    - d) ist so mit den unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.
- **„qualifizierte“ elektronische Signatur**
  - Ist eine fortgeschrittene Signatur
  - beruht auf einem qualifizierten Zertifikat
  - mit einer qualifizierten Signaturerstellungseinheit (QSCD) erzeugt.

Rechtswirkung

- „Einfache“ & „fortgeschrittene“ Signatur
  - müssen als Beweismittel zugelassen werden
  - unterliegen der richterlichen Beweiswürdigung
  - Grundsatz der Nichtdiskriminierung

Art. 25 (1) eIDAS-VO: „Einer elektronischen Signatur darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil sie in elektronischer Form vorliegt oder weil sie die Anforderungen an qualifizierte elektronische Signaturen nicht erfüllt.“

- **„Qualifizierte“ Signatur**
  - EU-weit der handschriftlichen Unterschrift gleichgestellt (Art. 25 Abs. 2 eIDAS-VO iVm § 4 Abs. 1 SVG (-Erfordernis der Schriftlichkeit nach §886 ABGB))
  - Ausnahmen:
    - Letztwillige Verfügungen (vgl. auch NO)
    - bei Schriftformerfordernis im Familien- & Erbrecht*
    - Bürgschaftserklärungen (außer Geschäftsverkehr)*

* Diese Willenserklärungen können in elektr. Form abgefasst werden, wenn Signator von Rechtsanwalt/Notar über Rechtsfolgen der Signatur aufgeklärt wurde.

Qual. Signatur – qual. Siegel

- Qualifizierte elektronische Signatur – nat. Person
  - Rechtswirkungen (Art. 25 eIDAS-VO): „der handschriftlichen Unterschrift gleichgestellt“
- Elektronische Siegel – jur. Person (weiter Begriff)
  - Rechtswirkung qual. elektronischer Siegel (Art. 35 Abs. 2 eIDAS): „Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.“

Berücksichtigung innovativer Möglichkeiten:
Fernsignatur-/ Fernsiegelerstellungseinheiten…
(server/remote signing; HSM etc.)

Qualifiziertes Zertifikat

- Basis für qualifizierte elektronische Signatur (Anhang I eIDAS-VO):
  - Hinweis, dass es sich um ein qualifiziertes Zertifikat handelt
  - den unverwechselbaren Namen des qu. Vertrauenssdiensteanbieters (VDA) und den Staat seiner Niederlassung
  - Namen des Signators
  - Signaturvalidierungsdaten
  - Gültigkeitsdauer des Zertifikats
  - eindeutige Kennung des Zertifikats
  - Signatur/Siegel des qu. VDA

Vertrauensdiensteanbieter (VDA)

- VDA (Art. 3 Z 19 eIDAS-VO) =
  natürliche od. juristische Person, die einen oder mehrere Vertrauensdienste erbringt
- Spezielle Anforderungen an qualifizierte VDA in Art. 24 eIDAS-VO
- Zulassung durch die Aufsichtsbehörde (Telekom-Control-Kommission bzw. RTR) – konstitutive Liste
- Vor Zulassung als qualifizierter Vertrauensdienste ist vom VDA ein Konformitätsbewertungsbericht vorzulegen (Art. 21 eIDAS-VO)

Ausstellung eines qualifizierten Zertifikats

Qu. VDA (od. in seinem Auftrag tätige Stelle) hat gem. Art. 24 Abs. 1 eIDAS-VO iVm § 8 Abs. 1 SVG die Identität **von persönlich anwesenden Personen** anhand:

- eines amtlichen Lichtbildausweises oder
- durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis festzustellen

Bei **nicht persönlich anwesenden Personen**, können auch gem. § 8 Abs. 2 SVG auch sonstige Identifizierungsmethoden, die eine gleichwertige Sicherheit hinsichtlich der Verlässlichkeit bei der persönlichen Anwesenheit bieten, angewendet werden.

- Rückgriff auf bereits erfolgte Identifizierung anhand eines Nachweises gem. Abs. 1 durch vertrauenswürdige Stelle

Qualifizierte Signaturerstellungseinheit

- Verarbeitung der Signaturerstellungsdaten
  - Chipkarte/ HSM

- Nicht: Systemumgebung/ Kartenleser/ Signatursoftware/…
- Erfüllung der Sicherheitsanforderungen muss von einer Bestätigungsstelle gem. § 7 SVG (in Ö: A-Sit) bescheinigt sein (Art. 30 Abs. 1 eIDAS-VO)

Berufsspezifische Ausprägungen der elektronischen Signaturen

- Für Berufsgruppen
  - Elektronische Beurkundungssignatur der Notare
  - El. Notarsignatur
  - El. Anwaltssignatur
  - El. Beurkundungssignatur der Ziviltechniker
  - El. Ziviltechnikersignatur

- Für Behörden
  - Elektronische Signatur der Justiz
  - Amtssignatur

Seit 1.7.2016: eigentlich „Siegel“!

Elektronisches Siegel

- Für juristische Personen
- „digitaler Stempel“
- Für qu. elektr. Siegel gelten ähnliche Anforderungen wie für qu. elektr. Signaturen
- **Nicht** dieselben Rechtswirkungen einer qu. Elektronischen Signatur!
- Mit elektronischen Siegeln werden der Ursprung und die Unversehrtheit von Daten sichergestellt (Art. 3 Z 25 iVm. Art. 35ff eIDAS-VO).

Agenda Teil 2

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens: EU (eIDAS-VO) und national (SVG/SVV)
5. Verfahrensrechtliche Anforderungen, Amtssignatur
6. Weitere „Vertrauensdienste“ – insbes. nach der „neuen“ eIDAS-VO
7. Elektronische Signatur und Identitätsmanagement
8. Von der „Bürgerkarte“ und der „Handy-Signatur“ zur „Identity Austria“
9. EU-eID – „Wallet“ und aktuelle Entwicklungen

Amtssignatur (§ 19 Abs. 1 und 2 E-GovG)

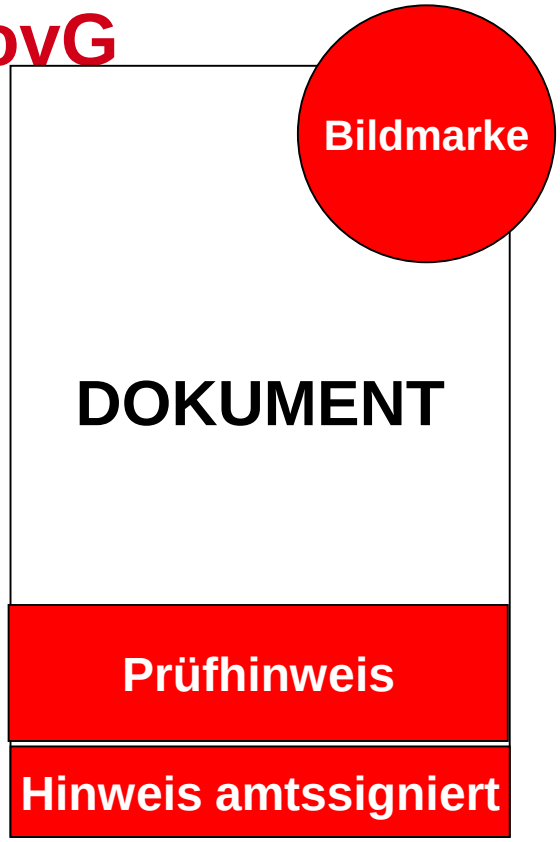
- Amtssignatur ist eine fortgeschrittene elektronische Signatur oder ein fortgeschrittenes elektronisches Siegel, deren **Besonderheit** durch ein **entsprechendes Attribut** im Signaturzertifikat oder Zertifikat für elektronische Siegel ausgewiesen wird
- Attribut ist ein **Object Identifier (OID)** der vom Vertrauensdiensteanbieter nach Prüfung der „Behördeneigenschaft“ (Verantwortlicher des öffentlichen Bereichs) in das Zertifikat eingetragen wird
- Amtssignatur dient der **erleichterten Erkennbarkeit der Herkunft** eines Dokuments von einem Verantwortlichen des öffentlichen Bereichs durch:
  - Automatisch durch OID
  - Durch die Visualisierung am Dokument (§ 19 Abs. 3 E-GovG)

Amtssignatur (§ 19 E-GovG)

- nur für Verwendung durch Verantwortliche des öffentlichen Bereichs (z.B. Erledigungen)
- Hoheits- & Privatwirtschaftsverwaltung (mit unterschiedlicher Rechtswirkung)
- mindestens „fortgeschrittene“ Signatur oder Siegel
- Behörde tritt seit 1. Juli 2016 in der Regel als Siegelersteller auf
- Amtssignatur kann auf softwarebasiertem Serverzertifikat beruhen (weil fortg. Siegel und nicht qual. Siegel…)

Amtssignatur – Mindestanforderung Visualisierung - § 19 Abs. 3 E-GovG

- Bildmarke, jedoch keine „fixen“ Designvorgaben
- der Verantwortliche des öffentlichen Bereichs muss die Bildmarke jeden-falls als die seine gesichert im Internet veröffentlichen
- Bereitstellung Information zur elektr. Prüfung
- Hinweis, dass amtssigniert
- Anordnung der Elemente im Dokument frei
  - Vgl. Entscheidung des VwGH vom 16.12.2015, Ra 2015/03/0017
  - z.B. Bildmarke auf der ersten Seite des Erkenntnisses



Empfohlene Darstellung der Amtssignatur

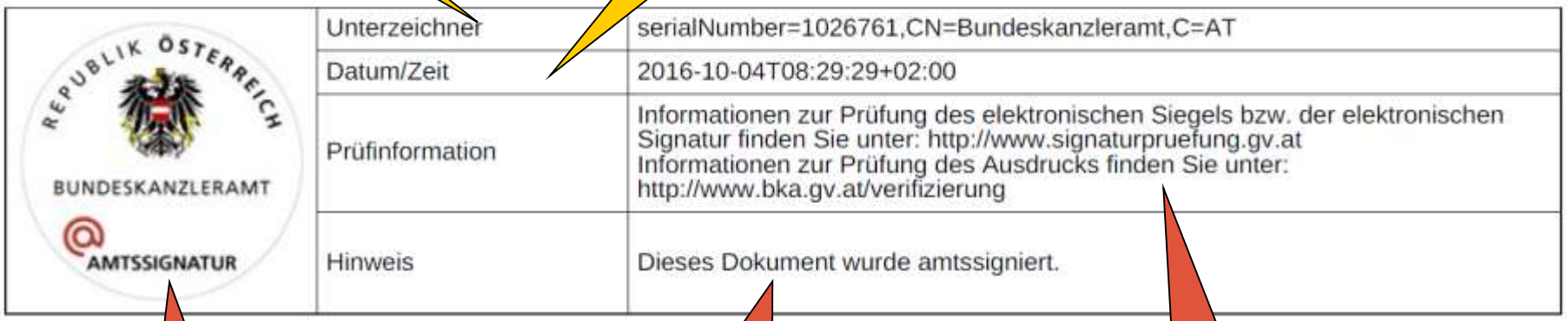
- Signaturblock am Ende des Dokuments:

	**Unterzeichner/ Siegelersteller**	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Datum/Zeit-UTC	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://hierdieURL1.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://hierdieURL2.gv.at
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Amtssignatur Variante

Unterzeichner/ Siegelersteller

Datum & Uhrzeit der Ausstellung



Unterzeichner	serialNumber=1026761,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2016-10-04T08:29:29+02:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.

Bildmarke nach E-GovG

Hinweis auf Amtssignatur

Hinweis auf Prüfung

Bildmarken des öffentlichen Bereichs

- Sammlung der Bildmarken:
- https://www.usp.gv.at/it-geistiges-eigentum/e-government/bildmarken-des-oeffentlichen-bereichs.html

Beweiskraft (§ 20 E-GovG)

- elektronisches amtssigniertes Dokument ist das Original = öffentliche Urkunde
- auch **Ausdruck** eines amtssignierten Dokuments hat im Rahmen der Hoheitsverwaltung (z.B. Bescheid) die Beweiskraft einer öffentlichen Urkunde (§ 292 ZPO)
  - Amtssignatur muss prüfbar/verifizierbar sein, z.B. durch:
    - Online-Archiv
    - Kontaktadresse für die Prüfung der Echtheit
- unabhängig ob Behörde oder Empfänger das amtssignierte Dokument ausdruckt

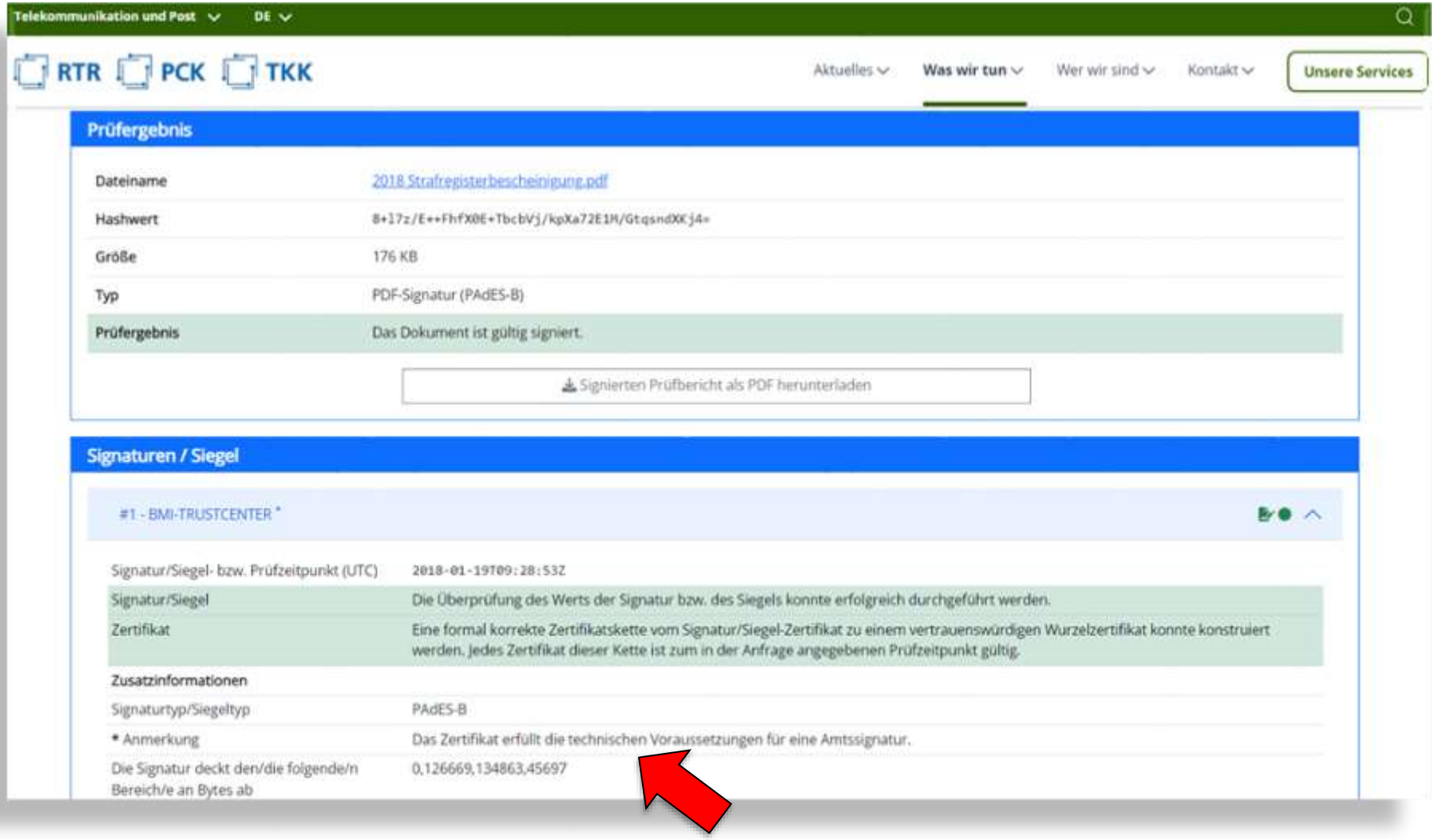
Elektronische Prüfung

- Behörde stellt selbst Prüfservice zur Verfügung

Oder

- Behörde verweist auf zentrales Prüfservice, z.B.:
  - www.signaturpruefung.gv.at
    (Betrieb RTR – Rundfunk u. Telekom Regulierungsbehörde, Aufsichtsstelle gem. SVG)

Ergebnis der Signaturprüfung



AVG – Erledigungen …. Ausfertigungen

- **§ 18.** (3) Schriftliche Erledigungen sind vom Genehmigungsberechtigten mit seiner Unterschrift zu genehmigen; wurde die **Erledigung elektronisch erstellt, kann an die Stelle dieser Unterschrift ein Verfahren zum Nachweis der Identität (§ 2 Z 1 E-GovG) des Genehmigenden und der Authentizität (§ 2 Z 5 E-GovG)** der Erledigung treten.
- (4) Jede schriftliche **Ausfertigung** hat die Bezeichnung der Behörde, das Datum der Genehmigung und den Namen des Genehmigenden zu enthalten. **Ausfertigungen in Form von elektronischen Dokumenten müssen mit einer Amtssignatur (§ 19 E-GovG) versehen sein**; Ausfertigungen in Form von **Ausdrucken von mit einer Amtssignatur versehenen elektronischen Dokumenten oder von Kopien solcher Ausdrucke brauchen keine weiteren Voraussetzungen** zu erfüllen. Sonstige Ausfertigungen haben die Unterschrift des Genehmigenden zu enthalten; an die Stelle dieser Unterschrift kann die Beglaubigung der Kanzlei treten, dass die Ausfertigung mit der Erledigung übereinstimmt und die Erledigung gemäß Abs. 3 genehmigt worden ist. Das Nähere über die Beglaubigung wird durch Verordnung geregelt.

Genehmigung der Erledigung

- Schriftliche Erledigungen sind vom Genehmigenden mit seiner Unterschrift zu genehmigen (§ 18 Abs. 3 AVG)

- Bei elektronischen Erledigungen kann an die Stelle dieser Unterschrift ein Verfahren zum Nachweis der Identität
(§ 2 Z 1 E-GovG) des Genehmigenden und der Authentizität (§ 2 Z 5 E-GovG) der Erledigung treten

Kann durch eine (qualifizierte) elektronische Signatur (auch Amtssignatur) oder durch ein Rechte- und Rollenkonzept im elektronischen Aktenverwaltungssystem erfüllt werden

AVG

- Ausfertigungen gem. § 18 Abs. 4 AVG
- Ausfertigung in elektronischer Form:
  - Amtssignatur ist zwingend erforderlich
- Ausfertigung in schriftlicher (nicht-elektronischer) Form:
  - auf einem Dokument zu basieren, das amtssigniert wurde oder
  - Unterschrift vom Genehmigenden oder
  - Beglaubigung durch die Kanzlei

Zusammenfassung

- mindestens „fortgeschrittene“ Signatur
- auch in Privatwirtschaftsverwaltung
- Vereinfachung der Darstellung
- erleichterte Prüfbarkeit – „Verifizierung“
- Auch Ausdruck hat Beweiskraft einer öffentlichen Urkunde (§ 292 ZPO)
- Amtssignatur auf elektronischen Ausfertigungen seit 1.1.2011 zwingend erforderlich

Agenda Teil 2

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens: EU (eIDAS-VO) und national (SVG/SVV)
5. Verfahrensrechtliche Anforderungen, Amtssignatur
6. Weitere „Vertrauensdienste“ – insbes. nach der „neuen“ eIDAS-VO
7. Elektronische Signatur und Identitätsmanagement
8. Von der „Bürgerkarte“ und der „Handy-Signatur“ zur „Identity Austria“
9. EU-eID – „Wallet“ und aktuelle Entwicklungen

Zur Erinnerung: eIDAS1-VO vs eIDAS2-VO Wesentliche Neuerungen auf einen Blick:

Vertrauensdienste

- **Einführung neuer Vertrauensdienste**
  - **elektronische Attributsbescheinigungen** (El. attestations of attributes/ „EAA“)
  - **elektronische Journale** (Electronic ledgers)
  - **Verwaltung elektronischer Fernsignatur- und Fernsiegelerstellungseinheiten**
  - **elektronische Archivierungsdienste**
- Neue Regeln für **Website-Authentifizierung**
- Angleichung an **NIS 2 -Regime**

eID

- **Verpflichtung** für alle MS, eine **eID auszustellen**
- **„Europäische Brieftasche für die Digitale Identität“ („Wallet“)** als neuer zwingender Bestandteil in allen MS
- Obligatorische gegenseitige Anerkennung dieser eIDs in allen Mitgliedstaaten – **Anerkennungsverpflichtungen auch** für (große) Player im **Wirtschaftssektor** (Zwei-Faktor-Auth. KYC/ Online Plattformen)

Elektronische Attributsbescheinigungen (EAA)

- „**Attribut**“: ein Merkmal, eine Qualität, ein Recht oder die Erlaubnis einer natürlichen oder juristischen Person oder eines Objekts.
- „**Elektronische Attributsbescheinigung**“: eine in elektronischer Form vorliegende Bescheinigung, die die Authentifizierung von Attributen ermöglicht.
- „**Qual. el. EAA**“: EAA von qual. VDA ausgestellt und erfüllt Anhang V.
- „**Von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellte** elektronische Attributsbescheinigung“: eine EAA, die gemäß Artikel 45f und Anhang VII von einer öffentlichen Stelle, die für eine authentische Quelle zuständig ist, oder von einer öffentlichen Stelle, die von dem Mitgliedstaat dafür benannt wurde, solche Attributsbescheinigungen im Namen der öffentlichen Stellen, die für authentische Quellen zuständig sind, auszustellen, ausgestellt wurde.

Rechtswirkungen von EAA

- Qual. EAA und EAA, die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden: „**dieselbe Rechtswirkung wie rechtmäßig ausgestellte Bescheinigungen in Papierform**“ – in allen MS.
- EK erlässt DfRA (innerhalb von 6 Monaten nach Inkrafttreten der VO)
- MS müssen dann innerhalb von 24 Monaten sicherstellen, dass die Attribute des Anhangs VI anhand der authentischen Quellen überprüft werden können:
  - Adresse, Alter, Geschlecht, Personenstand, Familienzusammensetzung, Staatsangehörigkeit oder Staatsbürgerschaft, Bildungsabschlüsse, Titel und Erlaubnisse, Berufsqualifikationen, Titel und Berechtigungen, Vollmachten und Mandate, eine natürliche oder juristische Person zu vertreten, behördliche Genehmigungen und Lizenzen, für juristische Personen Finanzdaten und Unternehmensdaten.

EAA die von oder im Namen einer für eine authentische Quelle zuständigen öffentlichen Stelle ausgestellt werden

- Gesonderte Bestimmung (Art. 45f) und eigener Anhang VII für die Anforderungen.
- Verwendung eines qual. Zertifikats für die Signatur/ das Siegel der öff Stelle (mit spezifischem Attribut).
- Anforderungen an die ausstellende öff. Stelle vergleichbar jenen der qual. VDA.
- **Hintergrund**: Architekturentscheidung der MS, auch ohne Dazwischentreten eines qual. VDA die authentischen Registerdaten mit derselben Wirkung zu bescheinigen (und zB in die Wallet auszustellen).

Sicherheit/ Datenschutz bei EAA

- Strikte Trennung der personenbez. Daten der EAA von den anderen personenbez. Daten beim Anbieter der EAA.
- Kein „Kombinieren“
- Logische Trennung bei Speicherung
- Funktionale Trennung der Dienste

El. Archivierungsdienste

- **Definition**: ein Dienst für die Entgegennahme, die Speicherung, den Abruf und die Löschung elektronischer Daten und elektronischer Dokumente, der ihre Dauerhaftigkeit und Lesbarkeit gewährleistet sowie ihre Unversehrtheit, Vertraulichkeit und den Nachweis ihrer Herkunft während des gesamten Bewahrungszeitraums erhält.
- **Rechtswirkung**: Für Daten und Dokumente , die mit qual. Archivierungsdienst aufbewahrt werden: Vermutung der Unversehrtheit und der Richtigkeit der Herkunftsangabe für den Zeitraum der Bewahrung durch den qualifizierten Vertrauensdiensteanbieter.
- DfRA innerhalb von 12 Monaten.

El. Journale

- **Definition**: eine Abfolge von Aufzeichnungen elektronischer Daten, die die Unversehrtheit dieser Aufzeichnungen und die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.
- **Rechtswirkung**: Für Datensätze in einem qualifizierten elektronischen Journal gilt die Vermutung der eindeutigen und genauen fortlaufenden chronologischen Reihenfolge und der Unversehrtheit.
- DfRA innerhalb von 12 Monaten.

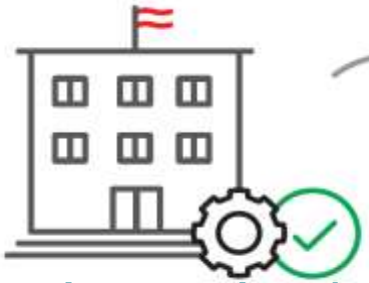
„Aufregerthema“ Website-Authentifizierung

- Verpflichtung für Anbieter von Webbrowsern, qual. Zertifikate für die Website-Authentifizierung anzuerkennen und die bescheinigten Daten und Attribute „benutzerfreundlich“ darzustellen.
- Ausnahme für KMU.
- Aber: Art. 45a Abs. 2: „ …in Fällen begründeter Bedenken hinsichtlich Sicherheitsverletzungen oder eines Integritätsverlusts eines bestimmten Zertifikats oder eines Satzes von Zertifikaten, können Anbieter von Webbrowsern Vorsorgemaßnahmen in Bezug auf dieses Zertifikat oder diesen Satz von Zertifikaten ergreifen.“ – Mitteilungspflicht gegenüber EK, Aufsichtsstelle und VDA – Prüfung durch Aufsichtsstelle. Und: ausführlicher EG (65) dazu.

Agenda Teil 2

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens: EU (eIDAS-VO) und national (SVG/SVV)
5. Verfahrensrechtliche Anforderungen, Amtssignatur
6. Weitere „Vertrauensdienste“ – insbes. nach der „neuen“ eIDAS-VO
7. Elektronische Signatur und Identitätsmanagement
8. Von der „Bürgerkarte“ und der „Handy-Signatur“ zur „Identity Austria“
9. EU-eID – „Wallet“ und aktuelle Entwicklungen

Ziel: durchgängige elektronische Prozesse



Portal

z.B. Oesterreich.gv.at,
USP.gv.at,
Wien.gv.at etc.

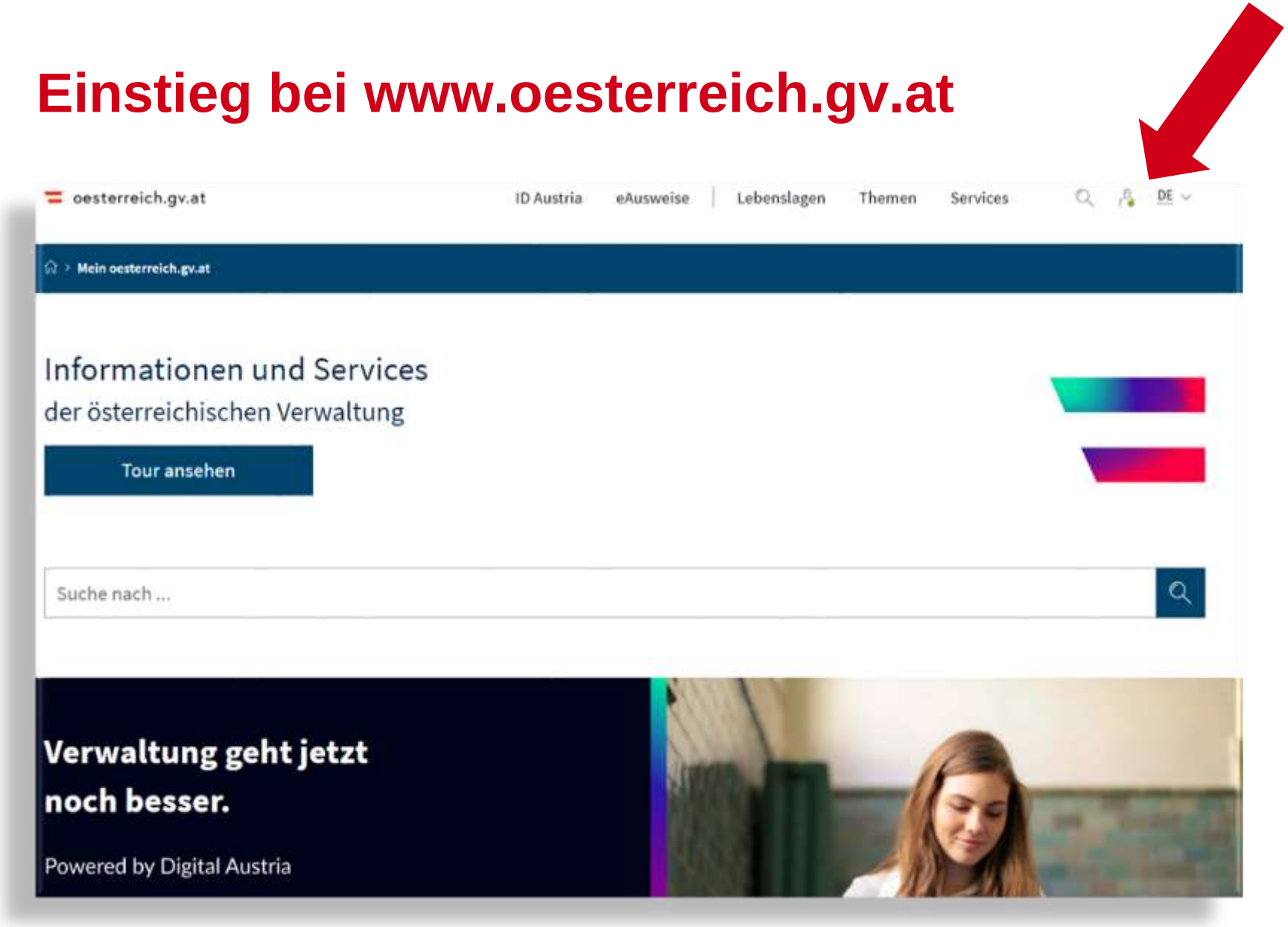
Fachanwendung/ Backoffice

z.B. ELAK, Register,
Finanz Online, etc.

Elektronische Zustellung

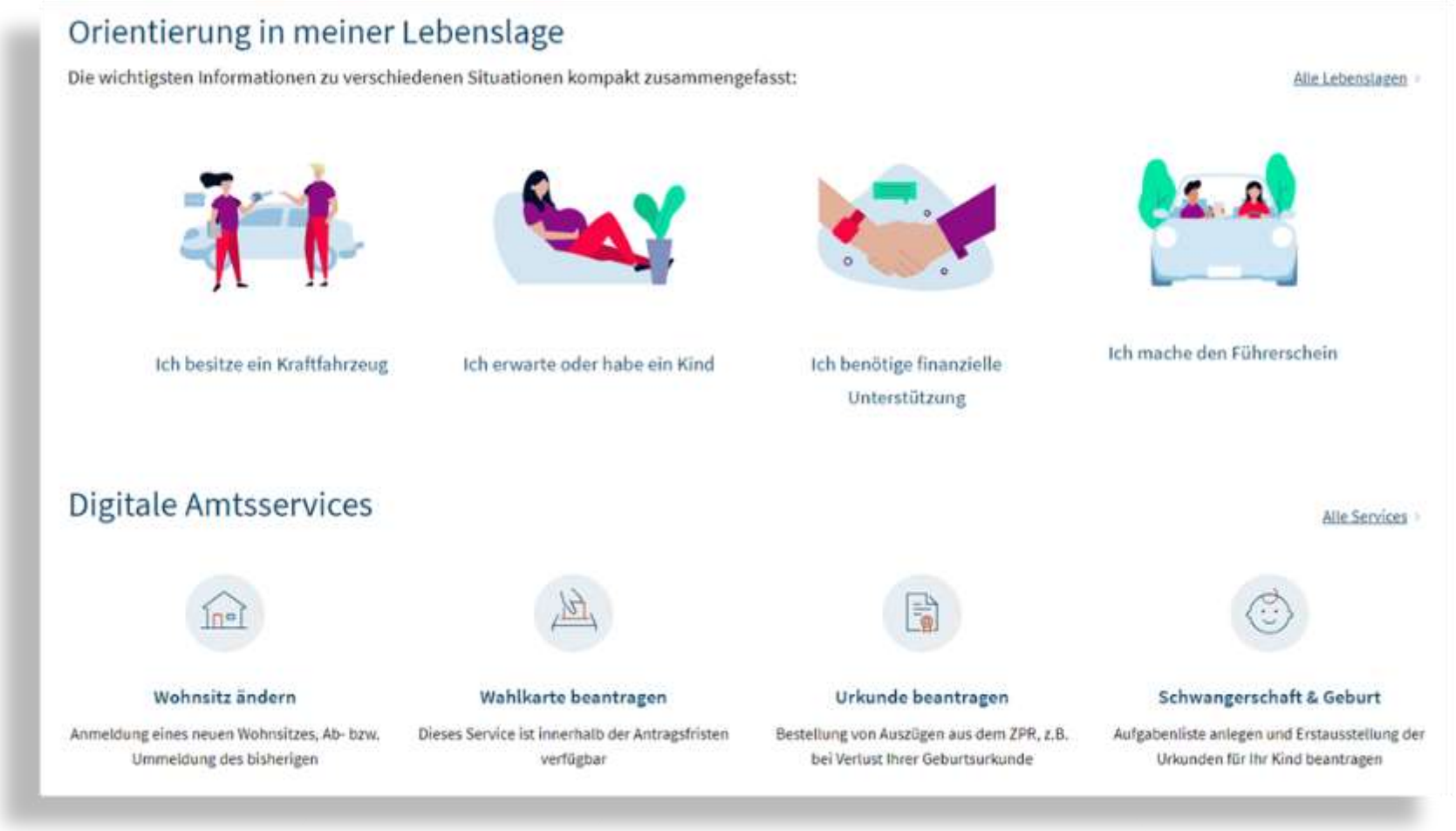
Mein Postkorb

Einstieg bei www.oesterreich.gv.at



Login mit ID Austria

Urkundenservices



Kostenlos zur Verfügung stehende Urkunden

….das Ergebnis

REPUBLIK ÖSTERREICH

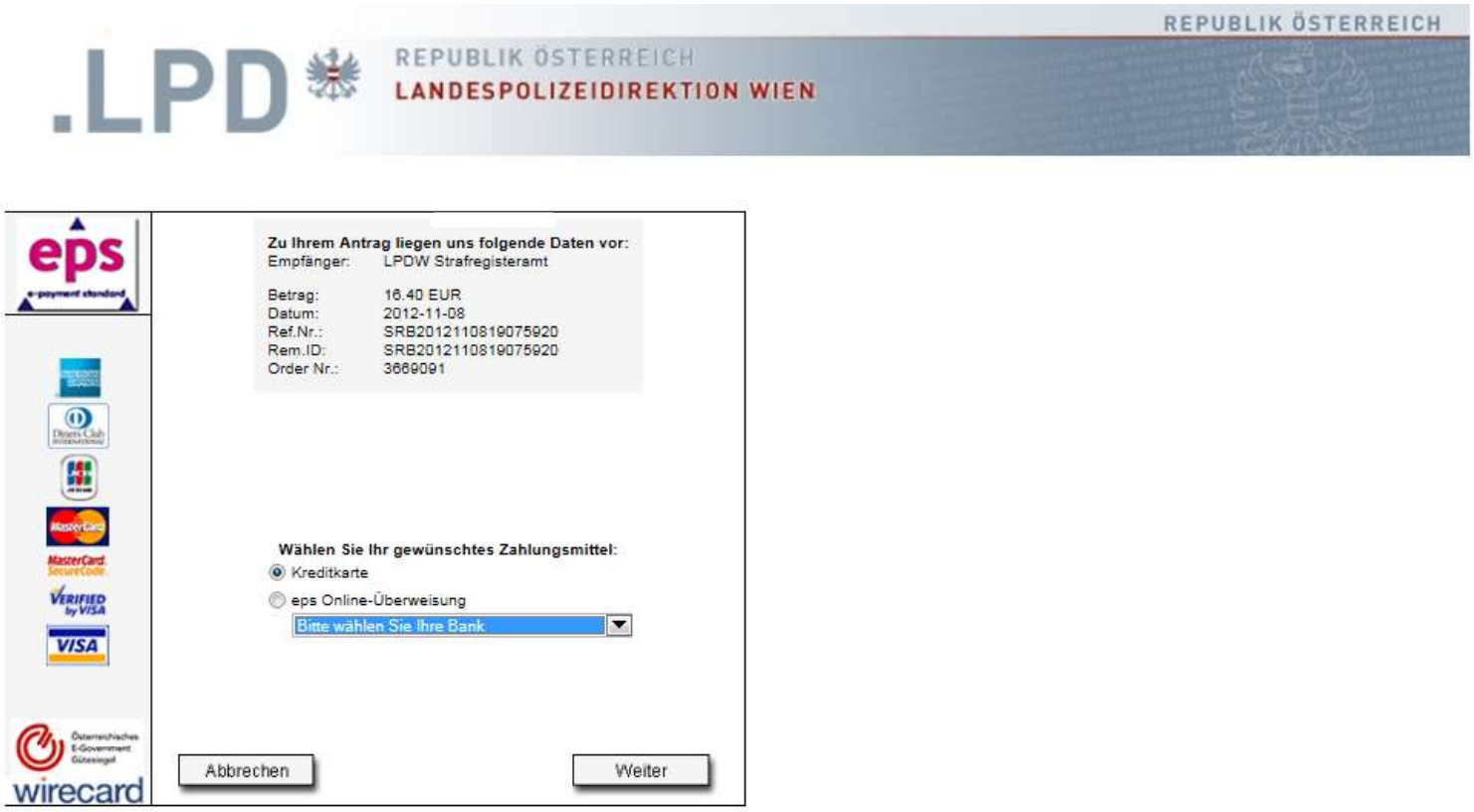
Bundesland	Wien
Behörde	BMI ZPR - Clearingstelle
Zahl	021085/2024

Teilauszug gemäß § 58 PStG 2013
über die Geburt

Familiennamen	Kustor
Akademische Grade/ Standesbezeichnungen	Mag.iur.
Vorname	Peter Michael
Sonstige Namen	—
Geburtsnamen	—
Geschlecht	männlich
Zeitpunkt und Ort der Geburt	[redacted] Wien
Mutter/Elternteil (Familiennamen, Vornamen, Datum u. Ort der Geburt)	Kust[redacted]4, Wien
Vater/Elternteil (Familiennamen, Vornamen, Datum u. Ort der Geburt)	Kustor [redacted], Wien
Datum der Ausstellung	10.05.2024

Datum/Zeit	2024-05-10T10:31:50+02:00
Aussteller-Zertifikat	a-sign-corporate-07
Serien-Nr.	1423925363
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.
Hinweis	Dieses Dokument wurde amtssigniert.

Beispiel Strafregisterbescheinigung – asynchron mit Gebühren…



Abschluss der Antragstellung

.LPD

REPUBLIK ÖSTERREICH
LANDESPOLIZEIDIREKTION WIEN

REPUBLIK ÖSTERREICH

Zeichenerklärung

* Feld muss aufgefüllt sein. Hinweis auf Fehler. Information und Hilfe zum Ausfüllen. Zutreffendes ankreuzen oder auswählen.

Sehr geehrter Herr Mag. iur. Peter Michael Kustor ,

Ihr Antrag mit der Nummer SRB2012112609000324 wurde registriert.

Sollten Sie Fragen zu Ihrem Antrag haben, so wenden Sie sich bitte an die Landspolizeidirektion Wien, Strafregisteramt: e-Mail: (LPD-W-SVA-FB-Strafregisteramt@polizei.gv.at) bzw. telefonisch unter 01/31310/79231 (Mo-Fr 07:30 - 15:30).

Ihre Landespolizeidirektion Wien
Strafregisteramt
DVR Nr. 0003506

Schließen Sie nun bitte den Browser, um ein gesichertes Logout zu ermöglichen.

Zustellverständigung

Fr. 11.03.2022 02:26

noreply_meinpostkorb@brz.gv.at

Mein Postkorb - Verständigung über die Bereithaltung eines Dokuments zur Abholung

peter.

Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

benachrichtigung_signiert.pdf
146 KB

Mein Postkorb

Sehr geehrte(r) Mein Postkorb Teilnehmer(in),

im elektronischen Postfach Mein Postkorb wurde diese E-Mail-Adresse als Verständigungsadresse beim Teilnehmer **Peter Kustor** eingegeben.

Sie haben eine neue Nachricht in Mein Postkorb unter oesterreich.gv.at erhalten. Klicken Sie hier um die Nachricht abzuholen: **https://secure.oesterreich.gv.at/at.gv.mpk-p/**

Nachrichtendetails

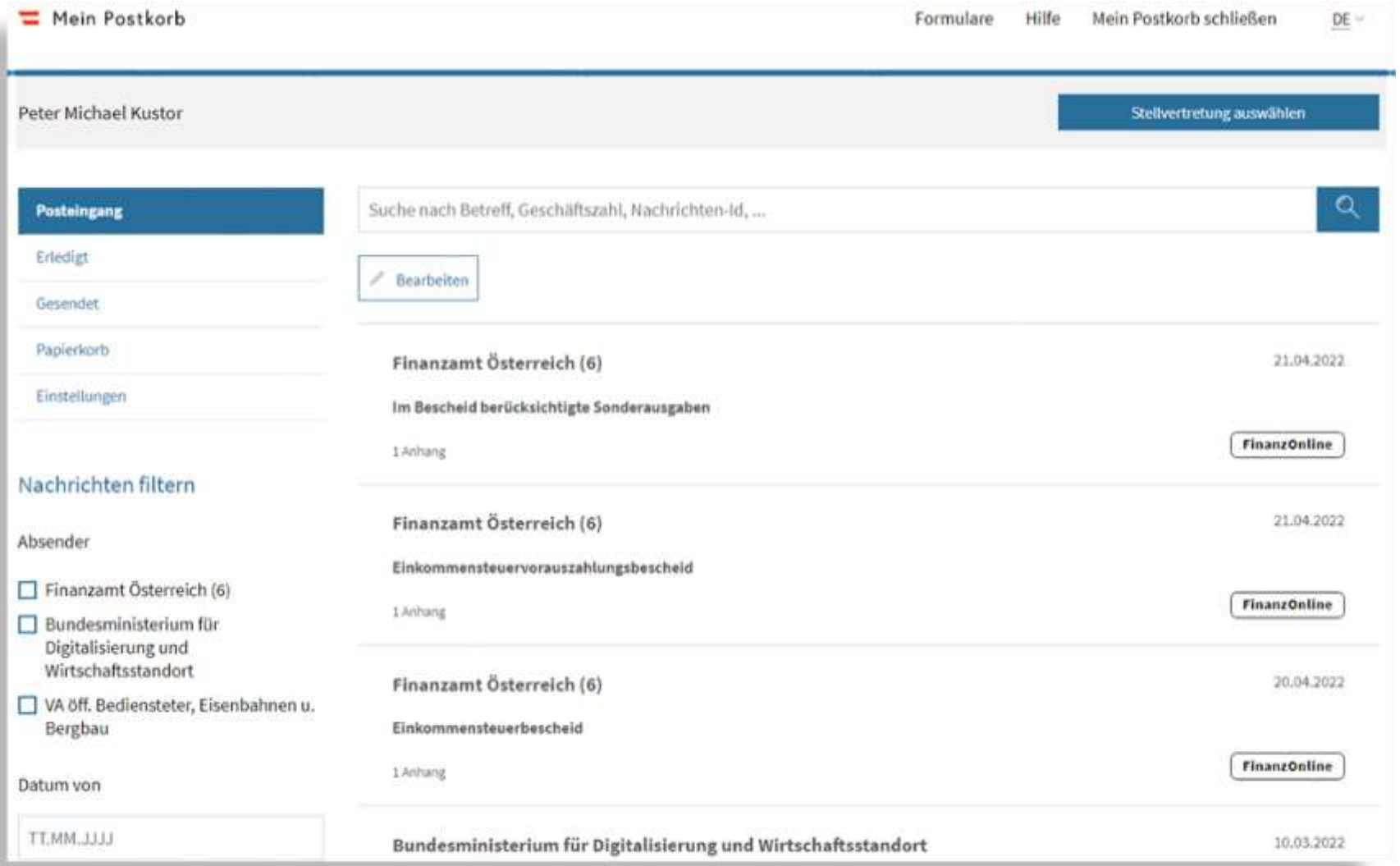
Absender
Bundesministerium

Geschäftszahl
BM-2

ID
a39e8d3d-a09d-11ec-ba9f-41d5b52c3a5c

Zustellqualität

Abholung aus „MeinPostkorb“ in oe.gv.at



Voilà…

Wien LPD SVA FB 2.2 Strafregisteramt — Gebühr entrichtet

Schottenring 7-9
1010 Wien

Geschäftszahl: (Reference Number:) SRB20170502125012652n SB

Strafregisterbescheinigung
(Criminal Record Certificate)

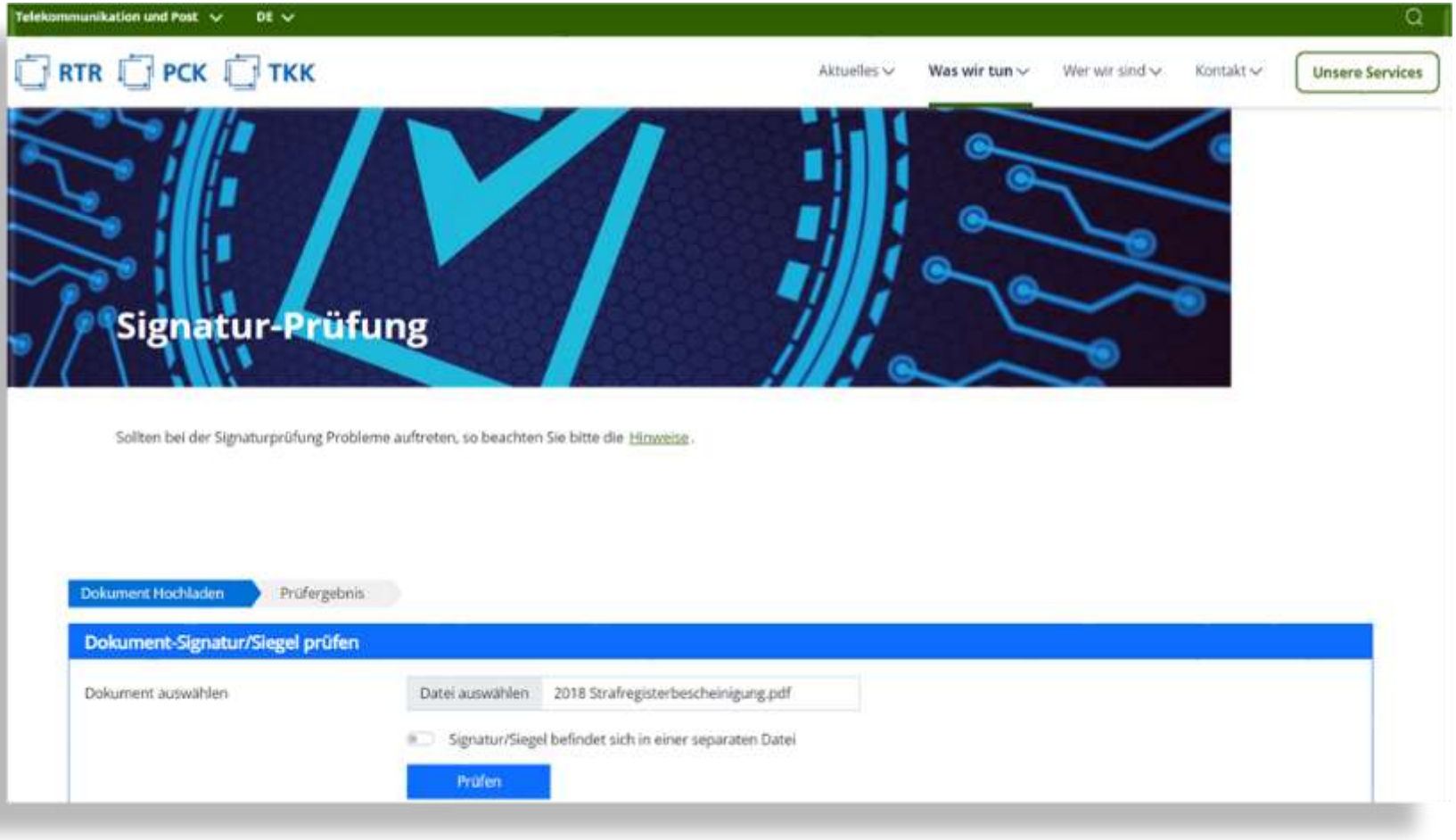
Akad. Grad vorangestellt: (Academic Degree in front of the name:)	Mag. iur.
Vorname(n): (First Name:)	Pet[redacted]
Familienname(n): (Surname:)	[redacted]
Akad. Grad nachgestellt: (Academic Degree behind the name:)	—
Geschlecht: (Gender:)	männlich male
Geburtsdatum: (Date of Birth:)	[redacted]
Geburtsort: (Place of Birth:)	Wien

Im Strafregister der Republik Österreich - geführt von der Landespolizeidirektion Wien - scheint keine Verurteilung auf.
(No convictions are listed in the criminal records database of the Republic of Austria, kept by the Federal Police Directorate of Vienna.)

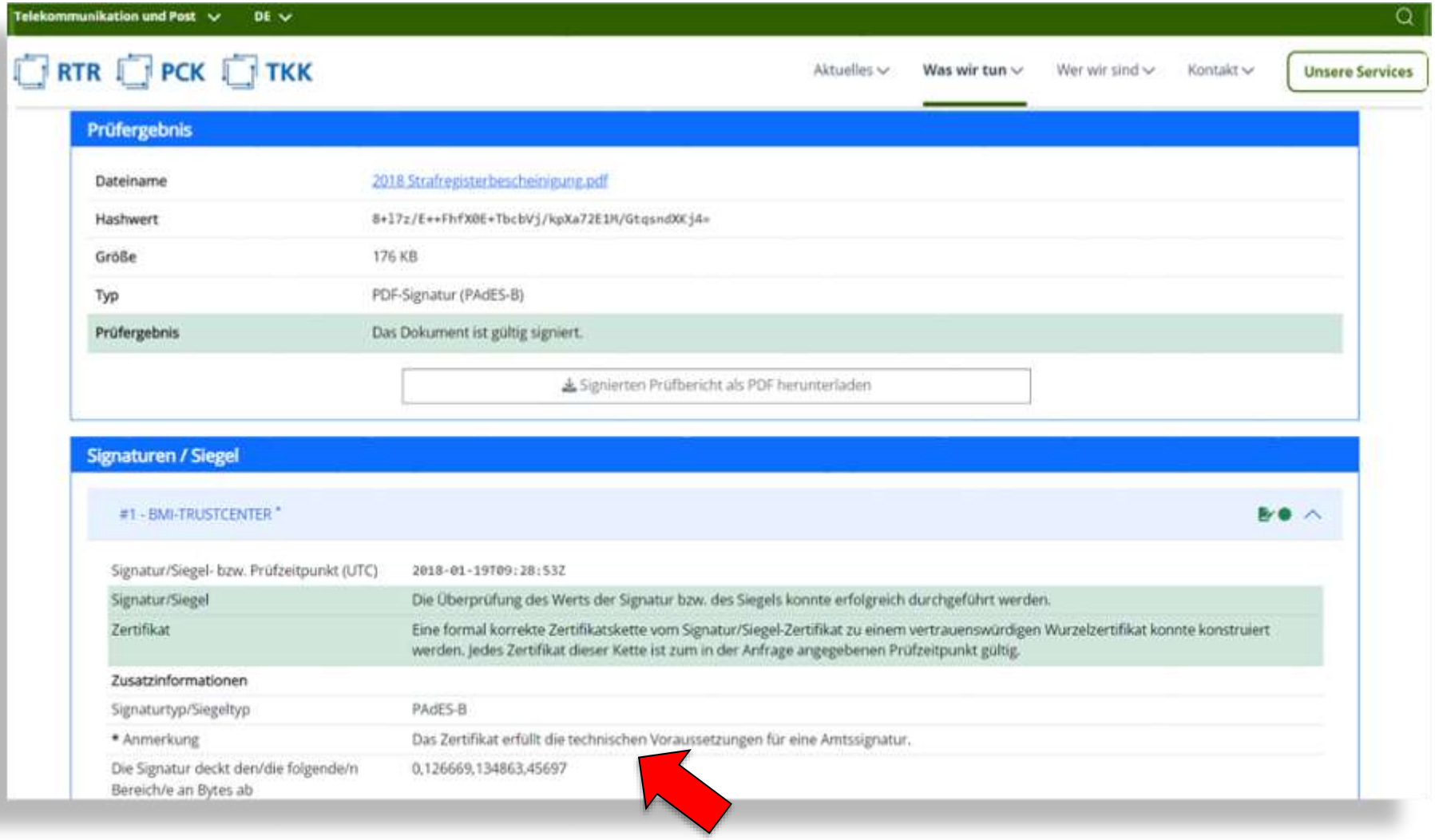
DVR: 0053506
Tagesdatum (Date)/Uhrzeit (Time): 02.05.2017/14:35:39

	Datum/Zeit	2017-05-02T14:34:54+02:00
	Aussteller-Zertifikat	e-sign-corporate-light-02
	Serien-Nr.	1624172
Prüfinformation		Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.
Hinweis		Dieses Dokument wurde amtssigniert.

Signaturprüfung



Ergebnis der Signaturprüfung



Was haben wir gesehen?

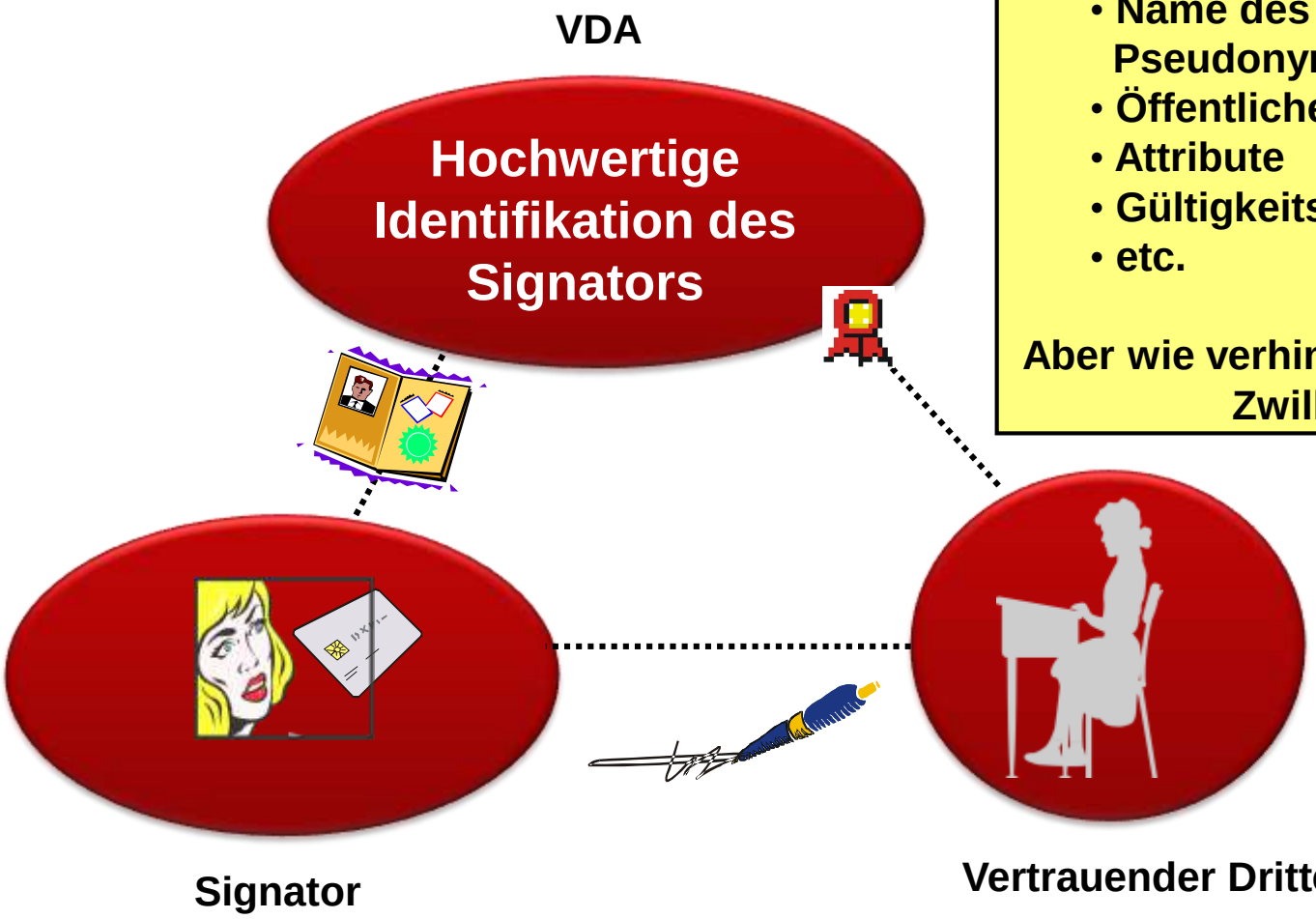
- Vollständig elektronisches Verfahren
- Komfortable „eID“-Verwendung
- Vertrauensdienste „in action“:
  - El. Signatur
  - Signaturprüfung
  - El. Zustellung
- Authentisches elektronisches Dokument mit Amtssignatur

Das “magische Dreieck” der PKI

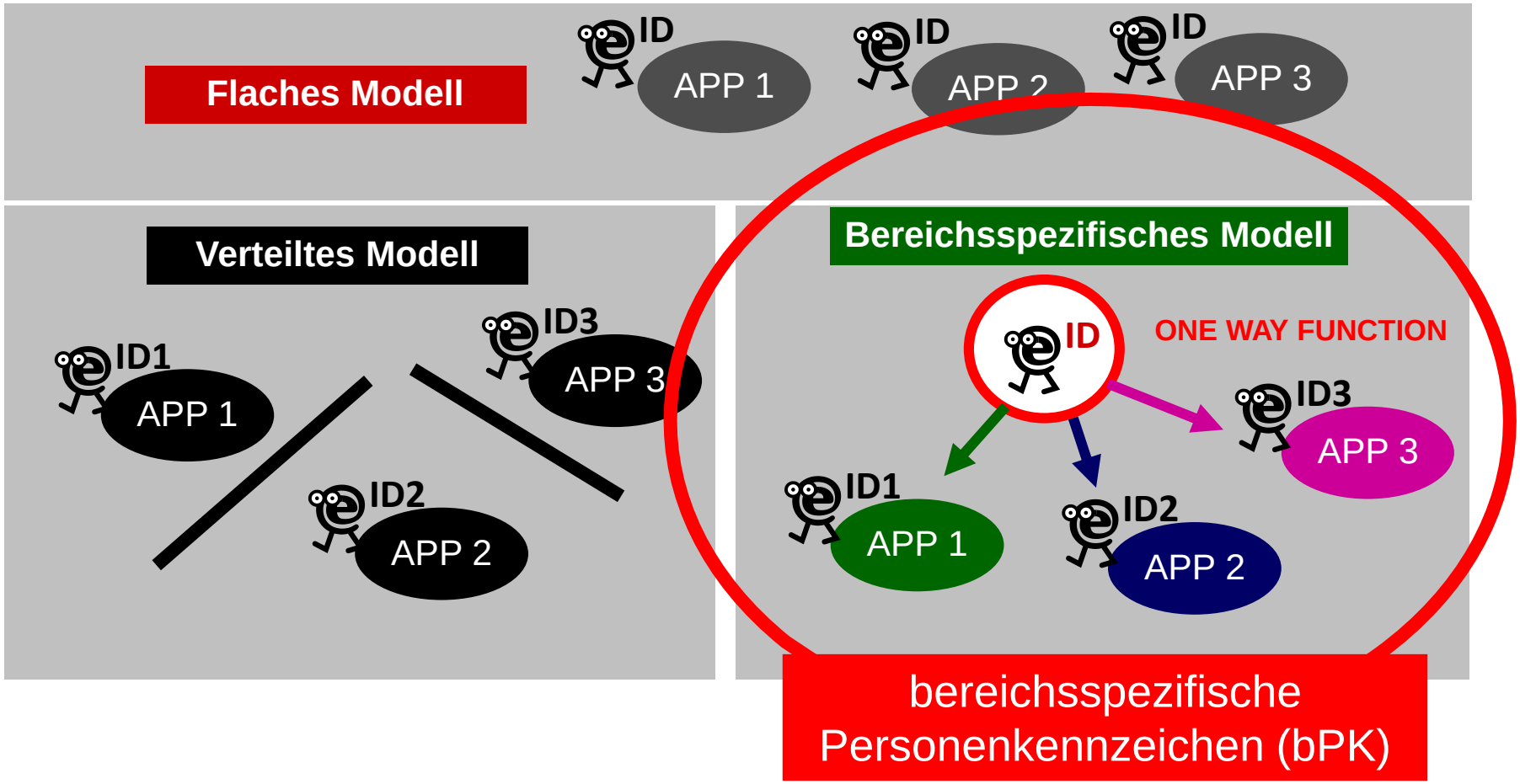
Zertifikatsdaten

- VDA
- Name des Signators oder Pseudonym
- Öffentlicher Schlüssel
- Attribute
- Gültigkeitsdauer
- etc.

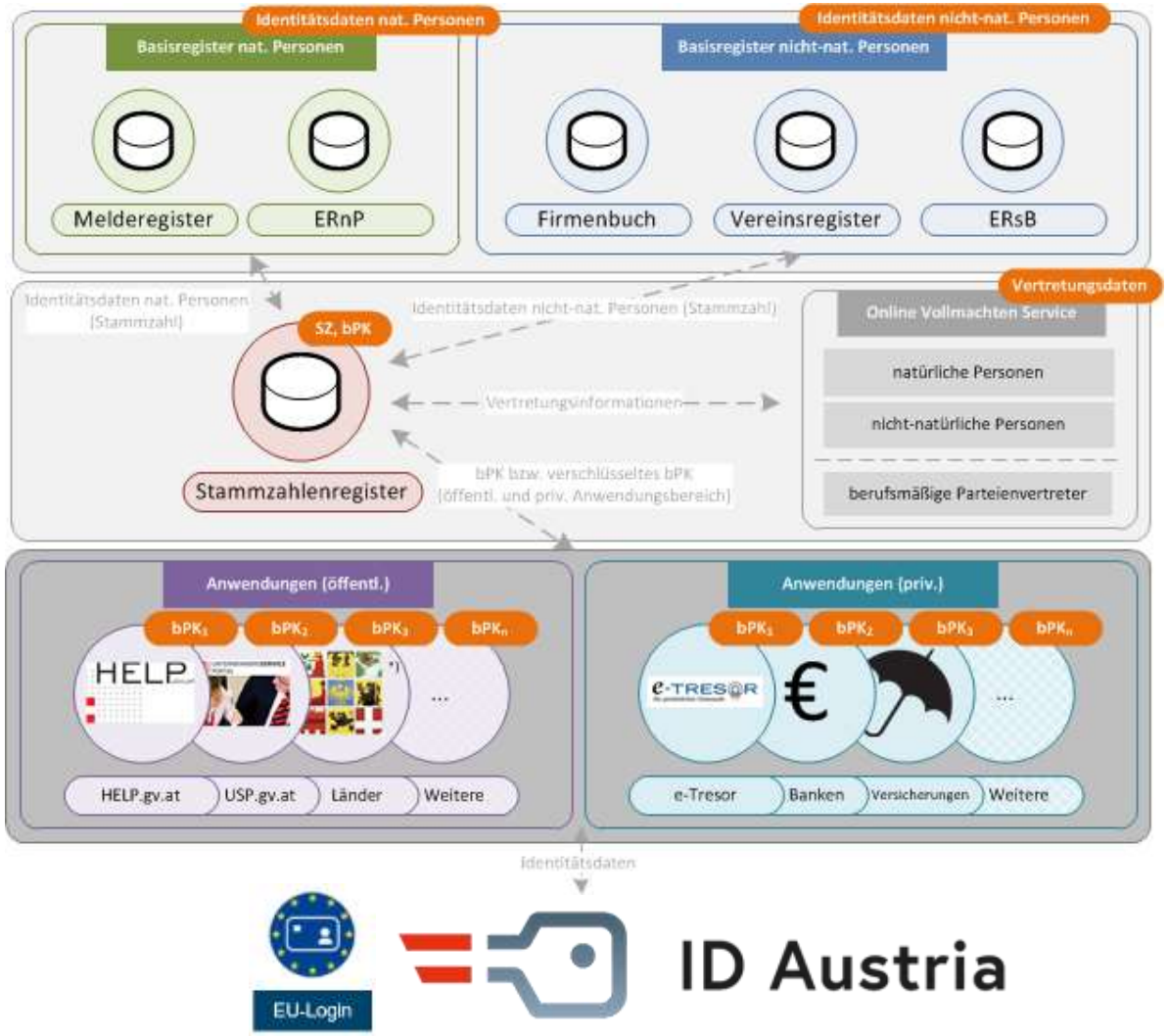
Aber wie verhindere ich digitale Zwillinge?



Identitätsmanagement - Modelle



eID – big picture



Register im Backoffice

Anwendungen

Zugang des Users

Funktionen der Bürgerkarte (§ 4 Abs. 1 E-GovG)

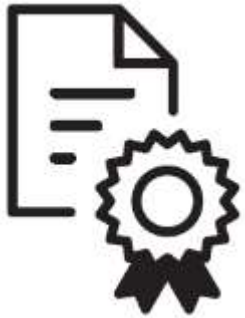
Die Bürgerkarte dient dem Nachweis

- der **eindeutigen Identität (und weiterer Merkmale)** eines Einschreiters und
- der **Authentizität** *(= Echtheit)* des elektronisch gestellten Anbringens (Rechtswirkung entspricht der Schriftlichkeit iSd § 886 ABGB)...

D.h. sie ist:

→ **E-Identitätsdokument** und

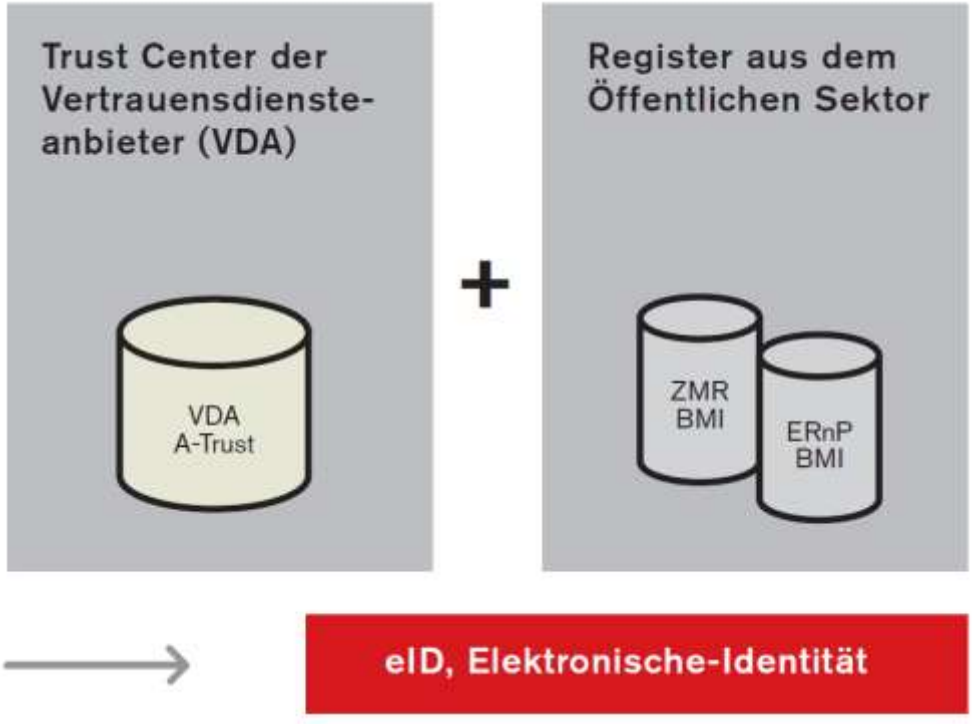
→ **Unterschrift** im Internet



Elektronische-Identität = qVDA + öffentliche Register

§ 4 Abs. 2 E-GovG:
Die eindeutige Identifikation einer natürlichen Person erfolgt mittels **Stammzahl**
(= verschlüsselte ZMR Zahl (ERnP-On))

§ 4 Abs. 4 E-GovG:
Die Authentizität des elektronisch gestellten Anbringens wird mittels **elektronischer Signatur** erbracht

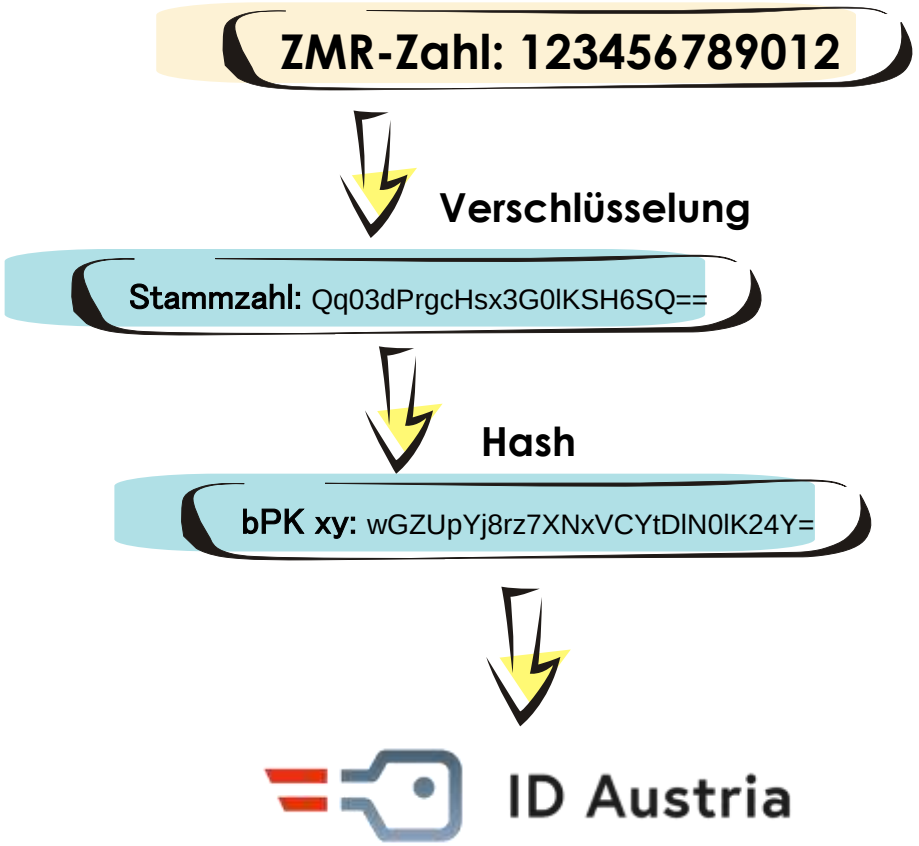


Stammzahl

- Stammzahl für Natürliche Personen:
  - gemeldete Personen: verschlüsselte ZMR-Zahl/ ERnP-On
  - Nicht meldepflichtige Personen: verschlüsselte Ergänzungsregisterzahl (ERnP)
- Stammzahl für Juristische Personen:
  - Unternehmen (inkl. natürliche Personen, die unternehmerisch tätig sind): unverschlüsselte Firmenbuchnummer oder Global Location Number (GLN)
  - Land- und forstwirtschaftliche Betriebe, Gewerbeinhaber, eGründung: unverschlüsselte Firmenbuchnummer oder Global Location Number (GLN)
  - Vereine: unverschlüsselte Vereinsregisterzahl
  - sonstige Betroffene (ausländische Unternehmen, KÖR, Stiftungen, etc.): unverschlüsselte Ergänzungsregisterzahl (ERsB)

Stammzahl (SZ) nat. Personen: Erzeugung (§ 6 Abs. 2 E-GovG)

- Verschlüsselte ZMR-Zahl/ ERnP-On
- Stammzahlregisterbehörde errechnet die Stammzahl
- Stammzahlregisterbehörde speichert die SZ NICHT (Virtuelles Register)
- darf nur verwendet werden zur Berechnung von **bereichsspezifischen Personenkennzeichen (bPK)**



Schutz der Stammzahl gem. § 12 E-GovG

- Darf nur zur **bPK-Berechnung** verwendet werden
  - Errechnungsvorgang nur bei der SZRB bzw. im BMI (Auftragsverarbeiter)
- **Keine Speicherung** außerhalb des Errechnungsvorgangs! (§ 12 E-GovG)
- 2 Varianten der bPK Berechnung
  - Mit Mitwirkung der Betroffenen (= E-ID Verwendung)
  - Ohne Mitwirkung der Betroffenen (= bPK “Ausstattung”)

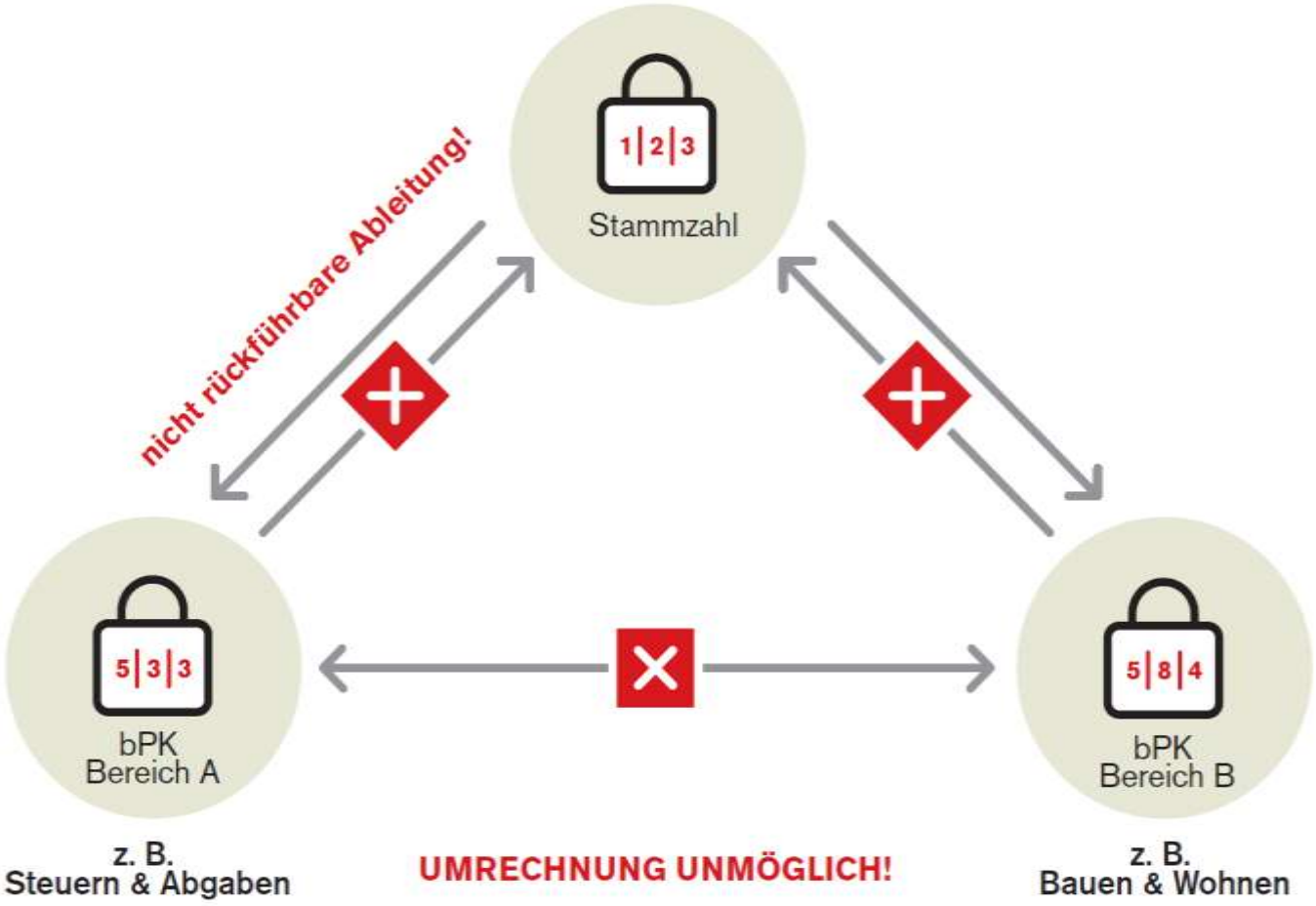
bPK – Bereiche (1/2)

- Jede Datenverarbeitung einer Stelle, die mit bPK ausgestattet werden soll, darf nur **einem Bereich** zugeordnet werden.
- Die Tätigkeitsbereiche der staatlichen Verwaltung wurden mit der **E-Government-Bereichsabgrenzungsverordnung** festgelegt.
- Kann eine Datenverarbeitung keinem der genannten Bereiche eindeutig zugeordnet werden, können auch **Sub-Bereiche** geschaffen werden, z.B.: bPK ZP-MH für oe.gv.at oder bPK BF-FO für Registerforschung
- Das bPK eines anderen Bereichs darf in nur als **verschlüsseltes** „bPK“ gespeichert werden.

bPK-Bereiche (2/2)

- Identifikationsfunktion der bPK ist auf jenen staatlichen Tätigkeitsbereich beschränkt, dem die Datenverarbeitung zuzurechnen ist, in der das bPK verarbeitet werden soll.
- Zurechnung einer Datenverarbeitung zu einem bestimmten staatlichen Tätigkeitsbereich ergibt sich aus ihrer Registrierung bei der Stammzahlenregisterbehörde.
- Die Abgrenzung der staatlichen Tätigkeitsbereiche ist für Zwecke der Bildung von bPK so vorzunehmen, dass zusammengehörige Lebenssachverhalte in ein- und demselben Bereich zusammengefasst werden und miteinander unvereinbare Datenverarbeitungen innerhalb desselben Bereichs nicht vorgesehen sind

bPK: Erzeugung



E-Government
BereichsabgrenzungsVO

Tätigkeitsbereich	Bereichskennung
Arbeit	AR
Amtliche Statistik	AS
Bildung und Forschung	BF
Bauen und Wohnen	BW
EU und Auswärtige Angelegenheiten	EA
Ein- und Ausfuhr	EF
Gesundheit	GH
Gesellschaft und Soziales	GS
Restitution	GS-RE
Justiz/Zivilrechtswesen	JR
Kultus	KL
Kunst und Kultur	KU
Land- und Forstwirtschaft	LF
Landesverteidigung	LV
Rundfunk und sonstige Medien sowie Telekommunikation	RT
Steuern und Abgaben	SA
Sport und Freizeit	SF
Sicherheit und Ordnung	SO
Vereinsregister	SO-VR
Strafregister	SR-RG
Sozialversicherung	SV
Umwelt	UW
Verkehr und Technik	VT
Vermögensverwaltung	VV
Wirtschaft	WT
Personenidentität und Bürgerrechte (zur Person)	ZP

bPK: Erzeugung (1/2)

- grundsätzlich: nur mit E-ID des Betroffenen!
  - nötig für bPK-Erzeugung: ID Austria

- **für Behörden** (§10 Abs. 2 E-GovG):
  - Anfrage an SZ-RegBehörde möglich („**Ausstattungsantrag**“)
  - Input: ausreichend identifizierende Merkmale (Name, Geb.datum, Anschrift...) & gewünschter (eigener) Bereich
  - Output: bPK für gewünschten (eigenen) Bereich

- Das bPK eines anderen Bereichs darf in den Datenanwendungen nur als verschlüsseltes „bPK“ gespeichert werden.

bPK: Erzeugung (2/2)

- **für Private** (§14 Abs. 1 und 2 E-GovG):
  - Anfrage an SZRB möglich („**Ausstattungsantrag“**)
    - Input: ausreichend identifizierende Merkmale (Name, Geb.datum, Anschrift...) & eigene Stammzahl bzw. bPK als Bereichskennung
    - Output: bPK für den privaten Bereich (für bestimmtes Unternehmen)
- Einschränkungen in § 15 E-GovG

- Das bPK eines öffentlichen Bereichs darf in den privaten Datenanwendungen nur als verschlüsseltes „bPK“ gespeichert werden (§ 6 StZRegBehV) sofern nicht gesetzliche Ausnahme geschaffen wurde.

bPK: Berechnung - Suchparameter

- Um einen Treffer bei der ZMR und ERnP Suche zu erzielen ist es erforderlich, dass die Suchdaten den Daten aus den beiden Registern gleichen. Weiters ist für diese Suche immer der Vorname, Nachname und ein weiteres Merkmal erforderlich. Ein weiteres Merkmal kann eines oder mehrere aus folgender Liste sein:
- Geburtsdatum
- Geschlecht
- Geburtsort
- Staatsangehörigkeit
- Anschrift (bzw. Einzelteile davon, wie etwa die Postleitzahl)

bPK: Berechnung - Zusammenfassung

- Um eine bPK zu berechnen, wird eine **Anfrage an das SZR** übermittelt, welche mit den angegebenen Suchdaten eine Suche im ZMR und im ERnP durchführt.
- Führt diese Suche zu einem **eindeutigen Ergebnis**, wird aus der ZMR-Zahl, respektive der Ordnungsnummer im ERnP von dieser Person die Stammzahl mittels kryptografischer Verfahren berechnet und daraus das bPK für den angefragten Bereich abgeleitet.
- Werden **verschlüsselte bPK** angefordert, werden diese in einem zusätzlichen Schritt mittels des Schlüssels (ist im SZR hinterlegt) des Empfängers der vbPK verschlüsselt, dieser hat bei sich das erforderliche Schlüsselmaterial, um die vbPK wiederum zu entschlüsseln zu können.

Registerzählung

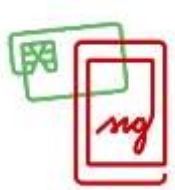
- bPk sind kein „Orchideenthema“, sondern weit verbreitet: Allein im Jahr 2023 wurden 1.45 Mrd. bPK oder verschlüsselten bPK errechnet!
  (2022: 836 Mio, 2021: 498 Mio, 2020: 411 Mio, 2019: 358 Mio, 2018: 341 Mio)

- Das bPK-Konzept ermöglichte den Ersatz der Volkszählung durch die Registerzählung!
- Weitere „große“ neuere Verwendungen:
  - Banken
  - Spenden für automatische Arbeitnehmerveranlagung
  - Registerforschung

- Das ö. bPK-System gilt seit vielen Jahren als „privacy by design“-System

eID: „Bürgerkartenkonzept“/ Handy-Signatur/ ID Austria

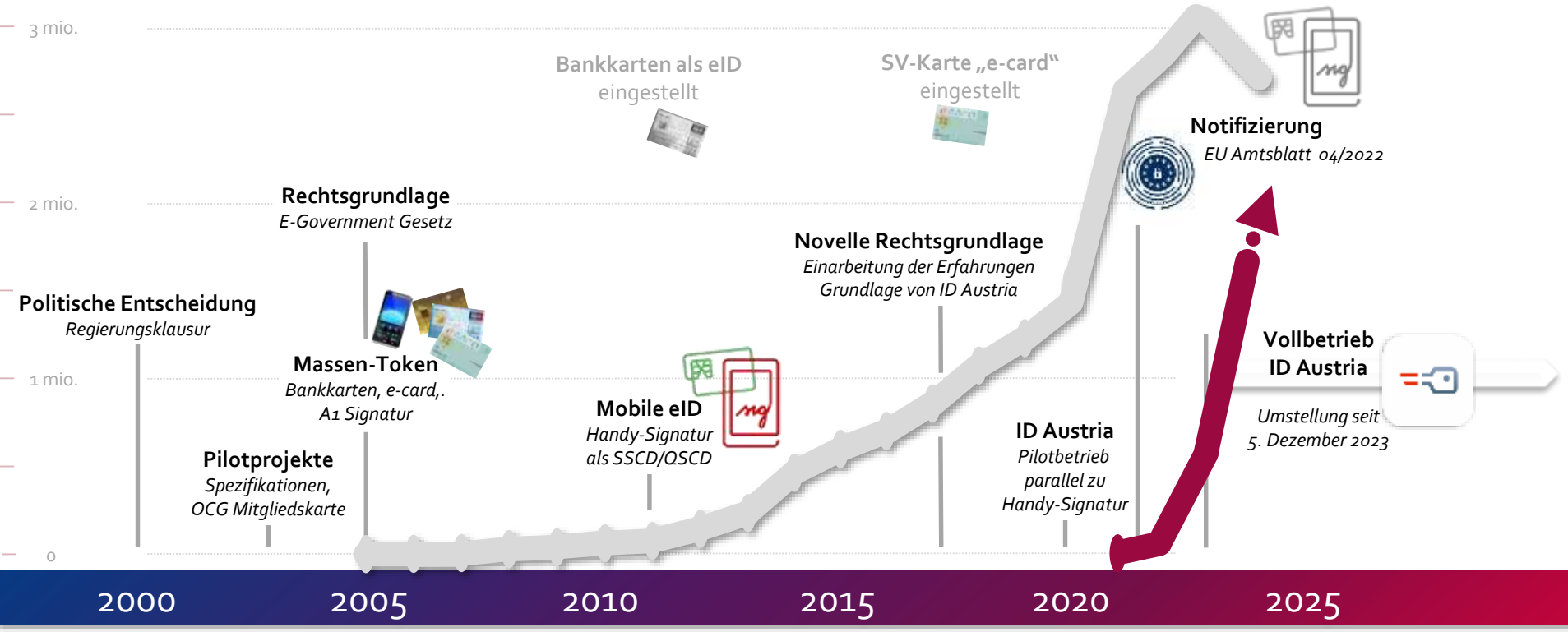
- **Freiwillige und kostenlose „eID“ wurde 2005 eingeführt**
  - Definiert Funktion, nicht Technologien
  - Qualifizierte elektronische Signatur
  - Elektronische Vertretung, Vollmacht
- **Nutzung für Verwaltung und Privatwirtschaft**
  - 350+ Anwendungen
- **Von Beginn verschiedene Träger**
  - Chipkarte: Bank, e-card (Krankenv.), Dienstausweis
  - Mobil: A1 Signatur (bis 2008), Handy-Signatur



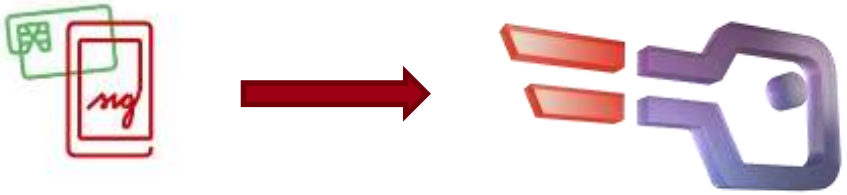
- Aus „Bürgerkarte“ wurde der **„E-ID“ („Identity Austria“)** - zunächst in Pilotierung, „Vollbetrieb“ seit 5.12.2023 - Schwerpunkt mobil

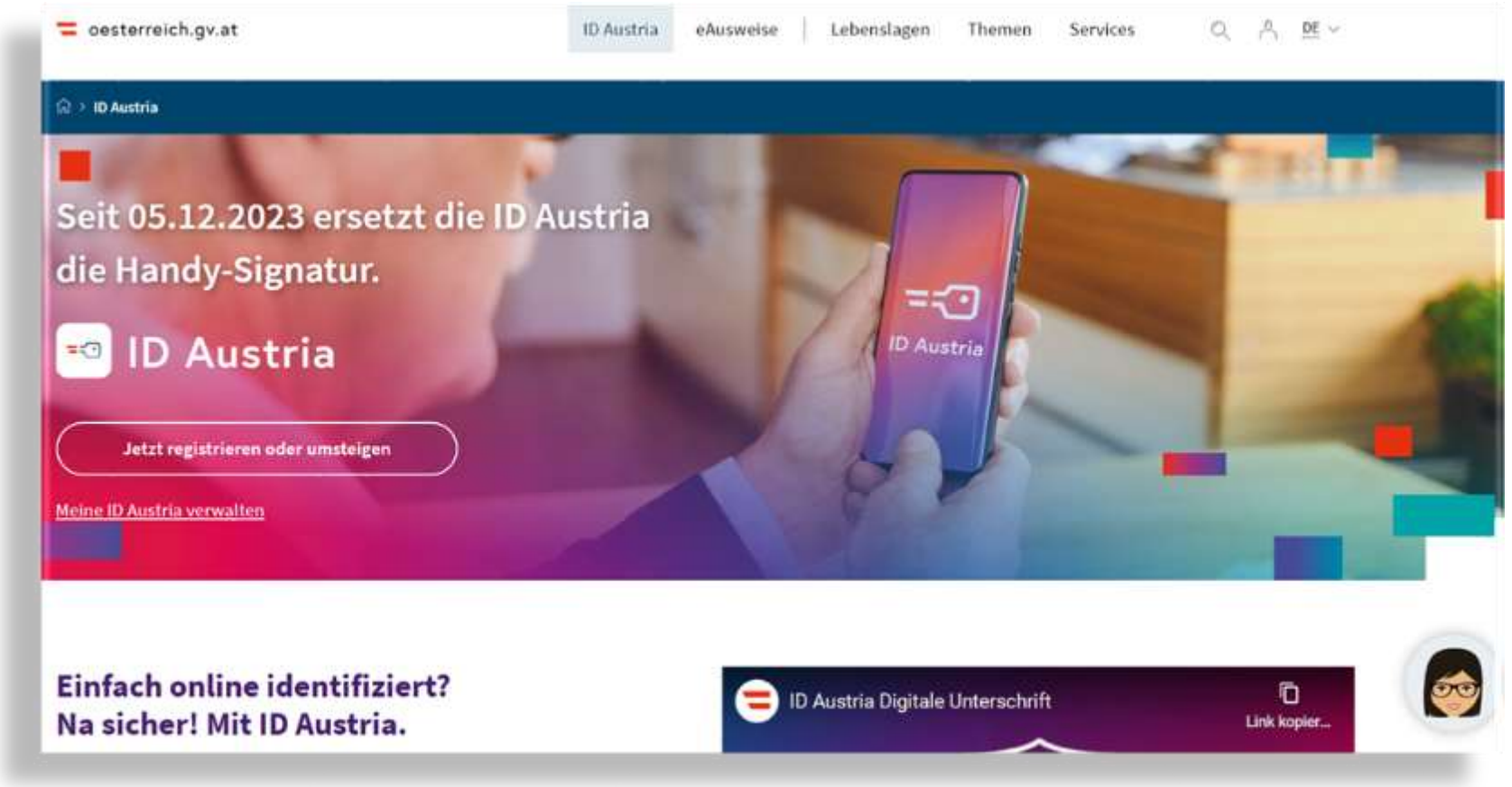
ID Austria

Entwicklung eID in Österreich



Aktuelle Entwicklung





ID Austria – Die konsequente Weiterentwicklung

- Handy-Signatur basierend auf dem Bürgerkartenkonzept war eine gute Ausgangslage, es bedurfte aber einer Weiterentwicklung ….
  …. daher die ID Austria
- EU-weite Anerkennung nach eIDAS Verordnung als einziges nationales elektronisches Identitätssystem in Österreich
  - auf Sicherheitsniveau „hoch“.
- Die APP „Digitales Amt“ ist die Basis der mobilen ID Austria
- Services innerhalb der APP aber auch APP2APP
- Qualifizierte el. Signatur ist fixer Bestandteil
- **Behördliche Registrierung – automatisch am Passamt**
- **Grundlage für „digitalen Führerschein“ und weitere el. „Ausweise“**

Eine ID Austria - endlose Anwendungen

Für digitale öffentliche Services.
Für wirtschaftlichen Erfolg.
Für alle Lebenslagen.

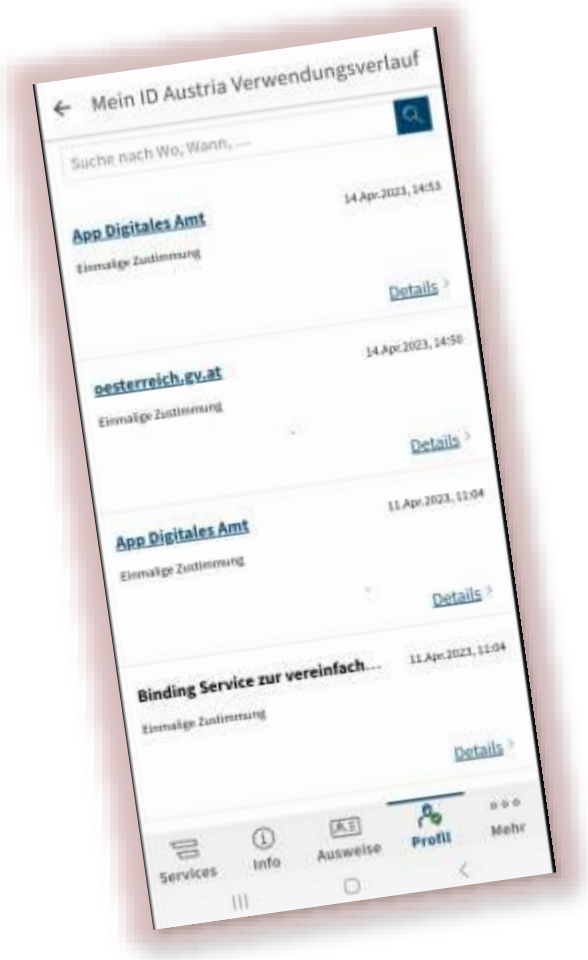
Voraussetzungen für die Nutzung der ID Austria

- → Vollendetes 14. Lebensjahr
- → Registrierung bei einer Registrierungsbehörde (insbes. Passamt, Landespolizeidirektion, Finanzamt)
- → Smartphone und Installation der App „Digitales Amt“ (bzw. A-Trust SignaturApp - mit eingeschränkten Funktionen) oder
  - → Signaturkarte (QSCD) bzw.
  - → FIDO2-Level2-Sicherheitsschlüssel

Smartphone

- Android: Betriebssystemversion Android 8 oder höher.
- iOS: Sie benötigen die Betriebssystemversion iOS 12.1 oder höher.
- App als apk-File bereitgestellt für User, die z.B. Graphene als Betriebssystem benutzen

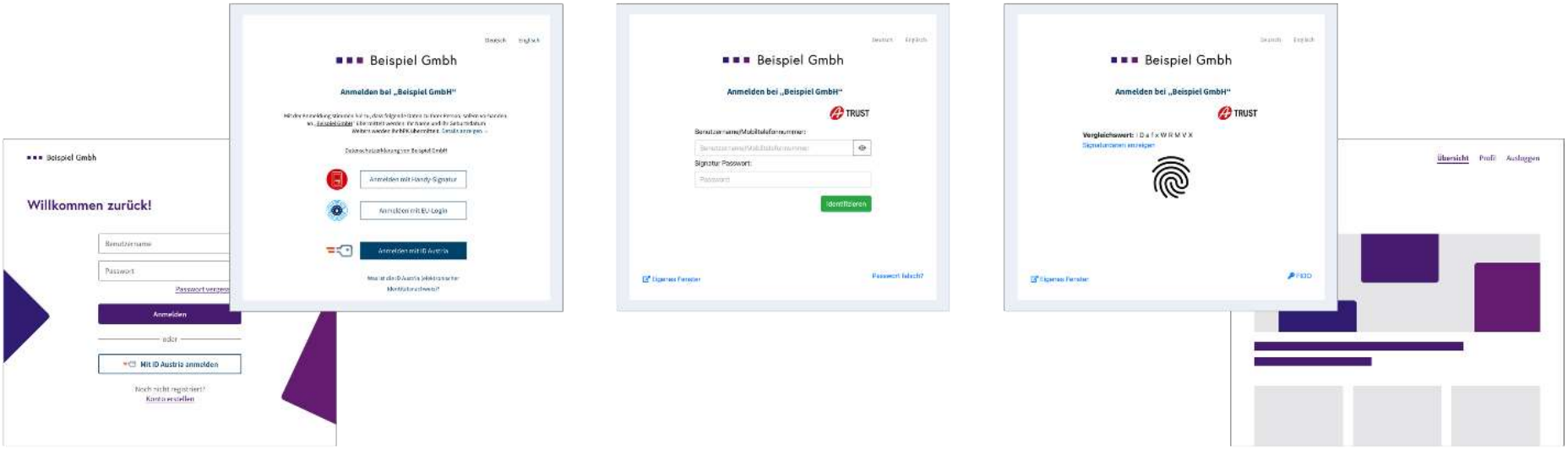
Rahmenbedingungen der ID Austria – User in control



- Datenhoheit der Bürger:innen
- Transparenz der Nutzung (Nachvollziehbarkeit der Verwendung für die Bürger:innen/Nutzer:innen)
- Selbstbestimmung
  - Wo und wann nutze ich die ID Austria und welche Daten will ich an wen weitergeben
  - Sichere Nutzung von Services im Internet (z. B. durch Zweifaktor-Identifizierung)

Ablauf der Anmeldung mit ID Austria im Web

Nutzer*in initiiert bei Service Provider die Anmeldung → Anmeldung über ID Austria und Einverständnis zur Datenverarbeitung wird aufgerufen → Nutzer*in meldet sich mit Benutzername und Passwort an → Nutzer*in bestätigt Anmeldung mit zweitem Faktor (z.B. App „Digitales Amt" oder FIDO-Sicherheitsschlüssel) → Nutzer*in ist bei Service Provider angemeldet

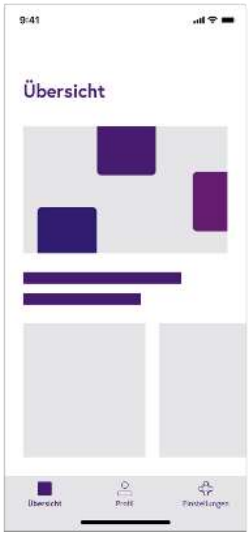


Ablauf der Anmeldung mit ID Austria am Smartphone

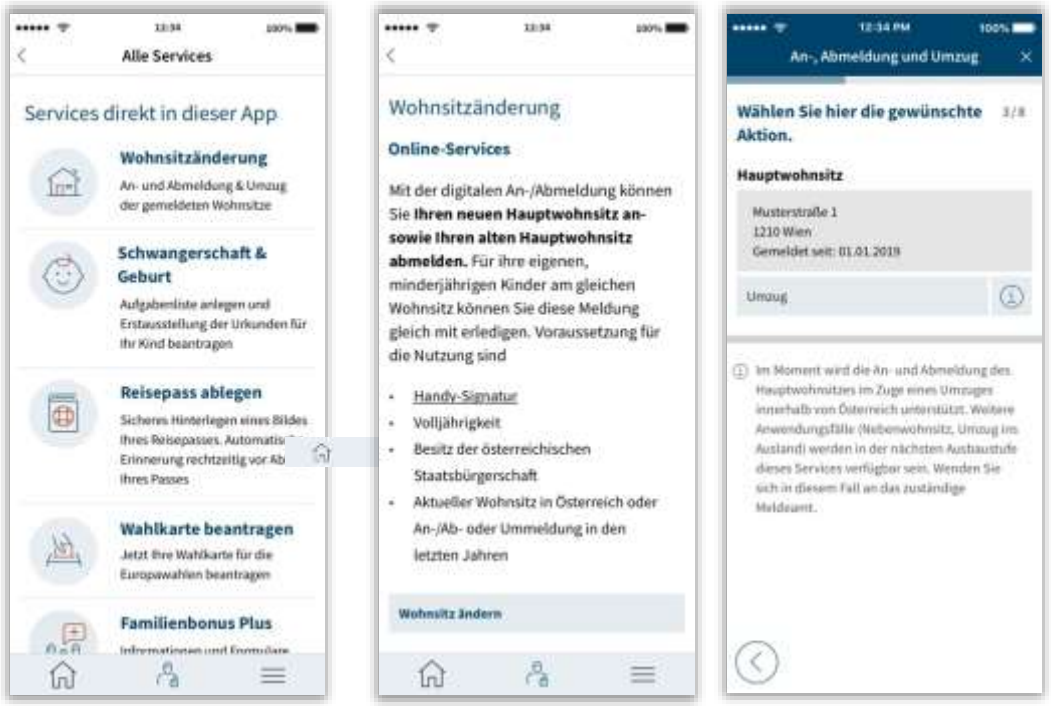
Nutzer*in initiiert in App oder auf Website des Service Providers die Anmeldung mit ID Austria

App „Digitales Amt“ öffnet sich.
Nutzer*in ist dort bereits angemeldet, gibt Einverständnis zur Verarbeitung der ID Austria Daten und bestätigt dies via Biometrie

Nutzer*in wird zur App oder Website des Service Providers zurückgeleitet und ist dort angemeldet



Beispiel: Wohnsitzänderung mobil

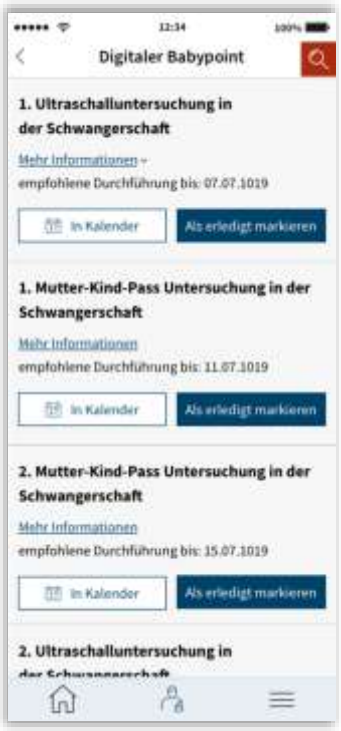


- Einbindung des Zentralen Melde-registers und des Adressregisters
- Abmeldung des bisherigen und Anmeldung neuen Wohnsitzes
- Bestätigung nach Abschluss

Reisepass Erinnerungsservice

- Verbunden mit Identitätsdokumenten-Register
- Erinnerung sechs Monate vor Ablauf
- Sichere Ablage

Digitaler Baby-Point



- Antrag Ausstellung
  - Geburtsurkunde
  - Staatsbürgerschafts-nachweis
  - Meldung des Kindes am Wohnsitz eines Elternteils
  - Zustellung der e-Card
- Persönliche Checklist um Schwangerschaft und Geburt, Termine

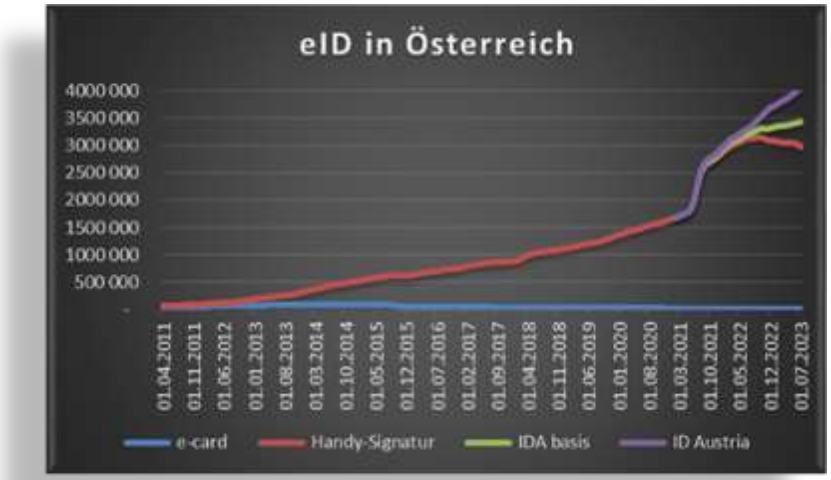
Aktueller Stand der ID Austria

→ Rd. 3.8 Mio User:innen haben eine „Handy-Signatur“ bzw. die ID Austria. (2,5 Mio. davon eine ID Austria, davon 1,65 Mio. mit vollen IDA-Attributen (Stand April 2024)).

→ Rd. 3 Mio. User:innen der App „Digitales Amt“.

→ Aktuell nutzen rd. 80 private und rd. 440 öffentliche Serviceprovider das IDA-Produktivsystem. Zu den aktiven Serviceprovider zählen Unternehmen und Organisationen aus den Branchen Versicherungen, Telekommunikation, Logistik (z.B. Post-App), Gesundheit (z.B. ELGA-Portal, SV-Portal, PV) und Verwaltung (z.B. Unternehmensserviceportal, eAMA-Portal).

→ IDA-Testsystem, mit dzt. 165 privaten und 181 öffentlichen Serviceprovidern.



ID Austria

Sichere digitale Identität für die
Anmeldung an Online-Services
und mobilen Apps

eAusweise

Sichere digitale Ausweise für den
Nachweis gegenüber Personen
und Geräten

eAusweise - die Ausweisplattform

- EINE Plattform für Ihre Ausweise
- Persönliches Ausweis-Wallet via App “eAusweise”
- Daten analoger staatlicher Ausweise digital am Smartphone verfügbar
- Aktuell verfügbare digitale Ausweise:
  - Digitaler Führerschein
  - Digitaler Altersnachweis
  - Digitaler Zulassungsschein

Digitale Aus-/Nachweise & eAusweise

Digitale Aus-/Nachweise:

- Ein digitaler Aus-/Nachweis ist ein kryptographisch signiertes Set von Attributen (bspw. einer Person)
- Diese Daten werden verschlüsselt in einer App auf einem Mobilgerät gespeichert
- Digitale Aus-/Nachweise müssen immer auch über einen elektronischen Prozess geprüft werden, **eine reine Verwendung als Sichtausweis ist nicht vorgesehen!**

eAusweise App:

- Für die Bürger:innen steht die App „eAusweise“ für digitale Aus-/Nachweise der Verwaltung zur Verfügung
- Die App „eAusweise” basiert auf der digitalen Identität der ID Austria
- Digitale Aus-/Nachweise können von anderen Bürger:innen, Unternehmen oder Organen der Verwaltung (z.B. Polizei) überprüft werden

Gesetzliche Grundlage eAusweise:

§ 4 Abs. 6 E-GovG:

(6) Nach Maßgabe der technischen Möglichkeiten kann der E-ID-Inhaber **Vorname, Familienname, Geburtsdatum und den Bestand weiterer Merkmale gemäß Abs. 5 letzter Satz einem Dritten gegenüber in vereinfachter Form nachweisen**. Zu diesem Zweck können Vorname, Familienname, Geburtsdatum und die weiteren Merkmale für einen begrenzten Zeitraum **zu seinem E-ID gespeichert** werden. Vorname, Familienname, Geburtsdatum dürfen für längstens drei Monate gespeichert werden. Ob und für welchen Zeitraum dies für ein bestimmtes weiteres Merkmal zulässig ist, hat jener Verantwortliche des öffentlichen Bereichs festzulegen, der das Register führt, aus dem die Stammzahlenregisterbehörde dieses Merkmal bezogen hat.

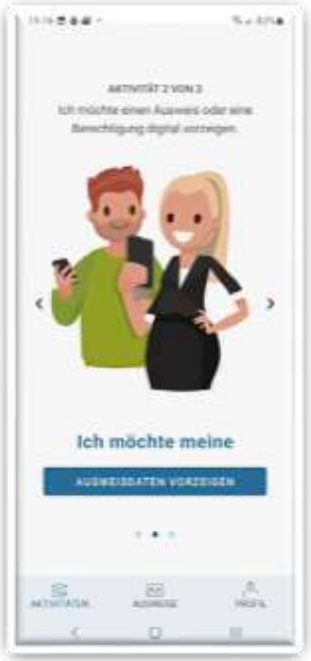
VO-Ebene: § 4 StZRegBehV 2022

(1) Die Speicherung von Merkmalen zum E-ID zum Zweck deren vereinfachten Nachweises gemäß § 4 Abs. 6 E-GovG ist nur auf Grund einer Anforderung des E-ID-Inhabers bei der Stammzahlenregisterbehörde unter Verwendung dessen E-ID zulässig. Diese Anforderung ist zu protokollieren.

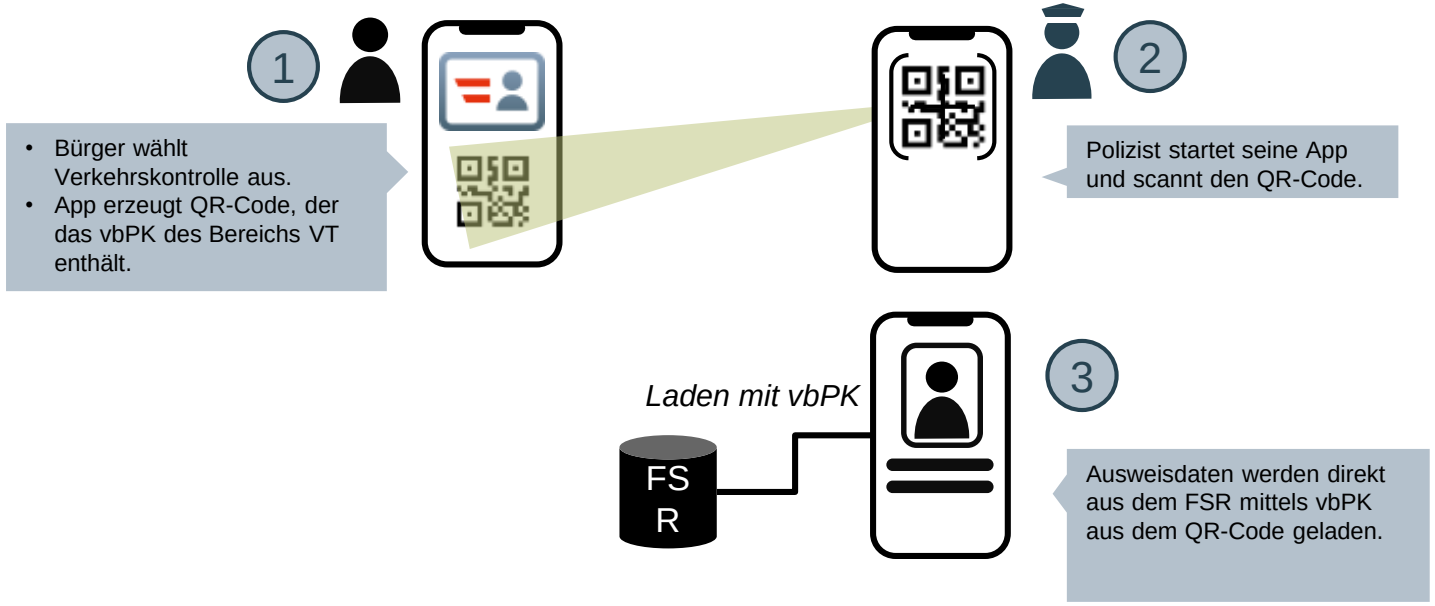
(2) Nach Maßgabe der technischen Möglichkeiten kann der E-ID-Inhaber die nach Abs. 1 gespeicherten Merkmale einem Dritten ohne Erstellung einer Personenbindung in einer der Verwendung des E-ID sicherheitstechnisch gleichwertigen Weise übermitteln.

(3) Die Stammzahlenregisterbehörde kann für Zwecke des Abs. 1 und 2 eine technische Plattform und die notwendigen Schnittstellen zur Verfügung stellen.

eAusweise “in Aktion”



Verkehrskontrolle mit dem digitalen Führerschein

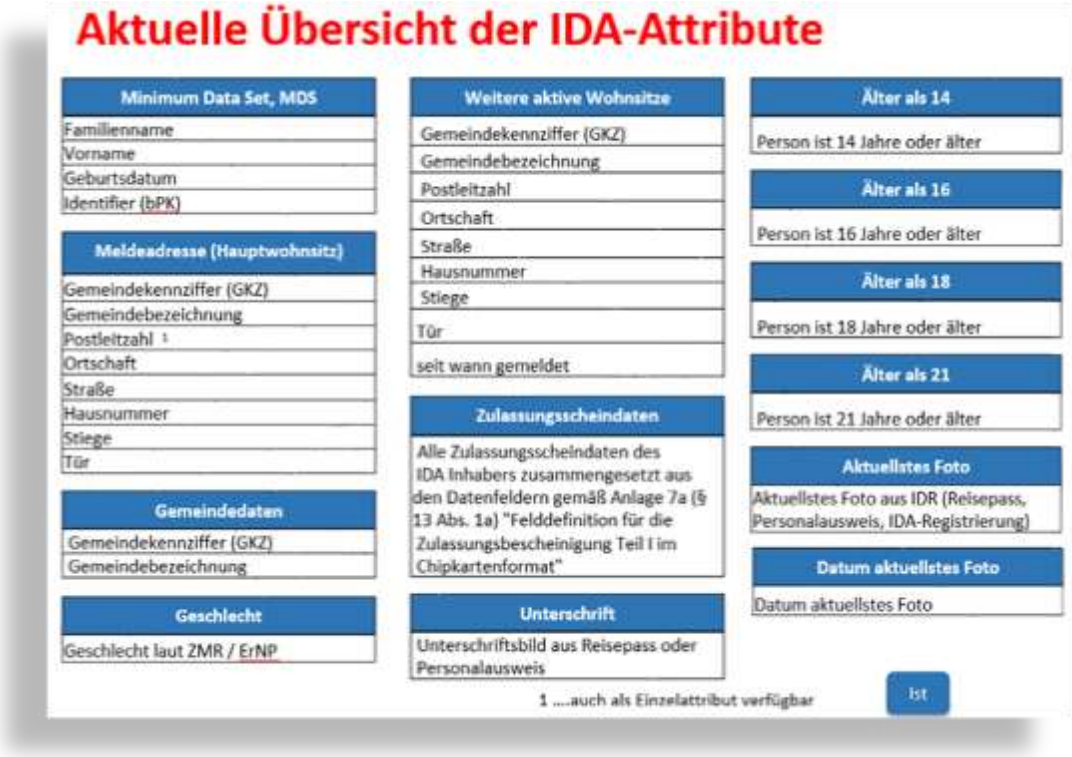


Aktueller Stand der eAusweise und Attribute (Stand April 2024)

→ Rd. 580.000 User:innen Digitaler Führerschein (seit Okt. 2022)

→ Rd. 220.000 User:innen Digitaler Altersnachweis (seit Sept. 2023)

→ Rd. 330.00 User:innen Digitaler Zulassungsschein (seit 15.2.2024)



Ausblick

- Erweiterung der Attribute (Reisepass- und Personalausweis-Attribute)
- Einführung zusätzlicher eAusweise (digitaler Identitätsnachweis, digitaler Zulassungsschein Phase 2)
- Erweiterung der Anwendungsgebiete in der Wirtschaft (z.B. Banken, Versicherungen)

- Technische Weiterentwicklung und Integration mit EUiD-Wallet

Agenda Teil 2

1. „Unterschrift“ - „Elektronische Unterschrift“
2. Praktische Demonstration
3. Technischer Hintergrund
4. Detaillierte Darstellung des Rechtsrahmens: EU (eIDAS-VO) und national (SVG/SVV)
5. Verfahrensrechtliche Anforderungen, Amtssignatur
6. Weitere „Vertrauensdienste“ – insbes. nach der „neuen“ eIDAS-VO
7. Elektronische Signatur und Identitätsmanagement
8. Von der „Bürgerkarte“ und der „Handy-Signatur“ zur „Identity Austria“
9. EU-eID – „Wallet“ und aktuelle Entwicklungen

eID - Rahmen der eIDAS1-VO 2014 (1/2)

- Keine Harmonisierung, keine „EU-eID“, keine zentrale Datenbank etc.
- Freiwillige Notifikation des eID-Systems durch den Mitgliedstaat (MS)
- Voraussetzungen für die Notifikation
- 3 Sicherheitsniveaus:
  „Niedrig“ – „Substanziell“ – „Hoch“,
  mit Durchführungsrechtsakt definiert
- Österreich hat den „E-ID“ (weiterentwickelte Bürgerkarte (Handy-Signatur) – „Identity Austria“) mit Sicherheitsniveau „Hoch“ notifiziert

eID - Rahmen der eIDAS1-VO 2014 (2/2)

- Verpflichtende gegenseitige Anerkennung der von den anderen MS notifizierten eIDs
- Sicherheitsniveau des eID ist gleich hoch oder höher als der verlangte Level („substanziell“ oder „hoch“)
- Anerkennung des Sicherheitsniveaus „niedrig“ auf freiwilliger Basis
- Für private Services auf freiwilliger Basis und unter den Konditionen des Ausstellers

eID Sicherheitsniveaus

Eine DurchführungsVO legt die technischen Spezifikationen und Verfahren für die Sicherheitsniveaus fest. Die Anforderungen betreffen insbes.:

a) das **Verfahren zum Nachweis und zur Überprüfung der Identität** der Antragssteller;

b) das **Verfahren zur Ausstellung** der Identifizierungsmittel;

c) den **Authentifizierungsmechanismus**;

d) die **Einrichtung**, die die Identifizierungsmittel ausstellt;

e) die **technischen und sicherheitsbezogenen Anforderungen der ausgestellten elektronischen Identifizierungsmittel**.

Sehr vereinfachtes Beispiel:

Niveau „substanziell“ und „hoch“ benötigen

2-Faktor-Authentifizierung …

eID Sicherheitsniveaus - Details

Zuordnungskriterien nach der DurchführungsVO:

- Anmeldung
  - Beantragung und Eintragung
  - Identitätsnachweis und –überprüfung
  - Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen
- Verwaltung elektronischer Identifizierungsmittel
  - Merkmale und Gestaltung elektronischer Identifizierungsmittel
  - Ausstellung, Auslieferung und Aktivierung
  - Aussetzung, Widerruf und Reaktivierung
  - Verlängerung und Ersetzung
- Authentifizierung
  - Authentifizierungsmechanismus
- Management und Organisation
  - Allgemeine Bestimmungen
  - Veröffentlichte Bekanntmachungen und Benutzerinformationen
  - Informationssicherheitsmanagement
  - Aufbewahrungspflichten
  - Einrichtungen und Personal
  - Technische Kontrollen
  - Einhaltung und Prüfung

„Personenidentifizierungsdaten“ (1/2)

- Siehe die Durchführungsverordnung (EU) 2015/1501 vom 8. September 2015 über den Interoperabilitätsrahmen:
- Mindestdatensatz einer **natürlichen** Person
  - obligatorische Merkmale:
  a) derzeitige(r) Familienname(n),
  b) derzeitige(r) Vorname(n),
  c) Geburtsdatum,
  d) eine **eindeutige Kennung**, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und **möglichst dauerhaft** fortbesteht.
  - optionale Merkmale:
  a) Vorname(n) und Familienname(n) bei der Geburt,
  b) Geburtsort,
  c) derzeitige Anschrift,
  d) Geschlecht.

„Personenidentifizierungsdaten“ (2/2)

- Mindestdatensatz einer **juristischen** Person
  - obligatorische Merkmale:

  a) derzeitige amtliche Bezeichnung,

  b) eine eindeutige Kennung, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und **möglichst dauerhaft** fortbesteht.

  - optionale Merkmale:

  a) derzeitige Anschrift,

  b) Umsatzsteuer-Identifikationsnummer,

  c) Steuerregisternummer,

  d) Kennnummer in Bezug auf Artikel 3 Absatz 1 der Richtlinie 2009/101/EG des Europäischen Parlaments und des Rates,

  e) Kennziffer der juristischen Person (LEI) gemäß der Durchführungsverordnung (EU) Nr. 1247/2012 der Kommission,

  f) Registrierungs- und Identifizierungsnummer des Wirtschaftsbeteiligten (EORI-Nr.) gemäß der Durchführungsverordnung (EU) Nr. 1352/2013 der Kommission,

  g) Verbrauchsteuernummer gemäß Artikel 2 Absatz 12 der Verordnung (EU) Nr. 389/2012 des Rates.

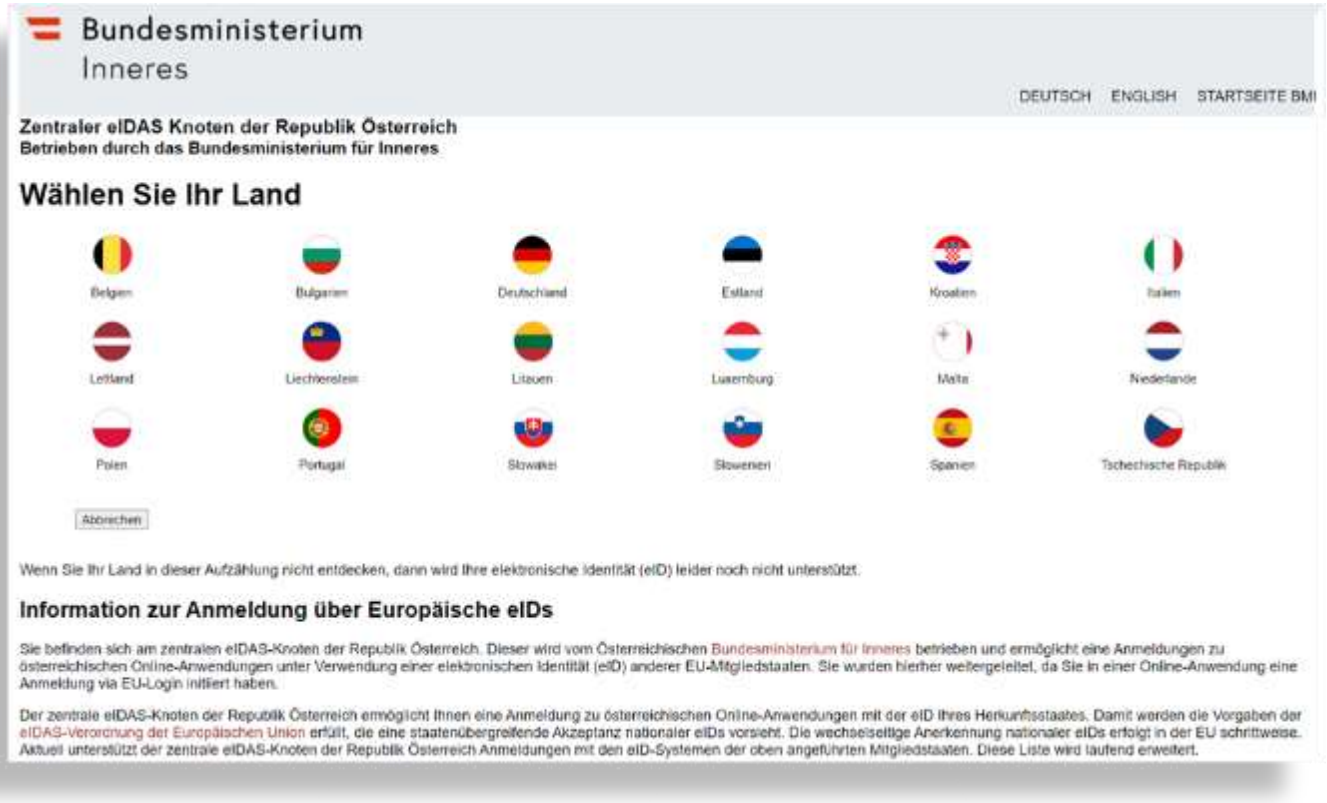
Durchführungsrechtsakte - eID

- Kooperationsmechanismus eID:
  - Durchführungsbeschluss (EU) 2015/296, ABl. Nr. L 53 vom 25.2.2015
- Interoperabilität
  - DurchführungsVO (EU) 2015/1501, Abl. Nr. L 235 vom 9.9.2015
- Sicherheitsniveaus
  - DurchführungsVO (EU) 2015/1502, Abl. Nr. L 235 vom 9.9.2015
- Notifikation
  - Durchführungsbeschluss (EU) 2015/1984, ABl. Nr. L 298 vom 5.11.2015

AT – eIDAS Notifikation und Umsetzung

- Ab Ende September 2021 lief auf EU-Expertenebene der „peer review“-Prozess zur ID Austria.
- Im Februar 2022 wurde vom „eIDAS Kooperationsnetz“ bescheinigt, dass die ID Austria den höchsten Sicherheitsanforderungen (Sicherheitsniveau „hoch“) auf EU Ebene entspricht.
- Die Notifikation wurde im April 2022 im Amtsblatt kundgemacht.
- Nach der max. 12-monatigen Übergangsfrist für die anderen MS ist nun sichergestellt, dass NutzerInnen der ID Austria diese auch für Anwendungen in ganz Europa nutzen können.

Gegenseitige Anerkennung - Notifizierungen



- bislang haben 24 MS notifiziert
- Schrittweise Abbildung in den eIDAS-Knoten
- ID Austria wurde im April 2022 notifiziert

Zur Erinnerung: eIDAS1-VO vs eIDAS2-VO Wesentliche Neuerungen auf einen Blick:

Vertrauensdienste

- **Einführung neuer Vertrauensdienste**
  - **elektronische Attributsbescheinigungen** (El. attestations of attributes/ „EAA“)
  - **elektronische Journale** (Electronic ledgers)
  - **Verwaltung elektronischer Fernsignatur- und Fernsiegelerstellungseinheiten**
  - **elektronische Archivierungsdienste**
- Neue Regeln für **Website-Authentifizierung**
- Angleichung an **NIS 2 -Regime**

eID

- **Verpflichtung** für alle MS, eine **eID auszustellen**
- **„Europäische Brieftasche für die Digitale Identität“ („Wallet“)** als neuer zwingender Bestandteil in allen MS
- Obligatorische gegenseitige Anerkennung dieser eIDs in allen Mitgliedstaaten – **Anerkennungsverpflichtungen auch** für (große) Player im **Wirtschaftssektor** (Zwei-Faktor-Auth. KYC/ Online Plattformen)

Europäische Brieftasche für die Digitale Identität („Wallet“)

- Elektronisches Identifikationsmittel - Vertrauensniveau „**hoch**“
- Ermöglicht es dem Nutzer,
  - Personenidentifizierungsdaten und
  - el. Attributsbescheinigungen

  sicher zu speichern, zu verwalten und zu validieren, um sie vertrauenden Beteiligten und anderen Nutzern von Wallets zu präsentieren und
- mittels **qualifizierter elektronischer Signaturen** zu unterzeichnen oder mittels qualifizierter elektronischer Siegel zu besiegeln
- **Kostenlose** Ausstellung, Verwendung und Widerruf für Nutzer (nat. Personen)

Europäische Brieftasche für die Digitale Identität („Wallet“)

- **Jeder MS** stellt mindestens eine Wallet zur Verfügung – innerhalb von **24 Monaten nach Inkrafttreten der DfRA**, mit denen die Referenzstandards und Spezifikationen definiert werden (innerhalb von 6 Monaten nach Inkrafttreten der neuen VO)
- EUDI Wallets können (bzw. müssen) ausgegeben werden:
  a) unmittelbar von einem Mitgliedstaat,
  b) im Auftrag eines Mitgliedstaats oder
  c) unabhängig von einem Mitgliedstaat, aber von diesem anerkannt
- **Quellcode** der Anwendungssoftwarekomponenten von Wallets: **Open-Source** - Ausnahmemöglichkeit für MS bei hinreichend begründeten Fällen für bestimmte Komponenten, die nicht auf den Geräten des Nutzers installiert sind.

Funktionen der Wallet („auf eine nutzerfreundliche und für die Nutzer transparente und nachvollziehbare Weise“)

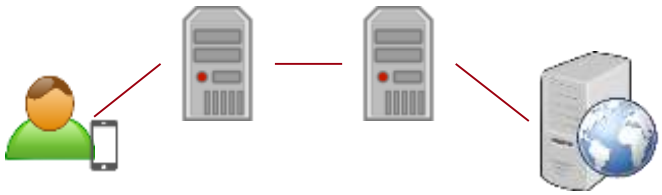
- sichere Anfordern, Erhalten, Auswählen, Kombinieren, Speichern, Löschen, Weitergeben und Vorweisen – unter alleiniger Kontrolle durch den Nutzer – **elektronischer Attributsbescheinigungen** und von **Personenidentifizierungsdaten** um sich **online** und, **gegebenenfalls, offline** für den Zugang zu **öffentlichen** und **privaten Diensten** zu **authentifizieren**, bei gleichzeitiger Sicherstellung, dass eine **selektive Offenlegung von Daten** möglich ist
- Generieren von Pseudonymen und deren Speicherung
- Authentifizierung und Austausch von Attributsbescheinigungen mit anderer Wallet

Funktionen der Wallet („auf eine nutzerfreundliche und für die Nutzer transparente und nachvollziehbare Weise“)

- Zugang zur Protokollierung der Transaktionen (Dashboard) inkl. Möglichkeit für Löschungsersuchen und Meldungen an Datenschutzbehörden
- Auslösen von qualifizierten el. Signaturen bzw. Siegel
- Herunterladen von Nutzerdaten, EAA und Konfigurationen „soweit techn. möglich“
- Ausübung der Rechte auf Datenübertragbarkeit

Wesentlicher technischer/ konzeptueller Unterschied „wallet“

- eIDAS bisher (bzw. weiterhin bei **notif. eIDs**)
  - nationale Knoten (eIDAS Nodes) entkoppeln MS-Situation
  - sowohl auf Seite des vertrauenden Beteiligten als auch eID-seitig
  - Attribute als Teil des SAML-AuthN Requests aus Quell-MS-Infrastr.



- **Wallet**
  - Schnittstelle Wallet ⇔ Anwendung
  - Attribute: Personenidentifizierungsdaten und EAA im Wallet oder in „Cloud“
  - Attribute über (qualifizierten) VDA oder aus authentischer Quelle

Dafür müssen wallets insbesondere unterstützen:

- gemeinsame Protokolle und Schnittstellen
  - für Ausstellung/ Anfordern/ Validieren von Personenidentifzierungsdaten (PID) und EAA
  - Weitergeben und Vorweisen von PID und EAA oder selektiven Daten
  - Interaktion mit anderen wallets
  - für qual. Signaturen/ Siegel…
- **Kostenlose qual. Signatur** für nat. Personen (Ausnahmemögl. für MS für gewerbl. Nutzung)

Grundsätze für die Wallet

- **Uneingeschränkte Kontrolle** der Nutzer über ihre Daten
- Keine „Tracing“-Möglichkeit für Anbieter der Wallets zum Nutzerverhalten.
- **Freiwilligkeit** der Nutzung und keine Benachteiligung bei Nichtnutzung
  - „…dürfen in ihrem Zugang zu öffentlichen und privaten Diensten und zum Arbeitsmarkt sowie in ihrer unternehmerischen Freiheit in keiner Weise eingeschränkt oder benachteiligt werden.“
  - „Der Zugang zu öffentlichen und privaten Diensten muss weiterhin über andere bestehende Identifizierungs- und Authentifizierungsmittel möglich sein.“
- **Datenminimierung**: Mindestdaten für den jeweiligen Dienst.

Vertrauende Beteiligte

- MS haben ein **Registrierungsverfahren** vorzusehen und eine **öffentliche Liste** zu führen.
- Vertrauende Beteiligte müssen **Pseudonyme** akzeptieren, wenn die Identifizierung des Nutzers nicht im Unionsrecht oder im nationalen Recht vorgeschrieben ist.
- **Private vertrauende Beteiligte**, die (vertraglich oder gesetzlich) verpflichtet sind, eine Online-Identifizierung mit **starker Nutzerauthentifizierung** vorzunehmen (auch in den Bereichen Verkehr, Energie, Bankenwesen, Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation) **müssen** spätestens 12 Monate nach Ausgabeverpflichtung der MS Wallets akzeptieren (Ausnahme für KMU).
- **VLOPs** gem. DSA (> 45 Mio EU-user) **müssen** zur Authentifiz. Wallets akzeptieren.

Onboarding

- Wallet ist ein Identifizierungsmittel auf Sicherheitsstufe „**hoch**“
- **„Heben“ bestehender eIDs mit Sicherheitsstufe „substanziell“:** Onboarding nicht nur über el. Identifizierungsmittel der Sicherheitsstufe ‚hoch‘, sondern auch der Sicherheitsstufe ‚substanziell‘–

  „in Verbindung mit zusätzlichen Verfahren der Ferneinbindung, die zusammen den Anforderungen der Sicherheitsstufe ‚hoch‘ entsprechen“.

  EK hat dazu DfRA zu erlassen.

Zertifizierung

- Im Gegensatz zu den notifizierten eIDs gibt es für Wallets keine „Notifizierung“ mit peer review-Mechanismus. Anstatt dessen: Zertifizierung
- Konformitätsbewertungsstellen zertifizieren die Konformität mit den Anforderungen (nationale Schemata).
- In Bezug auf Cybersicherheitsaspekte: CSA-Zertifizierung
- Zertifizierung gilt für 5 Jahre, alle 2 Jahre Schwachstellenbeurteilung

Governance

- Nationale Aufsichtsstellen für das Wallet einzurichten/ zu benennen
- Neuregelung der Aufsicht über VDA im Zusammenspiel mit NIS2-RL
- Benennung einer einheitlichen Anlaufstelle für VDA, Wallets und notfizierte eIDs
- „Europäische Kooperationsgruppe für die digitale Identität“

Nach den VO-Verhandlungen

…. ist **vor** den Verhandlungen zu den Durchführungsrechtsakten:

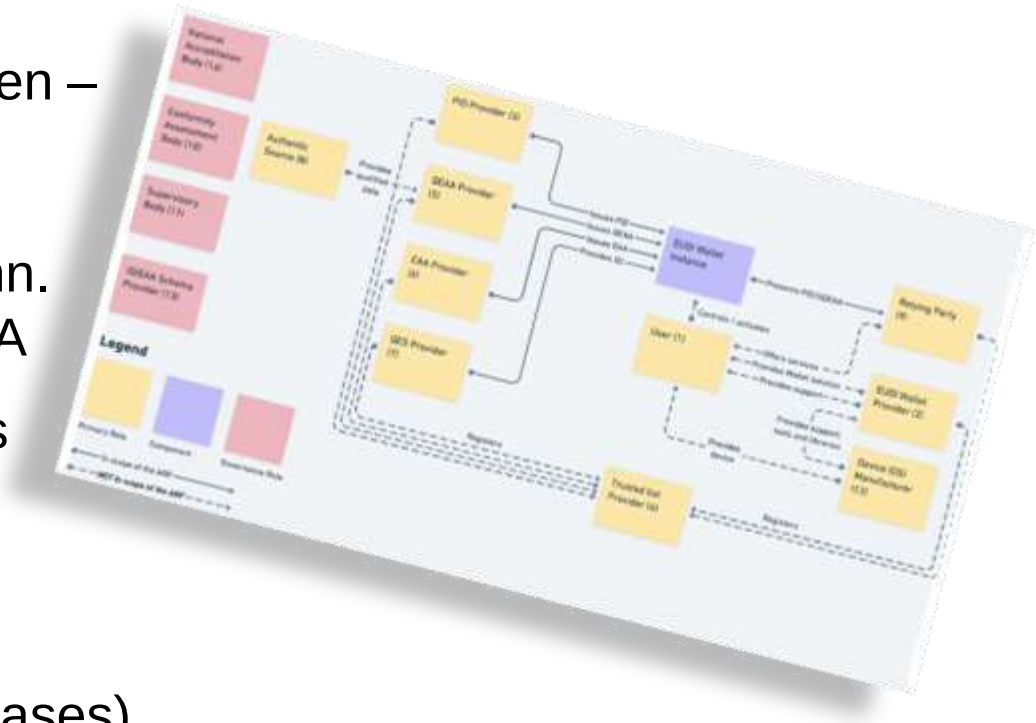
35

DfRA vorgesehen

- tw. optional
- Zeithorizont 6 Mo, 12 Mo, 24 Mo nach Inkrafttreten der neuen VO

eIDAS-Revision – Parallele Streams

- Parallel zu den VO-Verhandlungen liefen bereits Arbeiten zu
  - Architekturreferenzrahmen – ARF („Toolbox-Prozess“) – Vorbereitung für die techn. Spezifikationen/ die DfRA
  - Referenz-Wallet (EK) als Angebot an die MS
  - Large Scale Pilots (vier Konsortien zu unterschiedlichen Use Cases) samt Koordination zwischen diesen

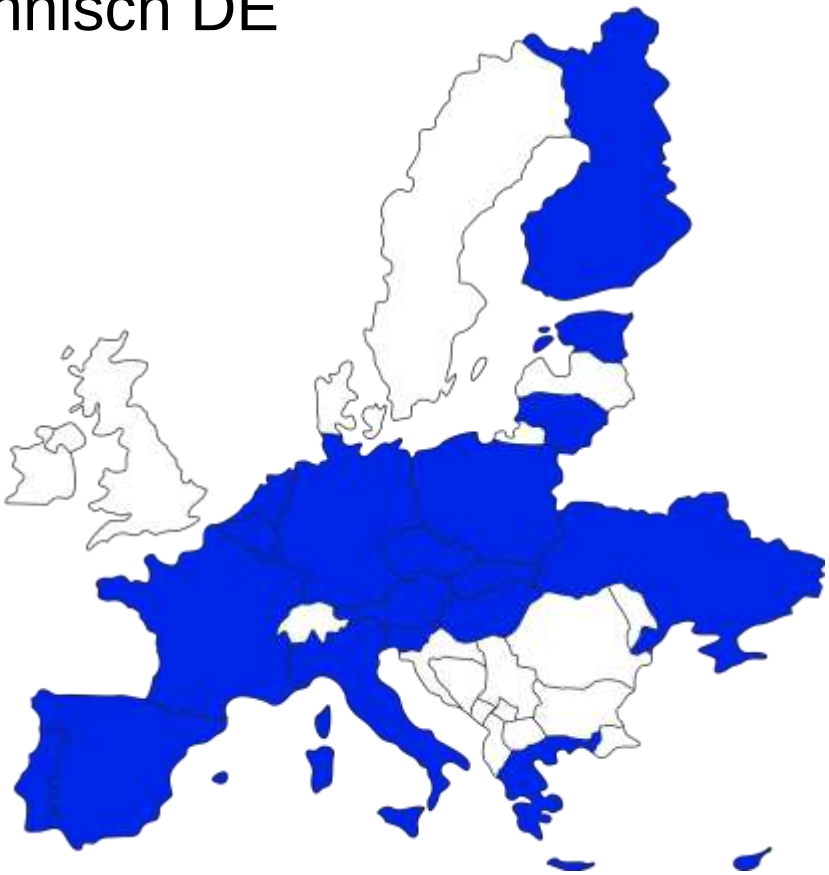


Large Scale Pilots

- EK fördert seit einiger Zeit Large Scale Pilots in wesentlichen Politikbereichen
- Ebenso zum Wallet mit Mitteln aus dem Digital Europe Programme
  - 4 LSPs werden gefördert:
    - DC4EU https://dc4eu.eu/
    - EWC https://eudiwalletconsortium.org/
    - NOBID https://www.nobidconsortium.com/
    - POTENTIAL https://www.digital-identity-wallet.eu/

LSP Potential: Eckdaten

- Gesamtkoordination FR, technisch DE
  - 19 MS plus Ukraine
  - ca. 140 Organisationen
  - In Österreich über Arbeitsgemeinschaft Wallet.at mit 13 Partnern
    - Zu Wallet BKA federführend
- Start 1. April 2023
- Dauer 26 Monate



LSP Potential: Technische Inhalte

- Umsetzung ARF und Integration in 6 Use Cases
  - Identifikation im E-Government
  - Kontoeröffnung
  - Digitaler Führerschein
  - SIM Registrierung
  - Qualifizierte Signatur
  - eMedikation

eIDAS-Revision – Bewertung

- eIDAS Revision bringt eine Reihe von Neuerungen
  - Viele positive Elemente (Einbeziehung Privatsektor, Betonung der mobilen Lösungen…)
- Herausforderungen:
  - Wallet muss markttauglich und nutzerfreundlich sein (zB breit einsetzbar auf unterschiedlichsten Gerätemodellen)/ Zertifizierungsthema
  - Online/ offline-Szenarien
  - Zeitliche Dimension „sportlich“
- AT hat mit ID-Austria und „Ausweisplattform“ einen guten Ausgangspunkt – intensive Beteiligung in den Verhandlungen und Entwicklungen

Danke

für Ihre Aufmerksamkeit!

Mag. Peter Kustor

Bundeskanzleramt
Abt. VII/A/2 - Legistik und Stammzahlenregisterbehörde, E-Government-Strategie sowie EU und Internationales

peter.kustor@bka.gv.at
@PeterKustor

Links

- Digitales Österreich
  https://www.bundeskanzleramt.gv.at/agenda/digitalisierung.html
  https://www.digitalaustria.gv.at/
- E-Government-Strategie:
  https://www.digitalaustria.gv.at/Strategien/E-Government-Strategie.html
- Rechtsvorschriften
  https://www.digitalaustria.gv.at/WissensWert/E-Gov-A-Z/Was-bedeutet-digitale-Verwaltung/Rechtlicher-Rahmen-der-Digitalen-Verwaltung.html
- Reference-Server
  Auf diesem Server werden die gemeinsam von Bund, Ländern und Gemeinden erarbeiteten Vorschläge und Empfehlungen publiziert.
  https://neu.ref.wien.gv.at/
- OESTERREICH.gv.at: http://www.oesterreich.gv.at/
- Unternehmensserviceportal: www.usp.gv.at
- IKT-Sicherheitsportal: https://www.onlinesicherheit.gv.at/
- Datenschutz - Website der österreichischen Datenschutzbehörde
  http://www.dsb.gv.at/

Links

- ID Austria: https://www.oesterreich.gv.at/id-austria.html und https://eid.egiz.gv.at/
- Monitoring Zertifikate (ua für ID Austria): https://www.a-trust.at/monitoring/zertifikate/
- Zentrum für sichere Informationstechnologie - Austria (A-SIT) http://www.a-sit.at/