eIDAS 2.0 Status

OSSBIG Webinar

Peter.Kustor@bka.gv.at

Wien, 26. Juni 2024

Der bisherige EU-Rechtsrahmen: die eIDAS-VO (2014)

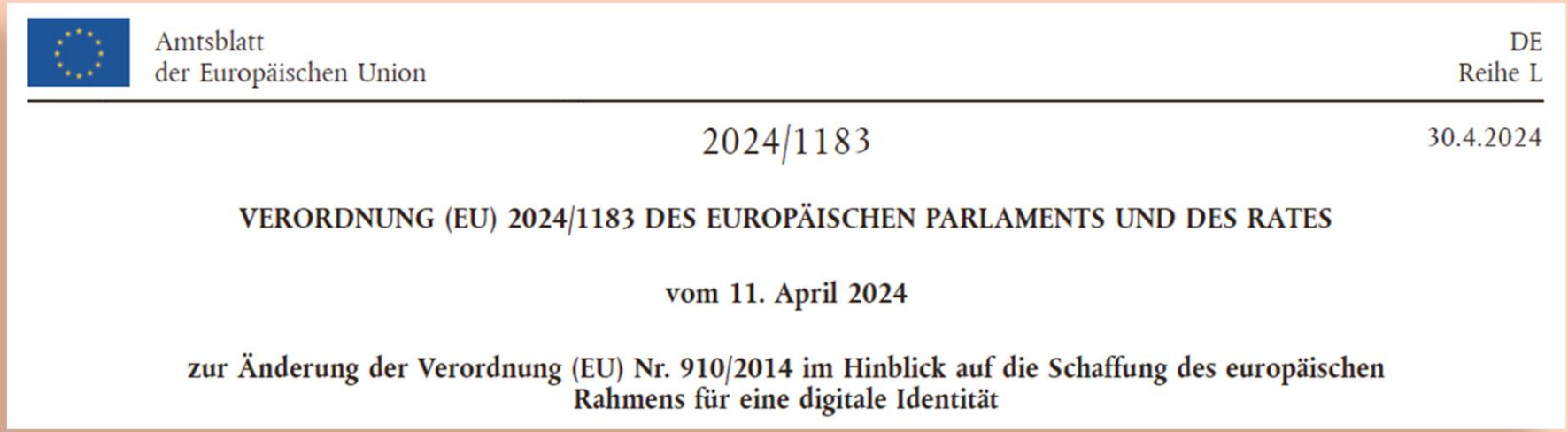
28.8.2014 DE Amtsblatt der Europäischen Union L 257/73

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

Der neue EU-Rechtsrahmen: eIDAS 2



Amtsblatt
der Europäischen Union

DE
Reihe L

2024/1183

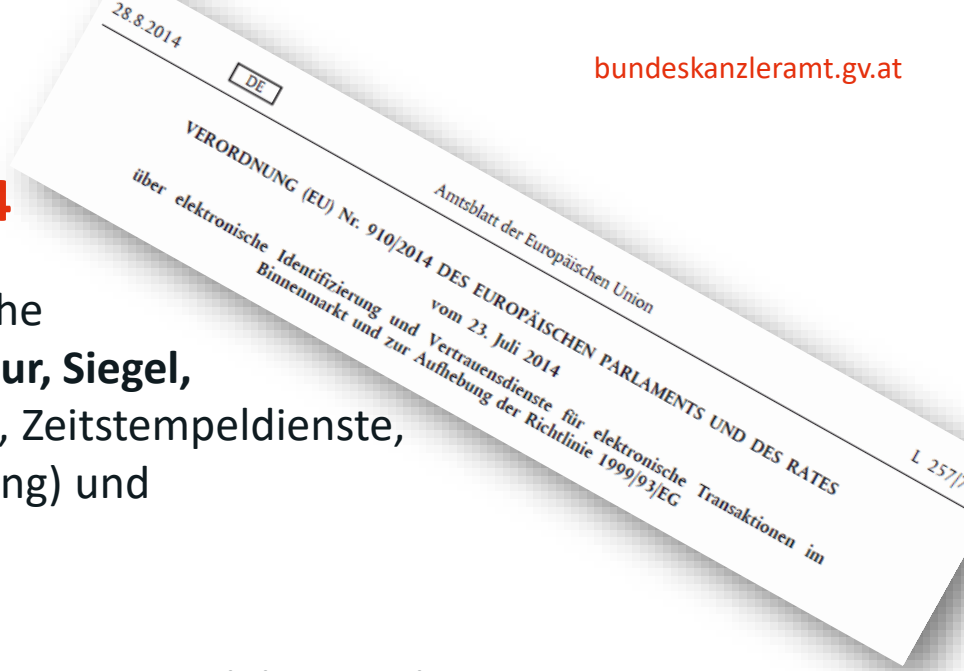
30.4.2024

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

Ausgangspunkt eIDAS-VO - 2014


28.8.2014 DE Amtsblatt der Europäischen Union L 257/

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

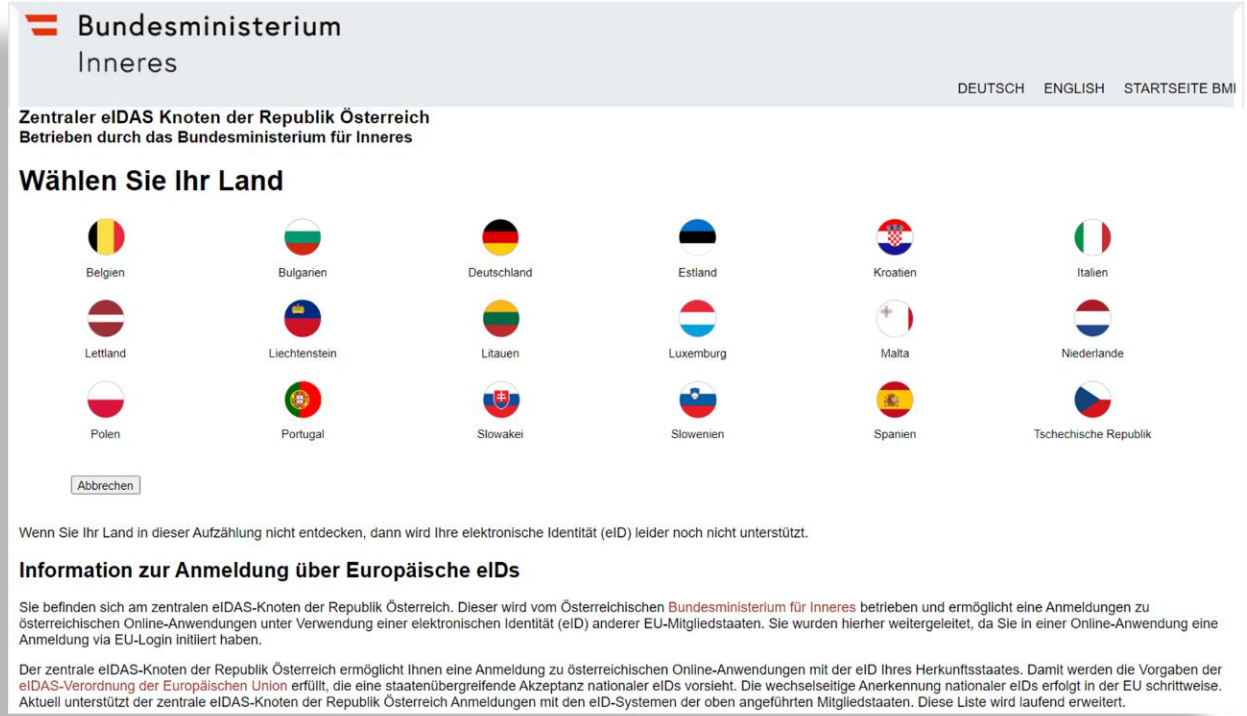
Ein Rechtsakt für die beiden Themenbereiche

- **Vertrauensdienste (elektronische Signatur, Siegel,** Bewahrungsdienste, Validierungsdienste, Zeitstempeldienste, „Zustelldienste“, Website Authentifizierung) und
- **elektronische Identität** („eID“)

Eckpunkte:

- Harmonisierung im Bereich Vertrauensdienste. Qu elektronische Signatur einer nat. Person „der handschriftlichen Unterschrift gleichgestellt“ …
- 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“)

eID – Anerkennung - Notifizierungen



Bundesministerium
Inneres

DEUTSCH ENGLISH STARTSEITE BMI

Zentraler eIDAS Knoten der Republik Österreich
Betrieben durch das Bundesministerium für Inneres

Wählen Sie Ihr Land

Belgien, Bulgarien, Deutschland, Estland, Kroatien, Italien
Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande
Polen, Portugal, Slowakei, Slowenien, Spanien, Tschechische Republik

Abbrechen

Wenn Sie Ihr Land in dieser Aufzählung nicht entdecken, dann wird Ihre elektronische Identität (eID) leider noch nicht unterstützt.

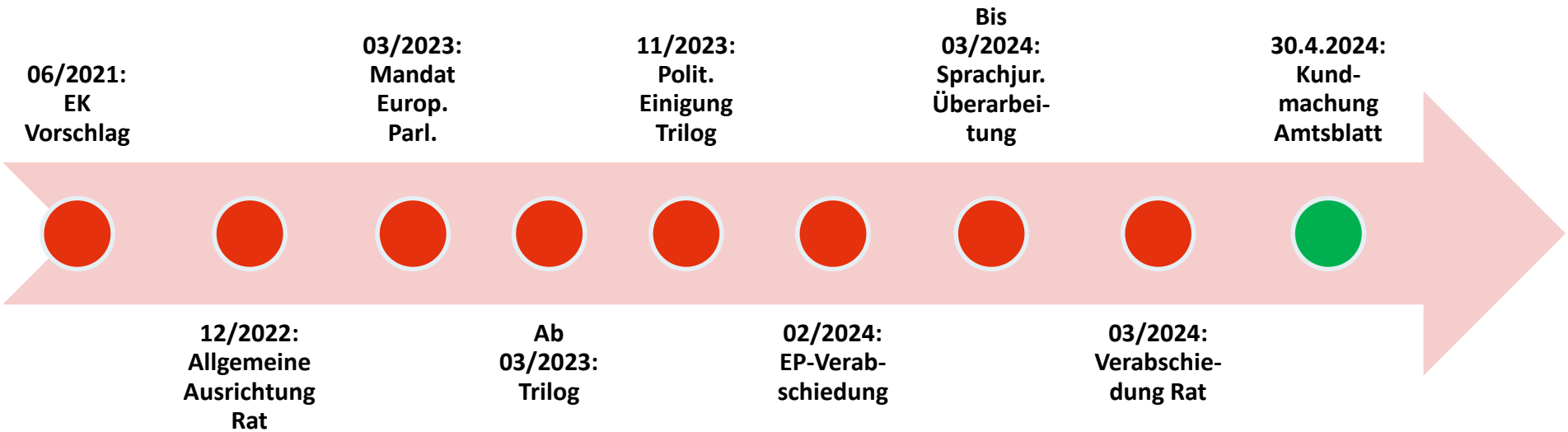
Information zur Anmeldung über Europäische eIDs

Sie befinden sich am zentralen eIDAS-Knoten der Republik Österreich. Dieser wird vom Österreichischen Bundesministerium für Inneres betrieben und ermöglicht eine Anmeldungen zu österreichischen Online-Anwendungen unter Verwendung einer elektronischen Identität (eID) anderer EU-Mitgliedstaaten. Sie wurden hierher weitergeleitet, da Sie in einer Online-Anwendung eine Anmeldung via EU-Login initiiert haben.

Der zentrale eIDAS-Knoten der Republik Österreich ermöglicht Ihnen eine Anmeldung zu österreichischen Online-Anwendungen mit der eID Ihres Herkunftsstaates. Damit werden die Vorgaben der eIDAS-Verordnung der Europäischen Union erfüllt, die eine staatenübergreifende Akzeptanz nationaler eIDs vorsieht. Die wechselseitige Anerkennung nationaler eIDs erfolgt in der EU schrittweise. Aktuell unterstützt der zentrale eIDAS-Knoten der Republik Österreich Anmeldungen mit den eID-Systemen der oben angeführten Mitgliedstaaten. Diese Liste wird laufend erweitert.

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

Prozess eIDAS Revision



Wesentliche Neuerungen zu eIDAS 1 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)

Blick in die Details

1. Vertrauensdienste

Hier: lediglich Fokus auf das neue Thema

„El. Attributsbescheinigungen (EAA)“

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

Blick in die Details

1. Vertrauensdienste
2. Elektronische Identität – „Wallet“

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“)

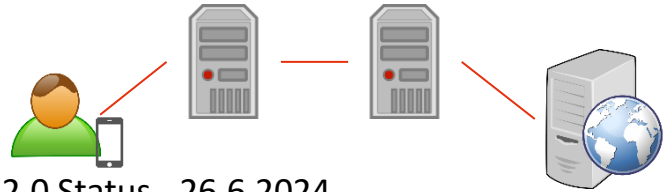
- sichere Anfordern, Erhalten, Auswählen, Kombinieren, Speichern, Löschen, Weitergeben und Vorweisen – unter alleiniger Kontrolle durch den Nutzer – **elektronischer Attributsbescheinigungen** und von **Personenidentifizierungsdaten** um sich **online** und, **gegebenenfalls, offline** für den Zugang 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
- Zugang zur Protokollierung der Transaktionen (Dashboard) inkl. Möglichkeit für Löschungsersuchen und Meldungen an Datenschutzbehörden

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

- 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 entweder
    - Personenidentifizierungsdaten
    - 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“

Strafbestimmungen

- Erhebliche Verschärfung gegenüber dem bisherigen Reglement
- Mindesthöchststrafe für qual. VDA: 5 Mio EUR bzw. 1% des gesamten weltweiten Umsatz des vorigen Geschäftsjahrs.

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 – 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!

Peter Kustor
Abteilung VII/2 – Legistik und Stammzahlenregisterbehörde,
E-Government-Strategie sowie EU und Internationales
peter.kustor@bka.gv.at