ELSTER-ZERTIFIZIERUNG NUN AUCH FÜR DIE KOMMUNIKATION MIT DER JUSTIZ – ZUKUNFTSWEISEND?

2. Digital Justice Lunch des EDVGT- Forum für digitale Innovation im Recht

Prof. Dr. Wilfried Bernhardt

Universität Leipzig

BISHERIGE RECHTLICHE GRUNDLAGEN FÜR KOMMUNIKATION VON ORGANISATIONEN MIT GERICHTEN

§§

§ 11 Abs. 2 ERVV: Der Postfachinhaber hat im Rahmen der Identitätsfeststellung seinen Namen und seine Anschrift nachzuweisen. 2Der Nachweis kann nur durch eines der folgenden Identifizierungsmittel erfolgen: (…)
(2) ein **qualifiziertes elektronisches Siegel** nach Artikel EWG_VO_910_2014 Artikel 38 der 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 (ABl. L 257 vom 28.8.2014, S. 73; L 23 vom 29.1.2015, S. 19; L 155 vom 14.6.2016, S. 44), (…)
(5) „ eine in öffentlich beglaubigter Form abgegebene Erklärung über den Namen und die Anschrift des Postfachinhabers sowie die eindeutige Bezeichnung des Postfachs.
Abs. 3: Eine nach Satz 2 Nummer 5 angegebene geschäftliche Anschrift ist durch eine Bescheinigung nach § 21 Abs. 1 der Bundesnotarordnung, einen amtlichen Registerausdruck oder eine beglaubigte Registerabschrift nachzuweisen. (4) Geht eine angegebene geschäftliche Anschrift nicht aus einem öffentlichen Register hervor, so stellt die Stelle nach Absatz 1 diese durch geeignete Maßnahmen fest. (..)

- **Organisationen oder Unternehmen** können bislang über ein **besonderes elektronisches Bürger- und Organisationenpostfach (eBO)** elektronische Erklärungen gegenüber der Justiz abgeben, § 130a Absatz 4 Satz 2 ZPO; Einzelheiten der erforderlichen Identifizierung in der **Elektronischer- Rechtsverkehr-Verordnung (ERVV)** geregelt.
- In Betracht kommen dabei
  - die Identifizierung **mit einem qualifizierten elektronischen Siegel**, § 11 Absatz 2 Satz 2 Nr. 2 ERVV in Verbindung mit Artikel 38 der VO (EU) Nr. 910/2014 („eIDAS VO“); gem. eIDAS entspricht dies dem Vertrauensniveau „hoch“,
  - oder das **Identifizierungsverfahren nach § 11 Abs. 2 Satz 2 Nr. 5 ERVV**.

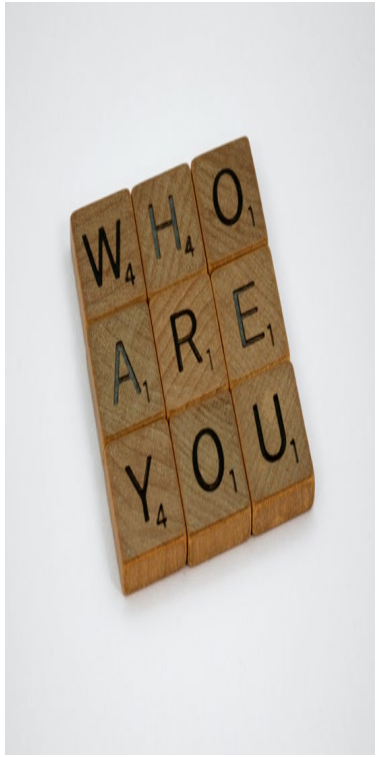


Photo by Brett Jordan on Unsplash

BISHERIGE RECHTLICHE GRUNDLAGEN FÜR KOMMUNIKATION ÜBER OZG-NUTZERKONTO

§§

§ 13 ERVV Elektronische Kommunikation über den Postfach- und Versanddienst eines Nutzerkontos

(1) Zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg kann der Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Abs.5 des Onlinezugangsgesetzes genutzt werden, wenn bei diesem Postfach- und Versanddienst

•1.eine technische Vorrichtung besteht, die auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht,

•2.die Identität des Nutzers des Postfach- und Versanddienstes durch ein Identifizierungsmittel nach § 11 Abs. 2 Satz 2 Nummer 1 oder 2 festgestellt ist,

•3.der Nutzer des Postfach- und Versanddienstes sich beim Versand eines elektronischen Dokuments entsprechend § 11 Abs. 3 authentisiert und

•4.feststellbar ist, dass das elektronische Dokument von dem Nutzer des Postfach- und Versanddienstes versandt wurde.

- Gem. § 130a Abs.4 Nr. 5 ZPO war zwar grundsätzlich auch die elektronische Kommunikation zwischen einem Postfach- und Versanddienst eines **Nutzerkontos nach § 2 Absatz 5 OZG** – und somit des Organisationskontos – und der elektronischen Poststelle des Gerichts als sicheren Übermittlungsweg zulässig.
- Aber diese Kommunikation war dennoch nicht möglich, da das im OZG vorgesehene Identifizierungsverfahren gem. § 2 Abs. 5 Satz 4, § 3 Abs. 2 Satz 3 OZG**, § 87a Abs. 6 AO (= Elster) **bisher** nicht als Identifizierungsmittel durch **§ 13 ERVV** zugelassen war.
- Die für Bürgerinnen und Bürger vorgesehene Browseranwendung **„Mein Justiz-Postfach (MJP)“** als Postfach- und Versanddienst des Nutzerkontos Bund ist nicht für Organisationen/Unternehmen vorgesehen.* Für Anlegen eines MJP ist erforderlich Identifizierung der Nutzer mit der BundID, welche unter **Verwendung der eID des Personalausweises** eingerichtet worden sein muss – für Unternehmen nicht möglich.

*https://mein-justizpostfach.bund.de/ **“Über das Organisationskonto können sich Nutzer im Sinne des § 2 Absatz 5 Satz 4 für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich über ein nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung eingesetztes sicheres Verfahren identifizieren und authentisieren“.

NEUE RECHTLICHE GRUNDLAGEN

§§

§ 13 ERVV
(1) Zur Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg kann der Postfach- und Versanddienst eines Nutzerkontos im Sinne des § 2 Absatz 5 des Onlinezugangsgesetzes genutzt werden, wenn bei diesem Postfach- und Versanddienst
1. eine technische Vorrichtung besteht, die auf dem Protokollstandard OSCI oder einem diesen ersetzenden, dem jeweiligen Stand der Technik entsprechenden Protokollstandard beruht,
2. die Identität des Nutzers des Postfach- und Versanddienstes durch ein Identifizierungsmittel nach § 11 Absatz 2 Satz 2 Nummer 1 oder 2 **oder für Nutzer des Organisationskontos im Sinne des § 2 Absatz 5 Satz 4 des Onlinezugangsgesetzes durch ein nach § 87a Absatz 6 der Abgabenordnung in der Steuerverwaltung eingesetztes sicheres Verfahren festgestellt ist**,
3. der Nutzer des Postfach- und Versanddienstes sich beim Versand eines elektronischen Dokuments entsprechend § 11 Absatz 3 authentisiert und
4. feststellbar ist, dass das elektronische Dokument von dem Nutzer des Postfach- und Versanddienstes versandt wurde.
(…)

- Nunmehr ist gem. **§ 13 Abs. 1 Nr. 2 ERVV (neu)** für die Übermittlung elektronischer Dokumente auf einem sicheren Übermittlungsweg aus dem Postfach eines OZG-Nutzerkontos ausreichend, dass sich die Nutzerin oder der Nutzer eines **Organisationskontos*** durch ein **ELSTER-Zertifikat** identifiziert.

- Neue Regelung eingefügt durch Art. 43 Gesetz zur weiteren Digitalisierung der Justiz, BGBl. 2024 I Nr. 234 vom 16.07.2024, in Kraft gem. Art. 50 seit 17. Juli 2024.

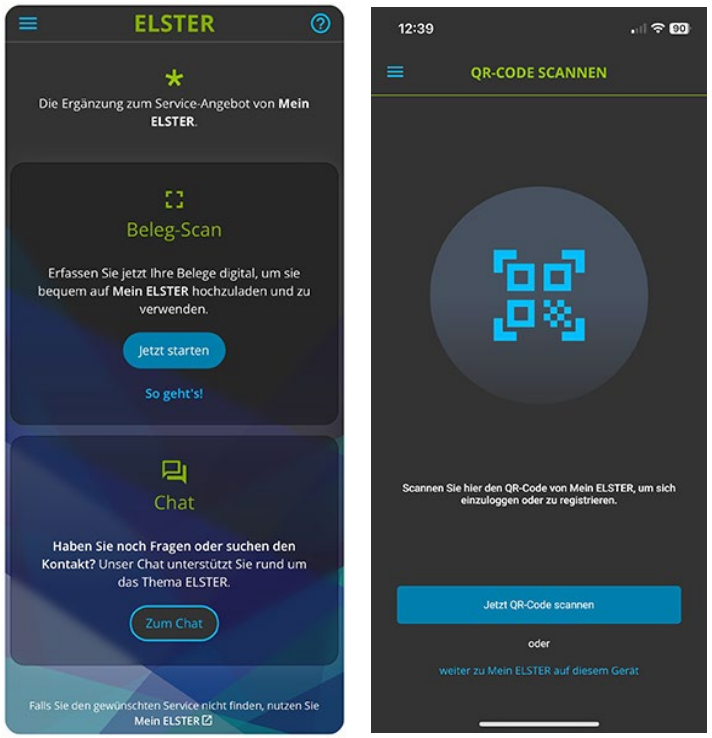
*Ein „Organisationskonto“ ist ein Nutzerkonto, das juristischen Personen, Vereinigungen, denen ein Recht zustehen kann, natürlichen Personen, die gewerblich oder beruflich tätig sind, oder Behörden zur Verfügung steht (§ 2 Abs. 5 Satz 4 OZG)

Photo by Conny Schneider on Unsplash

ZIEL DER NEUREGELUNG IN ERVV

- Begründung des Gesetzentwurfs (Drucksache 20/10943, S.70):
  - Zur Änderung des § 11 ERVV (Streichung der Anforderung, dass das nichtqualifizierte Authentisierungszertifikat über **im Internet erreichbare** Instrumente validierbar ist): „soll eine einheitliche Regelung für alle Authentisierungszertifikate schaffen. Das ELSTER-Zertifikat stellt ein nichtqualifiziertes Authentisierungszertifikat dar, welches grundsätzlich validiert werden kann. Die bisherige Einschränkung auf Dienste, die über das Internet erreichbar sind, ist hingegen nicht mehr erforderlich. Mit der Änderung soll auch die Authentisierung mithilfe des ELSTER-Zertifikat weiterhin ermöglicht werden."
  - Zur Änderung des § 13 ERVV: „Mit der Änderung werden die rechtlichen Rahmenbedingungen für die Anbindung des Organisations-(„Unternehmens"-)Kontos nach dem Onlinezugangsgesetz (OZG-Organisationskonto)* an das Elektronische Gerichts- und Verwaltungspostfach (EGVP) geschaffen." **„Im Interesse eines möglichst breiten elektronischen Zugangs zur Justiz** soll das ELSTER-Verfahren daher auch in der ERVV als Identifizierungsmittel **für das OZG-Organisationskonto** zugelassen werden."
  - Elster-Zertifizierung gilt also **nur** für Organisationen/Unternehmen.

WIE FUNKTIONIERT ELSTER-ZERTIFIKAT?



- ELSTER steht für „Elektronische Steuererklärung“
- Mit **Mein ELSTER** können Bürger und Unternehmen über den Browser ihre **Steuererklärungen** abgeben. Für den Erhalt der ELSTER-Zertifikatsdatei muss man sich **mit persönlichen Daten (insbesondere Steuernummer und E-Mail-Adresse) registrieren**. Anschließend wird **Link an die angegebene E-Mail-Adresse versandt**, der zu **bestätigen** ist.
- Nach Bestätigung der E-Mail-Adresse werden die Aktivierungsdaten **auf dem Postweg** an die bei der Finanzverwaltung gespeicherte Anschrift übermittelt, um so sicherzustellen, dass ausschließlich berechtigte Personen einen Zugang für eine Organisation erstellen können.
- Nach Abschluss der Registrierung kann die **Zertifikatsdatei heruntergeladen** werden. Sodann kann sich der Anwender über einen sicheren Login anmelden.
- Zwei Apps stehen inzwischen zur Verfügung: Mit der **App MeinELSTER+** können Belege (z. B. Handwerkerrechnung, Spendenquittung, etc.) für die nächste Steuererklärung in das Benutzerkonto bei Mein ELSTER hochladen werden. **ElsterSecure** als eine Login-App von übernimmt die Authentisierung bei ELSTER. Nach Einrichtung auf der Basis eines bestehenden Kontos mit Zertifikatsdatei und Verknüpfung über einen QR-Code mit dem Konto wird für den Login nur noch das Smartphone (ohne weitere Zertifikatsdatei oder Passwort) benötigt.
- ELSTER-Zertifikat kann mittlerweile auch für die Identifizierung zur internetbasierten Fahrzeugzulassung (online An-, Ab- und Ummeldung- „i-Kfz“) genutzt werden*

* https://bmdv.bund.de/SharedDocs/DE/Publikationen/StV/internetbasierte-fahrzeugzulassung.pdf?__blob=publicationFile

Fotos und Informationen von
https://www.elster.de/elsterweb/infoseite/apps

SICHERHEITSPROBLEME MIT ELSTER

Photo by Bermix Studio on Unsplash

https://www.elster.de/eportal/start;
abgerufen am 18.07.2024

⚠ **Betrugsversuche im Namen von ELSTER**

Aktuell versuchen Betrüger per E-Mail oder mit gefälschten Webseiten mit ELSTER-Bezug an Informationen von Bürgerinnen und Bürgern zu gelangen.

Sie versenden E-Mails mit Titeln wie "Dringende Handlung erforderlich: Ihr ELSTER Steuerrestbetrag" im Namen von ELSTER oder lotsen Bürgerinnen und Bürger auf gefälschte Webseiten mit ELSTER-Bezug.

Wir warnen ausdrücklich davor, auf diese Betrugs-E-Mail zu reagieren bzw. die Links in der E-Mail zu öffnen. Auch Webseiten mit ELSTER-Bezug sollten nur mit äußerster Vorsicht besucht werden.

Weitere Informationen zu Betrugs-E-Mails erhalten Sie auf der Seite **Sicherheit**.

NEUREGELUNG DES ONLINEZUGANGSGESETZES (OZG)*

Foto von Firmbee.com auf Unsplash

- § 3 Absatz 4 OZG neu (noch nicht im BGBl verkündet):
- „(4) Der Nachweis der Identität des Nutzers erfolgt
- 1. im **Bürgerkonto**
- a) für elektronische Verwaltungsleistungen, für die **höchstens das Vertrauensniveau „substantiell“ erforderlich ist**, durch ein **sicheres Verfahren nach § 87a Absatz 6 der Abgabenordnung**
- oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 Verordnung (EU) Nr. 910/2014 (eIDAS VO) **mindestens mit dem Sicherheitsniveau „substantiell“** im Sinne des Artikels 8 Absatz 2 Buchstabe b der Verordnung (EU) Nr. 910/2014 anerkannt worden ist,
- b) für elektronische Verwaltungsleistungen, für die das **Vertrauensniveau „hoch“ erforderlich** ist, durch einen elektronischen Identitätsnachweis nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes oder **durch ein anderes elektronisches Identifizierungsmittel,** welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 mit dem Sicherheitsniveau „hoch“ im Sinne des Artikels 8 Absatz 2 Buchstabe c der Verordnung (EU) 910/2014 anerkannt worden ist.

*lt. Beschlussempfehlung Vermittlungsausschuss, Drucksache 20/11790 vom 12.06.2024 https://dserver.bundestag.de/btd/20/117/2011790.pdf

NEUREGELUNG DES ONLINEZUGANGSGESTZES (OZG)*

Foto von Firmbee.com auf Unsplash

- 2. im **einheitlichen Organisationskonto** durch ein **sicheres Verfahren nach § 87a Absatz 6 der Abgabenordnung** oder durch ein anderes elektronisches Identifizierungsmittel, welches nach Artikel 6 der Verordnung (EU) Nr. 910/2014 **mindestens mit dem Sicherheitsniveau „substantiell“** im Sinne des Artikels 8 Absatz 2 Buchstabe b der Verordnung (EU) Nr. 910/2014 anerkannt worden ist.
- Gem. § 12 Abs. 2 werden die gem. § 87a Abs. 6 AO in der Steuerverwaltung bis einschließlich 31. Dezember 2019 eingesetzten sicheren Verfahren bundesweit zum Nachweis der Identität auf dem Vertrauensniveau „substantiell“ anerkannt.
- Ursprünglich im Gesetzentwurf in § 12 Abs. 3 vorgesehene Befristung von Elster als Identifizierungsmöglichkeit auf 5 Jahre gestrichen.
- **Also: Elster-Identifizierung bei Bürgerinnen und Bürgern nur, wenn kein Vertrauensniveau „hoch“ gefordert ist. Demgegenüber Elster-Zertifizierung bei Organisationen generell möglich.**

*lt. Beschlussempfehlung Vermittlungsausschuss, Drucksache 20/11790 vom 12.06.2024 https://dserver.bundestag.de/btd/20/117/2011790.pdf

KRITIK AN ELSTER-IDENTIFZIERUNG

ELSTER

BUNDESNOTARKAMMER
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

- **BNotK begrüßt** die **Anbindung der OZG-Nutzerkonten an den elektronischen Rechtsverkehr** grundsätzlich, da damit die Möglichkeiten eines digitalen Zugangs zur Justiz für die Bürgerinnen und Bürger und für Organisationen erweitert werden. Ferner Vereinfachung des Zugangs zum Gericht, da Nutzerkonto zur Inanspruchnahme von Verwaltungsleistungen sowieso wahrscheinlich eingerichtet und dies dann auch für die Justiz genutzt werden kann.
- ELSTER-Zertifikat allerdings **nicht hinreichend sicher**. Es bietet **keinen hinreichenden Authentizitätsschutz**, um die **prozessuale Schriftform ersetzen** zu können. Die Zulassung des ELSTER-Zertifikats als Identifizierungsmethode **nicht notwendig**, um **Organisationen an den elektronischen Rechtsverkehr anzubinden**.
- Eine rechtssichere Identifizierung findet nicht statt. Für eine erfolgreiche Identitätstäuschung müsste lediglich **die Steuernummer bekannt sein** und die **Post an die bei der Finanzverwaltung hinterlegte Anschrift abgefangen** werden.
- ELSTER-Zertifikatsdateien sind Softwarezertifikate, die **leicht und beliebig häufig kopiert werden können, ohne dass dies für den Zertifikatsinhaber bemerkbar wäre.** Passwortschutz für das Zertifikat kann allerdings umgangen werden, beispielsweise unter Einsatz von „Brute-Force-Angriffen“ umgangen werden.

KRITIK AN ELSTER-IDENTIFZIERUNG

ELSTER

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

- :
- **Prof. Ulrich Kelber (bisheriger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)** in öffentlicher Anhörung des Ausschusses für Inneres und Heimat am 9. Oktober 2023 zum Gesetzentwurf der Bundesregierung zur Änderung des Onlinezugangsgesetzes, abrufbar unter www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/969432-969432; dort ab Timecode 43:32
- Elster-Zertifizierung erreiche nicht einmal das Vertrauensniveau „substanziell“ i.S.d. eIDAS-Verordnung, werde den hohen Ansprüchen an die IT-Sicherheit bei der Digitalisierung nicht gerecht werde und sei deshalb nicht „zukunftsführend“
- Die Anerkennung der Identifizierung mittels ELSTER-Zertifikat für eine Übermittlung auf dem sicheren Übermittlungsweg **entwerte den im Rahmen des sicheren Übermittlungsweg bezweckten Authentizitätsschutz erheblich**. Damit ein elektronisches Dokument die prozessuale Schriftform ersetzen kann, müssen die Authentizität und die Integrität des Dokuments gewährleistet sein, vgl. § 130a Abs. 4 Satz 1 Nr. 6 ZPO. Die Authentizität im elektronischen Rechtsverkehr setzt aber voraus, dass die Postfachinhaber **sicher identifiziert werden und dass ein Identitätsmissbrauch ausgeschlossen ist.**
- Die **erfolgreichen Bemühungen der Justiz um die Gewährleistung der Integrität und Authentizität** der übermittelten Nachrichten im Bereich des elektronischen Rechtsverkehrs und um einen hohen Sicherheitsstandard in den vergangenen **sollten nicht durch die Zulassung einer unsicheren Identifizierungsmethode konterkariert werden**.
- Gleichzeitig sei diese Identifizierungsmethode angesichts der schon bestehenden Möglichkeiten nicht notwendig, um Organisationskonten an den elektronischen Rechtsverkehr anzubinden.

ELSTER VS. ELEKTRONISCHE ID DES PERSONALAUSWEISES

ELSTER

- **Elster-Zertifizierung**
  - Browser prüft über eine sichere Verbindung, ob das automatisch übermittelte elektronische SSL-Zertifikat gültig ist.
  - SSL-Zertifikat von ELSTER dient dazu, einen kryptographischen, öffentlichen Schlüssel an die Webseite von ELSTER zu binden. Die Bindung des Schlüssels an ELSTER wird wiederum kryptographisch mit einer elektronischen Signatur einer vertrauenswürdigen dritten Stelle, einem international anerkannten Trustcenter abgesichert.
  - ELSTER weit verbreitet: Über 20 Millionen Nutzer (2023).
  - ELSTER-Konto kann auch für **nichtsteuerliche Zwecke genutzt** werden. Hierzu ist unter www.meinunternehmenskonto.de zu Elster-Zertifikat laden. Danach kann man sich an diversen teilnehmenden Portalen von Städten, Gemeinden und öffentlichen Verwaltungen anmelden und die dortigen Dienste in Anspruch nehmen

ELSTER VS. ELEKTRONISCHE ID DES PERSONALAUSWEISES

ELSTER

- Die Anwendung von ELSTER wird gegenüber der derzeitigen Nutzbarkeit der AusweisApp als **„einfacher“** angesehen, weil ausschließliche digitale Instrumente zur Anwendung kommen (also ohne Karte).
- ELSTER erreicht aber lediglich Sicherheitsniveau „substantiell“ im Sinne der eIDAS Verordnung und kann auch für Identifizierungen für Verwaltungsleistungen nur genutzt werden, für die höchstens das Vertrauensniveau „substantiell“ erforderlich ist.
- ELSTER- Kommunikation mit der Justiz (auch mit den Finanzgerichten) erfüllt nicht die Anforderungen an eine qualifizierte elektronische Signatur, daher Unzulässigkeit einer Übermittlung einer Klage per Elster-Portal,
    - FG Münster, Urteil vom 26.04.2017 - 7 K 2792/14 E: „Eine Klage, die innerhalb der Klagefrist elektronisch über das Elster-Portal an das Finanzamt übermittelt wurde, ist unzulässig, da das Elster-Portal bei der Identifizierung nicht die Anforderungen an eine qualifizierte Signatur nach dem Signaturgesetz – SigG – erfüllt.“

ELSTER VS. ELEKTRONISCHE ID DES PERSONALAUSWEISES

AusweisApp
eID-Client des Bundes

- eGovernment Monitor 2023: nur 14 Prozent der Online-Bevölkerung, die einen Personalausweis besitzen, haben die Online-Funktion schon einmal angewandt.
- Geringe Anwendung beruht aber auch darauf, dass 38 % keine Anwendungs-möglichkeiten bekannt (eGoverment Monitor 2023)

- **eID:**
  - 2020 besaßen **62 Millionen** Deutsche einen Personalausweis mit Chip und damit die eID[1]. Hinzu kommen Bürgerinnen und Bürger mit elektronischen Aufenthaltstiteln und EU-Bürgerinnen und Bürger mit eID-Karte, die ebenfalls die Online-Ausweisfunktion als sicheren elektronischen Identitätsnachweis verwenden können.
  - Seit 2017 **kein Kartenlesegerät mehr nötig**, Nutzung direkt über Smartphone möglich.
  - allerdings muss Personalausweis-Karte noch an das Smartphone gehalten werden.
  - **SmartID Gesetz** (im September 2021 in Kraft getreten) sieht eID-Nutzung ohne Karte vor, allerdings wurde technische Lösung bisher nicht ausgerollt. Unklar auch, ob technische Lösung hinreichend sicher.
  - Im Gegensatz zu anderen Ländern (wie z.B. Dänemark) **kein einheitliches eID-Ökosystem.**
  - Tatsächliche Nutzung der eID auf niedrigem Niveau.

ZUKUNFTSFÄHIGKEIT DER EIDAS 2.0 REGELUNGEN*

Photo by jasper benning on Unsplash

- European Digital Identity Wallet (EUDIW) ermöglicht **zukünftig einfache online- Authentifizierung für privatwirtschaftliche sowie Verwaltungsdienstleistungen**
- VO enthält Vorgaben zu Interoperabilität, Datenschutz und Sicherheit der Wallets sowie zur Verifizierung digitaler Attribute.
- Konkrete Anforderungen an die Wallets noch von den europäischen Standardisierungs- und Normierungsgremien auszuarbeiten und in delegierten Rechtsakten festzulegen.
- Grenzüberschreitende Anerkennung von Identifizierungen im Rahmen der Wallet nur bei „starker Authentifizierung“ i.S. von Art. 3 Nr. 51 eIDAS (neu): unter Heranziehung von **mindestens zwei Authentifizierungsfaktoren aus verschiedenen Kategorien** entweder von **Wissen, Besitz oder Inhärenz** (Authentifizierung meist aus biometrischen Daten, die untrennbar mit der Person verbunden sind).

* EU-VO 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, ABl. L vom 30.04.2024

ZUKUNFTSFÄHIGKEIT DER EIDAS 2.0 REGELUNGEN* (2)

Photo by jasper benning on Unsplash

- Identitätsnachweise werden von **qualifizierten Vertrauensdiensteanbietern** oder **berechtigten staatlichen Quellen** (etwa Einwohnermeldeamt) geprüft und **elektronisch signiert** und wie bei der Smart-eID , aber in einer sichereren Umgebung in der Wallet auf dem Smartphone des Inhabers/ Inhaberin gespeichert.
- Weitergabe der Identitätsdaten an die **Relying Parties** (Behörden, Banken, Unternehmen) nur mit **Zustimmung des Smartphone-Inhabers/der Inhaberin**. Die Relying Party prüft über eine **EU Trusted List**, ob Daten auch wirklich von der ausstellenden Instanz verifiziert wurden.
- „Europäische Brieftaschen für die Digitale Identität sollten für die Zwecke der elektronischen Identifizierung und Authentifizierung ein **Höchstmaß an Datenschutz und Sicherheit gewährleisten**, um den Zugang zu öffentlichen und privaten Diensten zu ermöglichen“ (Ewgr. 30; weitere Anforderungen siehe Ewgr. 31 ff.).

* EU-VO 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, ABl. L vom 30.04.2024

ZUKUNFTSFÄHIGKEIT DER EIDAS 2.0 REGELUNGEN* (3)

Photo by jasper benning on Unsplash

- Schon durch eIDAS 1.0 Verpflichtungen zur Anerkennung elektronischer Identitäten (nach Notifizierung), es **fehlt aber Alltagsrelevanz** zur Nutzung im privatwirtschaftlichen Kontext.
- Wallet soll Ende 2026 verfügbar sein.
- Alle Mitgliedsstaaten sind dann zur Verfügungstellung einer Wallet zur gegenseitigen Anerkennung der Wallet verpflichtet, aber keine Verpflichtung der User.
- Neben der eID soll Wallet auch weitere Ausweise und weitere Attribute (RA-Eigenschaft) beinhalten; ferner Möglichkeiten zu digitalen Zahlungsfreigaben, Mietverträgen, Flugbuchungen, Autoanmietungen usw.
- EUDI-Wallet auch datenschutzkonform: Nutzer entscheidet selbst, an wen und in welchem Umfang personalisierte Daten weitergegeben werden.

* EU-VO 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, ABl. L vom 30.04.2024

ZUKUNFTSFÄHIGKEIT- ? EIDAS 2.0 REGELUNGEN* (4)

Photo by jasper benning on Unsplash

In vier **EU- Large Scale Pilots** werden Anwendungsszenarien durchgetestet, z.B. :

- Zugang zu staatlichen Diensten (etwa Beantragung eines Führerscheins, Steuerwesen),
- Eröffnung eines Bankkontos,
- SIM-Registrierung,
- Speicherung und Präsentation des mobilen Führerscheins,
- Unterzeichnung von Verträgen durch Erstellung sicherer digitaler Signaturen,
- Rezepte für Apotheken,
- Reisedokumente (z. B. Reisepass, Visum),
- digitale Identitäten für Unternehmen mit Ausweis der Vertreterfunktion,
- Zahlungen: Überprüfung der Identität eines Benutzers beim Beginn einer Online-Zahlung,
- Bildungsnachweise,
- Zugang zu Sozialversicherungsleistungen.

* EU-VO 2024/1183 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, ABl. L vom 30.04.2024

NUTZUNG ELSTER VS. EUDI- WALLET:

ELSTER

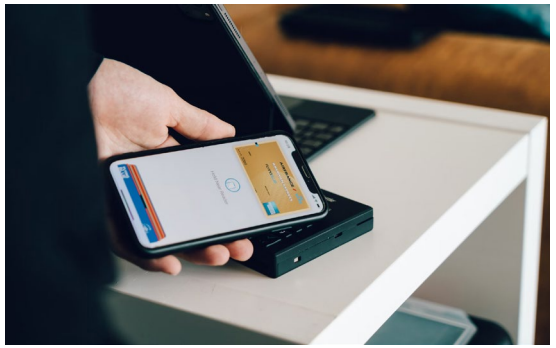


Foto von CardMapr.nl auf Unsplash

- **Grenzüberschreitende Anerkennung** von Identifizierungen im Rahmen der Wallet nur bei „starker Identifizierung“ (nicht bei ELSTER gegeben), also bei 2-Faktor Authentifizierung. Elster Zertifikat auf andere Geräte kopierbar, also keine starke Authentifizierung.
- ELSTER als Identifizierung **nicht** für Anwendungen mit **Vertrauensniveau „hoch“** nutzbar.
- ELSTER- Einsatz in **deutschem Steuersystem** entstanden, das nicht auf andere Systeme ausgerichtet war. In geschlossenem Ökosystem (Steuer) sinnvoll, aber wohl nicht in der gesamten Justiz.
- **Bisherige Identifizierungsinstrumente** für wesentliche Justizkommunikation erfüllen Kriterium des **Vertrauensniveaus „hoch“**. Fraglich, ob es sich lohnt, für einzelne Justizanwendungen (Terminanfragen etc) spezifisches Instrument (ELSTER) zu regeln.
- ELSTER zwar **übergangsweise für Unternehmen/Oranistationen sinnvoll**, da weit verbreitet und z.B. Unternehmen zur elektronischen Steuererklärung verpflichtet sind, insoweit Unternehmen über Nutzerkonto Identifizierungsinstrument zur Kommunikation mit Verwaltung und Justiz nutzen können, das bereits in ähnlichem Zusammenhang genutzt wird.
- Gerade die flächendeckende (und wohl auch dann sehr leichte, da vom Smartphone aus direkt nutzbare) Identifizierung mit EUDI-Wallet wird angesichts der Einbettung in umfassendes eID-Ökosystem den Anwendungskomfort von ELSTER wohl übertreffen.

Photo by Jen Theodore on Unsplash

SCHLUSSFOLGERUNGEN (THESEN)

- ✓ ELSTER für die Justizkommunikation der **Unternehmen/Organisationen** über das Portalnutzerkonto **noch** akzeptabel.
- ✓ Zwar leidet digitale Justizkommunikation in D derzeit oft an Defiziten im Anwendungskomfort (es fehlt Einfachheit).
- ✓ IT Sicherheit in der Justizkommunikation aber entscheidender Vertrauensfaktor.
- ✓ Für Bürgerinnen und Bürger, die an Identifizierung via AusweisApp gewöhnt sind, bringt ELSTER keine Verbesserungen, da AusweisApp sicherer und nicht weniger komfortabel als ELSTER.
- ✓ Vor einigen Jahren wäre ELSTER auch für Bürgerkommunikation mit Justiz evtl. als Übergangstechnologie sinnvoll gewesen, nun angesichts der bevorstehenden EUDI-Wallet nicht mehr.
- ✓ EUDI-Wallet wird aufgrund ihrer vielseitigen Einsatzmöglichkeiten und ihrer grenzüberschreitenden Anerkennung auf größere Akzeptanz stoßen.
- ✓ EUDI-Wallet sollte zukünftig auch für Justizkommunikation einsetzbar sein, evtl. auch Kommunikation über besondere elektronische Postfächer ersetzen.
- ✓ eID-Ökosysteme sollten bereits heute an zukünftig geltenden europarechtlichen Vorgaben ausgerichtet werden, um nachhaltige Lösungen zu schaffen.

Vielen Dank für die Aufmerksamkeit!

FRAGEN/ANMERKUNGEN?

PROF. DR. WILFRIED BERNHARDT

bernhardt.gmbh@t-online.de

Rechtsanwalt und Of Counsel bei Büsing, Müffelmann & Theye, Berlin
Geschäftsführer Bernhardt IT Management Consulting GmbH
Honorarprofessor für IT-Recht, insbesondere E-Government und E-Justice an der Juristenfakultät der Universität Leipzig

Weitere Fragen zur eiDAS 2.0
und zur EUDI Wallet:
AK Europa auf dem EDVGT am
13. 9. 2024 11h bis 12:30h