



Stellungnahme

der Deutschen Rentenversicherung Bund

vom 14.04.2026

zum

Referentenentwurf
des Bundesministeriums für Digitales und Staatsmoderni-
sierung

Entwurf eines Gesetzes über die Europäische Briefftasche
für die Digitale Identität und zur Änderung anderer Rechts-
vorschriften

(Digitale Identitätengesetz – DIdG)

Bearbeitungsstand: 26.03.2026

A. Einleitung

Der vorliegende Referentenentwurf eines Gesetzes über die Europäische Brieftasche für die Digitale Identität und zur Änderung anderer Rechtsvorschriften (Digitale Identitätengesetz – DIdG) dient der nationalen Umsetzung der europäischen eIDAS-Verordnung ((EU) Nr. 910/2014 in der Fassung der Verordnung (EU) 2024/1183). Ihr Ziel ist es, sichere, vertrauenswürdige und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen grenzüberschreitend in ganz Europa zu ermöglichen. Kern der Verordnung ist ein unmittelbar geltender Rechtsrahmen für die Europäische Brieftasche für die Digitale Identität. Diese sogenannte EUDI-Wallet ist ein elektronisches Identifikationsmittel, das es dem Nutzer ermöglichen soll, Personenidentifizierungsdaten und elektronische Attributsbescheinigungen sicher zu speichern, zu verwalten und zu validieren, um sie vertrauenden Beteiligten und anderen Nutzern der Europäischen Brieftasche präsentieren und mittels qualifizierter elektronischer Signaturen unterzeichnen oder mittels qualifizierter elektronischer Siegel besiegeln zu lassen. Die Nutzung der EUDI-Wallet ist für die Bürgerinnen und Bürger freiwillig. Andere Identifizierungs- und Authentifizierungsmittel bleiben erhalten und können den Bürgerinnen und Bürgern auch weiterhin angeboten und von diesen genutzt werden. Der vorliegende Referentenentwurf konkretisiert die genannten europarechtlichen Vorgaben im Hinblick auf Zuständigkeiten, die Ausgestaltung von Rechtsgrundlagen und die Anpassung nationaler Regelungen.

B. Wesentliche Inhalte des Gesetzentwurfs

Das vorliegende Gesetzgebungsvorhaben verfolgt das Ziel, den elektronischen Rechts- und Wirtschaftsverkehr für Bürgerinnen und Bürger sowie Unternehmen deutlich zu vereinfachen. Neben einer europaweit verwendbaren digitalen Identität werden hierzu elektronische Signatur- und Siegelfunktionen sowie der Einsatz von elektronischen Nachweisen (Attributen) eingeführt. Die EUDI-Wallet soll dabei einen vereinfachten Zugang zu öffentlichen und privaten Dienstleistungen auf hohem Sicherheitsniveau ermöglichen und trägt damit ganz wesentlich dazu bei, die im Rahmen des Onlinezugangsgesetzes (OZG) verfolgte Verwaltungsmodernisierung zu fördern. Die Deutsche Rentenversicherung Bund (DRV Bund) unterstützt dieses Vorhaben. Der Referentenentwurf stellt hierfür einen wichtigen und richtigen ersten Schritt dar. Für eine tragfähige Umsetzung in der Verwaltungspraxis bedarf es jedoch weiterer fachlicher, technischer und organisatorischer Konkretisierungen sowie Änderungen am vorliegenden Gesetzentwurf. Dies betrifft insbesondere die interoperable Einbindung in bestehende Fachverfahren, die verlässliche Verarbeitung und Nutzung elektronischer Attributsbescheinigungen sowie den Umgang mit Fällen, in denen das attributbasierte Identity-

Matching für eine eindeutige fachliche Zuordnung nicht ausreicht. Insoweit sollten ergänzende, datenschutzkonforme und interoperable Mechanismen vorgesehen beziehungsweise weiter konkretisiert werden, insbesondere durch die Möglichkeit, bestehende Identifikatoren (z. B. die IDNr nach dem IDNrG) in geeigneter Form – etwa im Rahmen ergänzender elektronischer Attributsbescheinigungen – einzubinden und datenschutzkonform zu verarbeiten, um die praktische Nutzbarkeit der EUDI-Wallet für komplexe Verwaltungsverfahren nachhaltig sicherzustellen. Dabei betrifft die im Referentenentwurf geregelte Verpflichtung zur Ausstellung von elektronischen Attributsbescheinigungen allerdings lediglich die Bundesträger der Deutschen Rentenversicherung, d.h. die DRV Bund und die Deutsche Rentenversicherung Knappschaft-Bahn-See, nicht aber die 14 regionalen Rentenversicherungsträger.

C. Allgemeine Anmerkungen

Ausgangslage

Klassische IT-Authentifizierungsverfahren erzeugen innerhalb eines Systems eine digitale Identität, ordnen dieser entsprechende Berechtigungen (Autorisierung) zu und ermöglichen dem Nutzenden, diese Identität durch die Übermittlung bekannter Zugangsdaten (z. B. Benutzername und Passwort) nachzuweisen (Authentifizierung). Mit der Einführung der EUDI-Wallet wird dieses Paradigma teilweise aufgelöst. Die Identität wird nicht mehr im Fachverfahren erzeugt, sondern vom Nutzenden über die Übermittlung einer extern (beispielsweise durch die Bundesdruckerei) ausgestellten und signierten Personenidentität (PID) nachgewiesen. Die PID enthält dabei eine Vielzahl an Attributen, die vom Fachverfahren verarbeitet werden müssen, um eine Zuordnung zu einer bestehenden fachlichen Identität (z. B. einer Versicherungsnummer im Rentensystem) zu ermöglichen. Dieses attributbasierte Identity-Matching stellt dabei den vorgesehenen Regelfall dar. Eine eindeutige Zuordnung in einem Fachverfahren ist allein auf Basis der PID nicht zuverlässig möglich. Die PID ist dabei nicht als organisationsübergreifender, eineindeutiger Personenidentifizierer konzipiert, sondern als datenschutzfreundliches Identifikationsmittel zur situationsbezogenen Authentifizierung. Dieser Ansatz ist Ausdruck des europäischen Paradigmenwechsels hin zu einer kontextbezogenen und datenschutzfreundlichen digitalen Identität. Für eine Vielzahl von Verwaltungsleistungen sowie organisations- und perspektivisch mitgliedstaatenübergreifenden Anwendungsszenarien besteht jedoch fachlich die Anforderung, wiederkehrende Nutzerinnen und Nutzer eindeutig identifizieren und zuordnen zu können. Dies betrifft insbesondere Sachverhalte, bei denen Bescheide, Datenbestände, Versicherungsverläufe oder Rechtsverhältnisse eindeutig einer Person zugeordnet werden müssen. Ein solcher eineindeutiger Identifizierer ist, insbesondere in der deutschen PID, derzeit jedoch nicht vorgesehen. Die in der deutschen PID ent-

haltenen Attribute sind aus der Online-Ausweisfunktion des Personalausweises (eID) abgeleitet und damit strukturell auf den dort verfügbaren und freigegebenen Attributraum begrenzt. Diese helfen, dass sich Nutzerinnen und Nutzer digital eindeutig identifizieren können, sie sind aber nicht für eine Authentifizierung in Verwaltungsverfahren bestimmt. Gerade potenziell eineindeutige optionale Merkmale, wie bspw. die `personal_administrative_number`, sind im deutschen PID-Profil nicht verfügbar; auch unionsweit kann nicht davon ausgegangen werden, dass vergleichbare optionale Merkmale konsistent bereitgestellt werden. Eine verlässliche eindeutige Identitätszuordnung ist damit herausfordernd. Diese Identitätszuordnung wird zusätzlich dadurch verschärft, dass sich personenbezogene Attribute im Zeitverlauf ändern können (z. B. Nachname, Geschlecht). Eine eindeutige Zuordnung auf Basis dieser Attribute wird dann nicht mehr (zuverlässig) gelingen.

Technische Hinweise

Da die deutsche PID selbst keinen eineindeutigen Identifier enthält und dieser weder zuverlässig aus den garantierten Attributen abgeleitet noch aus der digitalen Signatur gewonnen werden kann, besteht aus technischer Sicht die Notwendigkeit, Mechanismen zur stabilen Wiedererkennung und Identitätszuordnung zu betrachten. Für Anwendungsszenarien, in denen eine eindeutige Zuordnung auf Basis von Attributen nicht hinreichend zuverlässig möglich ist, – wie z.B. in Fachverfahren der Verwaltung – wären deshalb ergänzende Ansätze erforderlich. Unterstützende Mechanismen zur Wiedererkennung innerhalb eines einzelnen Dienstes (zum Beispiel: Pairwise Pseudonymous Identifiers, PPID) könnten hierzu beitragen, sind jedoch auf Szenarien mit bereits erfolgter fachlicher Zuordnung beschränkt und für die initiale Identitätsbestimmung sowie organisationsübergreifende Anwendungsszenarien nicht ausreichend. Für entsprechende Anwendungsszenarien könnten deshalb ergänzende Ansätze in Betracht kommen, etwa in Form zusätzlicher elektronischer Attributsbescheinigungen („Secondary Credentials“), die eine eindeutige fachliche Referenz (z. B. eine sektorale Identifikationsnummer) enthalten. Diese wären dabei nicht als Ersatz, sondern als kontextbezogene Ergänzung zum attributbasierten Identity-Matching zu verstehen und könnten auf bestehenden sektoralen Identifikatoren (z. B. Sozialversicherungsnummern oder anderen geeigneten Registerkennungen) basieren. Dabei ist jedoch zu berücksichtigen, dass isolierte, dienstspezifische Lösungen zu einer Fragmentierung führen würden. Eine Vielzahl voneinander unabhängiger Secondary Credentials unterschiedlicher Dienste würde allerdings die Interoperabilität erheblich erschweren und den Nutzen für Anwender sowie Diensteanbieter reduzieren. Vor diesem Hintergrund besteht nach Einschätzung der DRV Bund Bedarf für eine koordinierte, idealerweise europäische Abstimmung zur Ausgestaltung und Anerkennung solcher ergänzenden Nachweise. In diesem Zusammenhang wäre auch die Frage zu klären, welche vertrauenswürdigen Stellen zur initialen Ausstellung eines solchen Credentials befugt

sind und wie ein initialer Identitätsabgleich erfolgen kann.

Fazit

Die dargestellten Überlegungen und technischen Ansätze verdeutlichen, dass im Bereich der Wiedererkennung und des Identity Mappings innerhalb des EUDI-Wallet-Ökosystems derzeit noch weiterer Klärungs-, Abstimmungs- und vor allem noch ein deutlicher Handlungsbedarf besteht. Insbesondere zeigt sich, dass unterschiedliche Mechanismen jeweils nur Teilaspekte adressieren und eine konsistente, interoperable Gesamtlösung für organisations- und mitgliedstaatenübergreifende Anwendungsszenarien noch weiter zu konkretisieren ist.

Aus Sicht der DRV Bund ergeben sich folgende Anforderungen an die rechtliche und auch technische Ausgestaltung und Umsetzung für die EUDI-Wallet:

- Das attributbasierte Identity-Matching sollte als Regelfall vorgesehen werden und die Grundlage für die Identitätszuordnung in Fachverfahren darstellen.
- Für Anwendungsszenarien, in denen dieses Matching nicht ausreicht, müssten ergänzende, datenschutzkonforme und interoperable Mechanismen bereitgestellt werden, die eine stabile Wiedererkennung und eindeutige fachliche Zuordnung ermöglichen.
- Hierfür könnten insbesondere zusätzliche elektronische Attributsbescheinigungen („Secondary Credentials“) in Betracht kommen, die eine fachliche Referenz enthalten und kontextbezogen eingesetzt werden können.
- Diese Mechanismen sollten koordiniert und möglichst europaweit abgestimmt werden, um Fragmentierung zu vermeiden und Interoperabilität sicherzustellen.

Die dargestellten Ansätze stehen im Einklang mit den datenschutzrechtlichen Grundprinzipien der EUDI-Wallet, insbesondere der Datensouveränität der Nutzerinnen und Nutzer sowie der selektiven Offenlegung von Attributen (Selective Disclosure). Durch die gezielte und kontextbezogene Nutzung ergänzender elektronischer Attributsbescheinigungen könnte sichergestellt werden, dass jeweils nur die für den konkreten Anwendungsfall erforderlichen Informationen verarbeitet werden, ohne eine übermäßige Datenweitergabe zu erzeugen. Eine solche Ausgestaltung würde das Vertrauen in die Nutzung der EUDI-Wallet stärken und zugleich ermöglichen, fachlich anspruchsvolle Verwaltungsverfahren – wie im Bereich der Sozialversicherung – effizient, sicher und datenschutzkonform umzusetzen.

D. Zu den Regelungen im Einzelnen

Art. 1 § 9 EBDI-Gesetz-E (Personenidentifizierungsdaten)

Die in § 9 EBDI-Gesetz-E vorgesehene Regelung zu den PID adressiert, wie bereits eingangs ausgeführt, die Wiedererkennung von Nutzerinnen und Nutzern in Fachverfahren nicht ausreichend. Für die praktische Nutzung der EUDI-Wallet und der angeschlossenen Fachverfahren ist aber von zentraler Bedeutung, dass eine verlässliche und fachlich eindeutige Zuordnung von Nutzerinnen und Nutzern zu bestehenden Datenbeständen und Rechtsverhältnissen möglich ist. Aktuell fehlt eine eindeutige Vorgabe dazu, wie Personen beim erneuten Zugriff auf ein Fachverfahren, etwa über das Kundenportal der Deutschen Rentenversicherung, automatisch erkannt werden können, ohne den kompletten Registrierungsprozess erneut durchlaufen zu müssen.

Das attributbasierte Identity-Matching stellt den vorgesehenen Regelfall dar, ist jedoch insbesondere in komplexen fachlichen Szenarien nicht in allen Fällen ausreichend, um eine eindeutige Zuordnung sicherzustellen. Nach Artikel 11a Absatz 1 der eIDAS-Verordnung sind Mitgliedstaaten verpflichtet, einen Identitätsabgleich sicherzustellen. Gleichzeitig gilt ein Identity Matching nach Artikel 2 Absatz 7 der Durchführungsverordnung (EU) 2025/846 nur dann als erfolgreich, wenn eine eindeutige Zuordnung zu genau einer natürlichen Person möglich ist; bestehen Zweifel, ist das Matching als nicht erfolgreich zu bewerten. Vor dem Hintergrund der Haftungsregelung nach Artikel 11 eIDAS-Verordnung, wonach Mitgliedstaaten und beteiligte Stellen für fehlerhafte Identifizierungs- und Authentifizierungsprozesse haften, ist sicherzustellen, dass Identitätszuordnungen nur dann als eindeutig behandelt werden, wenn die hierfür unionsrechtlich definierten Anforderungen tatsächlich erfüllt sind. Die unionsrechtlichen Vorgaben sehen darüber hinaus vor, dass Personenidentifizierungsdaten durch zusätzliche, gegebenenfalls optionale Attribute so ausgestaltet werden sollen, dass eine eindeutige Zuordnung ermöglicht wird (vgl. Erwägungsgrund 12 der Durchführungsverordnung (EU) 2024/2977).

Aus Sicht der DRV Bund bestehen jedoch insbesondere im Hinblick auf den nationalen PID-Attributraum, der maßgeblich aus bestehenden Identitätsdaten (insbesondere aus dem eID-Kontext) abgeleitet wird, praktische Herausforderungen, in allen relevanten Anwendungsszenarien ein zweifelsfrei eindeutiges Matching sicherzustellen. Daher bedarf es, wie ausgeführt, ergänzender, datenschutzkonformer und interoperabler Mechanismen, die eine stabile Wiedererkennung und eindeutige fachliche Zuordnung ermöglichen, ohne den angesprochenen Paradigmenwechsel der eIDAS-Verordnung zu unterlaufen. Zugleich ist sicherzustellen, dass entsprechende Lösungsansätze benutzerfreundlich und effizient ausgestaltet sind und nur geringe zusätzliche Interaktion für die Nutzenden erfordern, sodass eine Verbesserung der Identitätszuordnung nicht mit Einbußen in der Usability einhergeht. In der praktischen Anwendung ist zudem zu berücksichtigen, dass bestimmte Personengruppen – insbesondere Drittstaatsangehörige – in der Regel nicht über eine elektronische Identität eines anderen Mitgliedstaates verfügen, obwohl gleichzeitig in vielen Verwaltungsvorfahren, insbesondere im Bereich der Sozialversicherung, regelmäßige Interaktionen mit dieser Personengruppe bestehen. Vor diesem Hintergrund sollte geprüft werden, inwieweit auch für diese Personengruppen ein Zugang zu Personenidentifizierungsdaten ermöglicht werden kann, um eine durchgängige Nutzung digitaler Verwaltungsleistungen sicherzustellen und entsprechende Nutzungslücken zu vermeiden. Dies betrifft insbesondere Fälle wie Rentenempfängerinnen und -empfänger mit Wohnsitz außerhalb der Europäischen Union, Drittstaatsangehörige mit Beschäftigungszeiten in Deutschland, die Rentenansprüche geltend machen, sowie sich rechtmäßig in Deutschland aufhaltende Personen, die Anträge auf Leistungen der sozialen Sicherung stellen oder mit den Trägern der Sozialversicherung in laufenden Verwaltungsvorfahren stehen (vgl. Art. 1, Art. 2 Abs. 1 sowie Art. 3 eIDAS-Verordnung ((EU) Nr. 910/2014 i. d. F. der Verordnung (EU) 2024/1183).

Wie bereits dargestellt könnten unterstützende Mechanismen zur Wiedererkennung innerhalb eines einzelnen Dienstes (zum Beispiel: PPID) hierzu beitragen, sind jedoch auf Szenarien mit bereits erfolgter fachlicher Zuordnung beschränkt und für die initiale Identitätsbestimmung sowie organisations- und mitgliedstaatenübergreifende Anwendungsszenarien nicht ausreichend. Für entsprechende Anwendungsszenarien könnten ergänzende Ansätze in Betracht kommen, etwa in Form zusätzlicher elektronischer Attributsbescheinigungen („Secondary Credentials“), die eine fachliche Referenz enthalten und eine eindeutige Zuordnung zu bestehenden Datenbeständen ermöglichen.

Der vorliegende Referentenentwurf sollte daher dahingehend konkretisiert werden, dass solche ergänzenden Mechanismen im Einklang mit den datenschutzrechtlichen Vorgaben vorgesehen werden, die interoperabel ausgestaltet werden können.

Art. 1 § 12 EBDI-Gesetz-E (Interoperabilität)

Die in § 12 EBDI-Gesetz-E vorgesehenen Regelungen zur Interoperabilität der EUDI-Wallet sind insbesondere aus Sicht des Prüfdienstes der DRV Bund für die Entwicklung im Bereich der Unternehmensanbindung von besonderer Bedeutung. Derzeit beschränkt sich das Angebot der DRV Bund im Rahmen ihrer Online-Agentur im Wesentlichen auf Privatperson bzw. Versicherte. Über diesen Kommunikationsweg wäre auch per EUDI-Wallet die Kontaktaufnahme von Einzelunternehmern und bei Rückfragen von Privatperson zu Statusfeststellungsverfahren im Kontext einer Betriebsprüfung denkbar. Ein erweitertes Serviceangebot für Arbeitgeber und für die steuerberatenden Berufe ist bislang nicht in vergleichbarer Weise vorhanden.

Die Einführung einer European Business Wallet (EUBW) könnte hier einen entscheidenden Fortschritt darstellen. Eine verlässliche digitale Identifikationslösung für Unternehmen würde die Grundlage dafür schaffen, Arbeitgeber eindeutig zu identifizieren und Verwaltungsprozesse, wie etwa die Zustellung von Bescheiden, vollständig digital und medienbruchfrei abzuwickeln. Voraussetzung hierfür ist jedoch, dass die Identifikationsmechanismen der EUBW mit bestehenden behördlichen Identifikationsmerkmalen interoperabel sind.

Derzeit ist nicht geregelt, ob eine Zuordnung zwischen einer natürlichen Person (EUDI-Wallet) und einem Unternehmen erforderlich ist oder Unternehmen unabhängig davon als eigenständige Einheiten registriert werden können.

Eine zentrale Rolle spielt dabei die bundeseinheitliche Wirtschaftsnummer für Unternehmen (beWiNr.). Diese wurde durch das Statistische Bundesamt (Destatis) zum Aufbau des Basisregisters für Unternehmen (BRU) als eineindeutiger, registerübergreifender Identifikator eingeführt und basiert auf der Wirtschafts-Identifikationsnummer (W-IdNr.). Die W-IdNr. wird gemäß § 139c Abgabenordnung vom Bundeszentralamt für Steuern (BZSt) vergeben. Diese Nummer eignet sich aus fachlicher Sicht besonders als eindeutiger Identifikator für Unternehmen.

Darüber hinaus bestehen im Bereich der Prüfdienste weitere Identifikationsmerkmale, insbesondere die Betriebsnummer. Hier fehlt bislang ein entsprechendes Mapping zu den künftigen Wallet-Strukturen. Dabei ist zu berücksichtigen, dass die Verarbeitung von betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, durch den Prüfdienst der Deutschen Rentenversicherung nach § 67 Absatz 2 SGB X eine Verarbeitung von Sozialdaten mit einem entsprechenden Schutzniveau erfordert.

Aus Sicht der DRV Bund ist es deshalb als kritisch zu bewerten, dass der Referentenentwurf zwar eine Registrierung von Unternehmen vorsieht, jedoch keine hinreichend konkrete Aussage dazu trifft, über welche Identifikationsmerkmale und Verfahren diese erfolgen soll. Hier besteht erheblicher Präzisionsbedarf. Denn es kann nicht zielführend sein, wenn jede Behörde verpflichtet wird, eine eigene Infrastruktur anzulegen und mit den eigenen Ordnungsmerkmalen zu mappen.

Aus Sicht der DRV Bund ist daher zwingend erforderlich, dass die EUBW an klare, bundeseinheitliche Identifikationsmerkmale geknüpft wird. Die Nutzung der durch das Basisregister für Unternehmen bereitgestellten beWiNr. erscheint hierbei als sachgerechte und zukunftsfähige Lösung. Nur auf dieser Grundlage kann ein effizienter, sicherer und interoperabler Datenaustausch zwischen Behörden gewährleistet werden.

Art. 1 § 16 EBDI-Gesetz-E (Elektronische Attributsbescheinigungen)

Die Verpflichtung aus § 16 EBDI-Gesetz-E erfasst seinem Wortlaut nach "Behörden des Bundes" und geht damit über die unmittelbare Bundesverwaltung hinaus, so dass auch die Bundesträger der Deutschen Rentenversicherung – die DRV Bund und die DRV Knappschaft Bahn See dem Anwendungsbereich der Norm unterliegen. Das ist problematisch, weil es zur Folge hätte, dass Ansprüche nur gegenüber diesen beiden Rentenversicherungsträgern geltend gemacht werden könnten, nicht aber gegenüber den 14 Regionalträgern, die 55 % des Versichertenbestandes der Deutschen Rentenversicherung repräsentieren.

Darüber hinaus bleibt der vorliegende Regelungsentwurf gänzlich vage hinsichtlich der konkreten Ausgestaltung und des Umfangs der behördlichen Verpflichtung, auf Verlangen des Antragsstellers Attributsbescheinigungen auszustellen. Es fehlt an einer konkreteren Ausgestaltung der Verpflichtung der Behörde im Hinblick auf das "Ob" und das "Wie" beim Einsatz und der Nutzung von Attributsbescheinigungen, d.h. in welchen Fällen ("Ob") und wenn ja, in welcher der drei Arten ("Wie") hat die Behörde "ausgestellte Entscheidungen und sonstige Dokumente auf Verlangen des Antragstellers als Attributsbescheinigungen auszustellen". Ebenso fehlt es an einer Regelung, inwieweit die vom Gesetz adressierten Behörden Verfahren und Prozesse entwickeln müssen, um die Akzeptanz von ausgestellten Attributsbescheinigungen zu prüfen und diese in den zugehörigen Fachverfahren weiterzuverarbeiten. Nicht zuletzt ist unklar, wie ein Widerruf oder eine Ungültigkeit von Attributen von Behörden erkannt werden kann, die das Attribut nutzen möchten oder nutzen müssen. Eine diesbezügliche Konkretisierung müsste deshalb vorgenommen werden.

Art. 1 § 21 EBDI-Gesetz-E (Experimentierklausel)

Eine Experimentierklausel zur Weiterentwicklung von Technik und Recht, etwa zur Automatisierung mit Künstlicher Intelligenz (KI) oder für neue, niedrighschwellige Methoden für die Bereitstellung von Services, die eine Verbreitung und gegebenenfalls die Nutzerakzeptanz der EUDI-Wallet erhöhen, ist sinnvoll und zu unterstützen.

E. Erfüllungsaufwand und Haushaltsmittel

Erfüllungsaufwände auf Seiten der Rentenversicherung sind in erster Linie hinsichtlich der §§ 15 und 16 EBDI-Gesetz-E zu erwarten. Dies betreäe sowohl die Bereitstellung der elektronischen Attributsbescheinigungen für den Nachweis der Sozialversicherungsnummer als auch die Anbindung an das NOOTS.

Die Kosten für Entwicklung und Betrieb der Verfahren im Bereich der Rentenversicherung können aber erst dann abgeschätzt werden, wenn endgültige Klarheit hinsichtlich der Ausgestaltung besteht und auch der technische Rahmen für das Format für die Attributsbescheinigungen feststeht. Darüber hinaus besteht nach dem vorliegenden Entwurf ein erhebliches und nicht bezifferbares Kostenrisiko dergestalt, dass § 16 EBDI-Gesetz-E nicht bestimmt, welche Dokumente Bürgerinnen und Bürger als elektronische Attributsbescheinigungen konkret verlangen können.

F. DigitalCheck

Im Rahmen der Bewertung des Referentenentwurfs wurde der DigitalCheck der DRV Bund durchgeführt. Die Ergebnisse des DigitalChecks sind in die Stellungnahme eingeflossen und sollen zu einer besseren digitalen Umsetzbarkeit beitragen. Auch aus Sicht des DigitalChecks ist die gesetzliche Regelung zur Umsetzung der europäischen Vorgaben zur EUDI-Wallet im Grundsatz sehr zu unterstützen. Die EUDI-Wallet kann als Katalysator des Once-Only Prinzip gesehen werden, auch über die Registernutzung hinaus. Vor einer gesetzlichen Regelung ist eine ausreichende inhaltliche Befassung – insbesondere zur Klärung der relevanten IT-Aspekte – erforderlich.