A-SIT Technology

E-Government Innovationszentrum

28. April 2025 Konzept · Digitale Identität · E-Government · 16 Min. Lesezeit

eIDAS Eingebettete Offenlegungsregelungen

Stefan More



Autorinnen und Autoren	Stefan More
Quelle	https://technology2.a-sit.at/veroeffentlichungen/eidas-eingebettete-offenlegungsregelungen/
Hinweis	Maschinell übersetzt.

Kernaussagen

- Eingebettete Offenlegungsregelungen (EDPs) sind maschinenlesbare Ausstellerregeln, die die Wallet bei jeder Präsentationsanfrage gegen die Relying Party prüft.
- Der Durchführungsrechtsakt nennt drei Regelungstypen: keine Regelung, nur autorisierte Relying Parties und spezifische Root of Trust.
- Ohne ausdrückliche Zustimmung darf die Wallet keine Daten an eine nicht zugelassene Partei senden; die Nutzenden werden über das Prüfergebnis informiert.
- Offen bleiben geringe Ausdrucksstärke, Interoperabilität, fehlender Widerruf ohne Neuausstellung und die Verwaltung der Roots.

- Der deutsche Ansatz tendiert zu bindender Durchsetzung; Registrierungszertifikate könnten künftig differenziertere Autorisierung ermöglichen.

Artikel 5a (Absatz 5e) der aktuellen eIDAS Regulierung („eIDAS 2“, 2024) führt sogenannte eingebetteten Offenlegungsregelungen („Embedded Disclosure Policies“) ein. Diese ermöglichen einem Aussteller (Issuer/Provider) von elektronischen Attributsbescheinigungen zu definieren, welche Service Anbieter auf das ausgestellte Dokument zugreifen dürfen.

Ein Beispiel ist ein elektronisches Credential mit personenbezogenen Attributen, auf welches der Zugriff nur für staatliche Behörden möglich sein soll. Diese Regelung/Policy wird maschinenlesbar encodet und an das Credential (die Attributsbescheinigung) eingebettet bzw angehängt, und von der Wallet Software kontrolliert.

Im Rahmen dieses Projektes wurde der Stand des eIDAS 2 Regelwerks und technischen Frameworks (ARF) betreffend eingebetteter Offenlegungsregelungen analysiert. Außerdem wurden weitere Möglichkeit über die geltenden Durchführungsrechtsakte und das derzeitige technische Framework hinausgehend untersucht.

1. Einleitung

Die digitale Landschaft in der Europäischen Union verändert sich grundlegend durch die Einführung des Europäischen Rahmens für eine digitale Identität (EUDI-Framework). Treiber ist vor allem die Verordnung (EU) Nr. 910/2014, bekannt als „eIDAS“ [1], und ihre Änderung von 2024 („eIDAS 2“) [2]. Die Verordnung soll das reibungslose Funktionieren des Binnenmarkts sicherstellen und ein angemessenes Sicherheitsniveau für elektronische Identifizierungsmittel und Vertrauensdienste in der gesamten Union gewährleisten. Ihr Ziel ist es, die sichere Teilnahme natürlicher und juristischer Personen an der digitalen Gesellschaft und ihren Zugang zu öffentlichen und privaten Online-Diensten in der gesamten EU zu ermöglichen und zu erleichtern. Ein Eckpfeiler dieses Rahmens ist die Europäische Brieftasche für die Digitale Identität (EUDI Wallet). Die EUDI Wallet ist ein elektronisches Identifizierungsmittel, mit dem Nutzende ihre Personenidentifizierungsdaten (PID) und elektronischen Attributsbescheinigungen (EAA) sicher speichern, verwalten und validieren können. Diese Daten können sie dann Relying Parties und anderen Wallet-Nutzenden vorlegen. Jeder EU-Mitgliedstaat ist verpflichtet, bis Dezember 2026 mindestens eine EUDI Wallet bereitzustellen.

Die EUDI Wallets sind ein wichtiger Fortschritt hin zu einem sicheren und interoperablen Ökosystem für digitale Identitäten in der gesamten Union. Sie stellen den Schutz personenbezogener Daten und der Privatsphäre in den Vordergrund und erleichtern zugleich den nahtlosen Zugang zu Diensten. EUDI Wallets sind nutzerzentriert gestaltet und geben Einzelpersonen die volle Kontrolle über ihre Attribute und ihre Privatsphäre. Nutzende erhalten transparente Informationen darüber, welche Attribute präsentiert werden und wem gegenüber. Maßnahmen verhindern das Tracking durch Relying Parties, PID-Provider oder Attestation Provider.

Ein zentrales Merkmal zur Stärkung von Privatsphäre und Kontrolle sind eingebettete Offenlegungsregelungen (Embedded Disclosure Policies, EDPs). Sie sind definiert als „ein Regelwerk, das von dem Anbieter in eine elektronische Attributsbescheinigung eingebettet wird und die Bedingungen angibt, die eine Wallet-nutzende Partei erfüllen muss, um auf die elektronische Attributsbescheinigung zuzugreifen“. In einfachen Worten: Embedded Disclosure Policies erlauben es Providern von Bescheinigungen festzulegen, welche Relying Party die Bescheinigung anfordern darf. Wallets müssen diese gängigen eingebetteten Offenlegungsregelungen dann verarbeiten und die Nutzenden über das Ergebnis informieren. So können Nutzende eine informierte Entscheidung treffen, die Präsentation der angeforderten Attribute zu genehmigen oder abzulehnen. Damit sind sie ein wesentlicher Bestandteil des EUDI-Frameworks, ermöglichen sensiblere Anwendungsfälle und erhöhen das Vertrauen der Nutzenden in das System.

2. Hintergrund

2.1. Gesetzgebung und Spezifikationsprozess

Das EUDI-Framework und der Mechanismus der Embedded Disclosure Policy werden durch mehrere Rechtstexte und technische Spezifikationen eingeführt und definiert:

1. Das EUDI-Framework wird durch die geänderte eIDAS-Verordnung eingeführt, die von der Europäischen Kommission vorgeschlagen und vom Europäischen Parlament gemeinsam mit dem Rat der EU als Vertretung der Mitgliedstaaten angenommen wurde [2].

2. Die Umsetzung des EUDI-Frameworks wird durch einen strukturierten Prozess mit Durchführungsverordnungen der Kommission (Commission Implementing Regulations, CIRs), auch Durchführungsrechtsakte (Implementing Acts, IAs) genannt, unterstützt. Sie klären die technischen Details, die die eIDAS-Verordnung offenlässt [3].

3. Die Architecture and Reference Framework (ARF) entwickelt die Konzepte und Spezifikationen auf Grundlage dieser Rechtstexte weiter. Sie dient als Referenz für eine einheitliche Umsetzung und definiert technische Spezifikationen, Standards und Verfahren [4].

4. CIRs und ARF stützen sich gemeinsam außerdem auf bestehende und etablierte technische Standards und Spezifikationen. Das erhöht die Übernahmefähigkeit und die Verlässlichkeit des Frameworks.

2.2. eIDAS EUDI Architecture & Trust Model

Das EUDI-Wallet-Ökosystem umfasst mehrere zentrale Rollen:

- Nutzende, die ihre Wallet Units kontrollieren, um Bescheinigungen zu empfangen, zu speichern, zu verwalten und zu präsentieren
- Person Identification Data (PID) Provider und Attestation Provider, die digitale Bescheinigungen an Nutzende ausstellen. Als Teil dieser Bescheinigungen erstellen und betten die Provider Offenlegungsregelungen ein.
- Relying Parties (RP), die diese Attribute von Wallets anfordern und die resultierende Präsentation der Attribute verarbeiten. Eine RP ist ein öffentlicher oder privater Dienst, der sich zur Authentifizierung oder Attributsprüfung auf die Wallet stützt. RPs müssen sich im europäischen oder nationalen

Register registrieren, ein Wallet-Relying-Party-Access-Zertifikat (ein eIDAS-2-Konzept) erhalten und optional ein Registrierungszertifikat, das angibt, welche Attribute sie anfordern wollen. Diese Zertifikate (von benannten nationalen Zertifizierungsstellen signiert) legen die Identität und den erklärten Zweck der RP fest. Bei der Verarbeitung einer Präsentationsanfrage prüft eine Wallet die entsprechenden Bescheinigungen und entscheidet, ob die RP berechtigt ist, die Bescheinigung anzufordern.

Die Interaktionen laufen im Wesentlichen in zwei Abläufen ab: der Ausstellung von Attributen an die Wallet und der Präsentation von Attributen durch die Wallet gegenüber einer Relying Party. Um Vertrauen in den Provider (Issuer) einer Bescheinigung herzustellen, prüft die Wallet die eIDAS-Vertrauensstatusliste (Trusted List).

Diese Beziehungen zeigt auch Abbildung 1. Das Diagramm stellt die Kernentitäten und Abläufe dar. Die Wallet Unit auf dem Gerät der Nutzenden interagiert rechts mit Relying-Party-Diensten und links mit Identity-(PID-)/Attribute-(Attestation-)Providern. PID- und Attestation Provider erscheinen in nationalen Trust Lists zertifizierter Aussteller. Relying-Party-CAs erscheinen in einer nationalen RP Trusted List und verwenden Access- und Registrierungszertifikate, um sich gegenüber der Wallet zu authentifizieren [6, 7]. Die Abbildung hebt auch Standardschnittstellen hervor: z. B. OIDC4VP für die Präsentation und Standard-Credential-Formate (W3C VC) [8, 9]. In der Praxis prüft eine Wallet Signaturen anhand von Trust Lists: Um etwa eine RP zu authentifizieren, prüft sie, ob das Access-Zertifikat der RP auf ein vertrauenswürdiges Root-Zertifikat in der RP Access CA Trust List zurückführt.

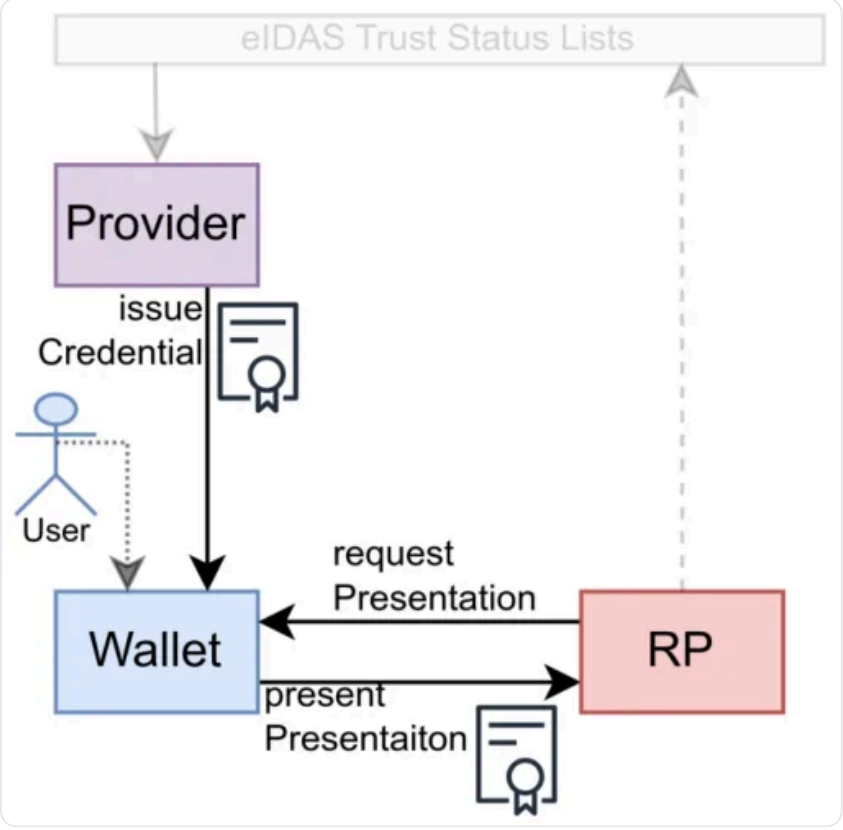


Abbildung 1: (Vereinfachte) EUDI-Architektur mit Fokus auf Ausstellung und Verifikation von Bescheinigungen

3. (Eingebettete) Offenlegungsregelungen

3.1. Definition

Embedded Disclosure Policies (EDPs) sind maschinenlesbare Regeln, die der Attribut-Provider in eine Electronic Attestation of Attributes (EAA) einbettet. Diese Regeln legen fest, unter welchen Bedingungen und von welchen Relying Parties (RPs) die Bescheinigung abgerufen und verarbeitet werden darf. Die EUDI Wallet muss diese Regelungen bei jeder Präsentationsanfrage auswerten. So ist sichergestellt, dass die RP gemäß der eingebetteten Regelung berechtigt ist, bevor Nutzerdaten offengelegt werden. Anders gesagt: Wenn ein Attestation Provider eine EAA (ein Credential mit Nutzerattributen) ausstellt, kann er ein Policy-Objekt einfügen, das besagt: „Nur diese RPs (oder RPs mit diesen Zertifikaten) dürfen dieses Credential erhalten." Damit soll verhindert werden, dass Nutzerattribute an unberechtigte oder ungeeignete Parteien weitergegeben werden. Dieser Mechanismus stärkt die Privatsphäre der Nutzenden und gibt Ausstellern Kontrolle darüber, wie ihre Credentials nachgelagert verwendet werden dürfen.

3.1.1. Rechtlicher Rahmen

Die Grundlage für Embedded Disclosure Policies wird in Artikel 5a der eIDAS-Verordnung [2] eingeführt. Dort ist festgelegt, dass EUDI Wallets im Fall der elektronischen Attributsbescheinigung mit eingebetteten Offenlegungsregelungen den geeigneten Mechanismus implementieren, um die Nutzenden darüber zu informieren, dass die Relying Party oder die nutzende Person der Europäischen Brieftasche für die Digitale Identität, die diese elektronische Attributsbescheinigung anfordert, die Berechtigung für den Zugriff auf diese Bescheinigung hat; [2, Artikel 5a (5) (e)] Die zugehörigen Durchführungsrechtsakte [3] legen weiter fest, dass eingebettete Offenlegungsregelungen die Wallet-Nutzenden vor unangemessener oder unrechtmäßiger Offenlegung von Attributen aus elektronischen Attributsbescheinigungen warnen sollen.

Wallet-Instanzen müssen prüfen, ob die Wallet-Relying-Party die Anforderungen der eingebetteten Offenlegungsregelung erfüllt, und die Wallet-Nutzenden über das Ergebnis informieren [3, Artikel 10].

Anhang III der Durchführungsverordnung (EU) 2024/2979 der Kommission [3, Anhang III] nennt die folgenden gängigen eingebetteten Offenlegungsregelungen, die unterstützt werden müssen (Stand April 2025):

- 'No policy': Gibt an, dass für die elektronischen Attributsbescheinigungen keine Regelung gilt und jede Relying Party sie anfordern kann.
- 'Authorized relying parties only policy': Legt fest, dass Wallet-Nutzende elektronische Attributsbescheinigungen nur gegenüber authentifizierten Relying Parties offenlegen dürfen, die in den Offenlegungsregelungen ausdrücklich aufgeführt sind.
- 'Specific root of trust': Diese Option ist eine flexiblere Alternative. Sie gibt an, dass Wallet-Nutzende die jeweilige elektronische Attributsbescheinigung nur gegenüber authentifizierten Wallet-Relying-Parties offenlegen sollen, deren Access-Zertifikate von einem bestimmten Root-Zertifikat oder einer Liste bestimmter Root- oder Zwischenzertifikate abgeleitet sind. Damit kann der Provider die Verwendung der Bescheinigung z. B. auf einen bestimmten Sektor (z. B. Gesundheit, Bildung) oder ein bestimmtes Unternehmen (z. B. eine bestimmte Firma) beschränken.

In allen Fällen darf die Wallet eine Regelung nicht ohne ausdrückliche Zustimmung der Nutzenden übergehen, um Daten an eine nicht zugelassene Partei zu senden. Ist keine Regelung eingebettet, gilt standardmäßig uneingeschränktes Teilen (nur vorbehaltlich der Zustimmung der Nutzenden). Diese Vorlagen sind bewusst einfach gehalten: Jede Regelung ist entweder eine Allow-List von RPs oder eine Allow-List von Roots. Die ARF stellt klar, dass Wallets die Unterstützung für die Regelungen „authorized RPs“ und „root of trust“ implementieren müssen und die Listen in Kombination mit den Daten der RP verarbeiten.

3.1.2. Technischer Rahmen

In der EUDI Architecture and Reference Framework (ARF) werden Embedded Disclosure Policies als Teil des Credential-Lebenszyklus und des Interaktionsmodells zwischen Wallet und RP behandelt. Aus technischer Sicht besteht die Durchsetzung von EDPs aus mehreren Schritten:

1. Policy Embedding: Während der Ausstellung fügt der Provider die relevante Offenlegungsregelung in einem standardisierten Format als strukturiertes und signiertes Element in die Bescheinigung ein.

2. RP Authentication & Certificate Evaluation: Bei einer Präsentationsanfrage authentifiziert die Wallet die RP und extrahiert deren Metadaten, einschließlich ihrer Zertifikatskette oder ihres Access-Tokens. Die Wallet muss außerdem prüfen, ob das Access-Zertifikat der RP (über Trust Lists) auf ein vertrauenswürdiges Root-Zertifikat zurückführt 3. Policy Evaluation Engine: Die Disclosure-Policy-Engine der Wallet wertet die Identität der RP anhand der eingebetteten Regeln aus. Sie prüft zum Beispiel, ob das Zertifikat der RP einem Eintrag auf einer Allow-List entspricht oder ob es auf ein zulässiges Root-Zertifikat zurückführt.

a. Bei einer Regelung „authorized RPs only“ wird geprüft, ob die Kennung der RP in der Liste erscheint.

b. Bei einer Regelung „root of trust“ wird geprüft, ob die Zertifikatskette der RP eines der zulässigen Roots enthält.

4. User Notification and Consent: Ist die RP berechtigt, legt die Wallet den Nutzenden die Offenlegungsanfrage vor, einschließlich regelbasierter Informationen (z. B. „Diese Bescheinigung darf nur an autorisierte Anbieter aus dem Gesundheitssektor weitergegeben werden“). Die Nutzenden können die Anfrage dann genehmigen oder ablehnen.

5. Presentation and Logging: Nach der Genehmigung wird das Attribut im Rahmen einer Präsentation offengelegt. Die Aktion wird gemäß den eIDAS-Anforderungen an Transparenz und Prüfbarkeit zur Nachvollziehbarkeit protokolliert.

In der Praxis laufen diese Prüfungen automatisiert in der Wallet-Software ab. Artikel 10 der CIR 2024/2979 schreibt vor, dass „Wallet-Instanzen prüfen, ob die Wallet-Relying-Party die Anforderungen der [EDP] erfüllt, und die Wallet-Nutzenden über das Ergebnis informieren“ [3]. Die ARF führt aus, dass die Wallet bei einer fehlgeschlagenen Regelprüfung die Transaktion entweder abbrechen oder den Nutzenden eine Warnung anzeigen soll. Die Durchsetzung von EDPs ist also ein Laufzeitschritt im Präsentationsablauf der Wallet.

EDPs sind bewusst ausstellerzentriert: Der Attestation Provider (z. B. ein Unternehmen oder eine Behörde) legt die Regelung fest, und die Wallet setzt sie durch. Das unterscheidet sich von typischen Self-Sovereign-Identity-Modellen, in denen allein die Zustimmung der Nutzenden und die Attributauswahl die Offenlegung

steuern. Hier fügt der Aussteller eine zusätzliche Kontrollebene hinzu.

4. Diskussion & Ausblick

Auch wenn es keine technische Einschränkung ist, kann das Einbetten einer Regelung die User Experience beeinträchtigen. Wallets müssen klare Meldungen anzeigen, wenn eine Regelung die Offenlegung blockiert. Erwägungsgrund 8 der Verordnung fordert ausdrücklich „angemessene Warnungen“ [2]. Intuitive Hinweise (z. B. „Ihr Führerschein kann nicht geteilt werden, weil diese App nicht auf der Liste zugelassener Apps steht“) sind für das Vertrauen der Nutzenden wichtig. Sind Regelungen zu streng oder zu undurchsichtig, könnten Nutzende oder Relying Parties Umgehungen suchen oder verwirrt sein.

4.1. Einschränkungen

Die derzeitigen rechtlichen und technischen Rahmenwerke definieren zwar grundlegende Fähigkeiten für Offenlegungsregelungen, doch es bleiben mehrere Herausforderungen:

- Ausdrucksstärke: Die aktuellen gängigen Regelungen decken grundlegende Zugriffskontrollszenarien ab, unterstützen aber möglicherweise keine komplexe Regellogik, etwa zeitliche Einschränkungen oder Kontextbedingungen (z. B. „nur wenn sich die nutzende Person an einem bestimmten Ort befindet“) [5].
- Interoperabilität: Unterschiedliche Credential-Formate und kryptografische Infrastrukturen zwischen Sektoren oder Mitgliedstaaten können eine einheitliche Durchsetzung der Regelungen erschweren.
- Widerruf & Regelaktualisierungen: Ist eine Bescheinigung einmal mit einer eingebetteten Regelung ausgestellt, ist es technisch schwierig, diese Regelung ohne erneute Ausstellung des Credentials zu aktualisieren oder zu widerrufen. Die ARF behandelt das noch nicht vollständig.
- Trust Bootstrapping: Die Verwaltung „spezifischer Roots“ erfordert robuste Governance-Mechanismen für Vertrauensanker. Es bleibt unklar, wie diese Roots in verschiedenen Mitgliedstaaten und Sektoren registriert, verteilt und gepflegt werden.

4.2. Deutsches „Architekturkonzept“ und Durchsetzung von Regelungen

Das deutsche Bundesministerium des Innern (BMI) hat ein nationales Architekturkonzept für die Umsetzung der EUDI Wallet veröffentlicht. Es führt aus, wie eingebettete Offenlegungsregelungen (EDPs) in der Praxis verwaltet und durchgesetzt werden können.

Eine zentrale Diskussion im deutschen Kontext betrifft die Frage, ob eingebettete Offenlegungsregelungen als harte Beschränkungen (unabhängig vom Kontext durchgesetzt) oder als beratende Hinweise (die informieren, aber keine Durchsetzung vorschreiben) ausgelegt werden sollen. Der deutsche Ansatz tendiert zu einem strikten Durchsetzungsmodell: Vom Aussteller eingebettete Regelungen sind bindend, und Wallets müssen die Offenlegung von Credentials an nicht berechtigte Parteien ausnahmslos verweigern. Diese Strenge soll Rechtskonformität und Schutz der Nutzenden sicherstellen, wirft aber Fragen zur Flexibilität der Regelungen und zu Aktualisierungsmechanismen auf.

Außerdem zeigt die deutsche Umsetzung Lücken bei Widerrufs- und Aktualisierungsverfahren für EDPs auf. Da EDPs nach der Ausstellung eines Credentials statisch sind, erfordert jede Änderung der Zugriffsberechtigungen eine vollständige Neuausstellung. Deutsche Stakeholder haben vorgeschlagen,

dass künftige Versionen der ARF Hooks für Endpunkte zum Widerruf von Regelungen oder dynamische Evaluations-APIs enthalten. Diese könnten mehr Anpassungsfähigkeit bringen, ohne die Absicht des Ausstellers zu beeinträchtigen.

5. Weitere Authentifizierungs- und Autorisierungsmechanismen

Embedded Disclosure Policies bieten Attestation Providern einen flexiblen Mechanismus, um den Zugriff auf die von ihnen ausgestellten Daten zu kontrollieren. Dazu stützen sie sich auf Authentifizierungsinformationen der Relying Party (RP). In eIDAS werden diese Authentifizierungsinformationen in Form von Zertifikaten an Relying Parties ausgegeben [2, 6]. Diese Zertifikate werden von Registrierungsstellen ausgestellt, die den Zugang zum eIDAS-Ökosystem kontrollieren. Sie stellen Zertifikate erst nach Prüfung der rechtlichen Identität der RP und Registrierung der Dienste der RP aus.

eIDAS 2 legt zwei Arten von Relying-Party-Zertifikaten fest [6, 7]:

- Relying Party Access Certificate: Dient dazu, einer RP Zugang zum eIDAS-Ökosystem zu gewähren und diese RP gegenüber Wallets zu authentifizieren. Enthält grundlegende Identitätsinformationen über die RP, die den Wallet-Nutzenden angezeigt werden und von einer eingebetteten Offenlegungsregelung verwendet werden können.
- Relying Party Registration Certificate: Der zweite Autorisierungsmechanismus neben den eingebetteten Offenlegungsregelungen. Definiert in maschinenlesbarer Form eine Menge von Attributen oder Bescheinigungen, die eine RP anfordern darf. Anhand dieser Informationen kann eine Wallet prüfen, ob die RP einen Anwendungsfall bzw. Dienst registriert hat, der die Anfrage nach der Bescheinigung rechtfertigt. Ein Dienst, der nur die Prüfung benötigt, ob das Alter der nutzenden Person über 18 liegt, gibt der RP zum Beispiel nicht die Berechtigung, andere Daten (oder auch nur das Geburtsdatum) anzufordern. Im aktuellen IA-Zyklus ist die Ausstellung von Registrierungszertifikaten optional, was Fragen zur Privatsphäre aufwirft. Außerdem erhöht es die Gesamtkomplexität des Systems, da Wallets nun mit einem fehlenden Registrierungszertifikat umgehen müssen.

6. Verwandte Arbeiten

6.1. EBSI-Policies

Die European Blockchain Services Infrastructure (EBSI) enthält ein Policy-Framework für Verifiable Credentials, das EDPs in wesentlichen Punkten ähnelt. In EBSI gilt:

- Presentation Policies (PresentationPolicy) werden vom Aussteller als Teil der Eigenschaft termsOfUse an ein Verifiable Credential angehängt. Das entspricht den EDPs, da der Aussteller damit Regeln definieren kann, wer das Credential abrufen oder verifizieren darf.
- Verifier Authorisation (VerifierAuthorisation) ist eine Erklärung, die der Verifier bzw. die Relying Party der Wallet bei der Präsentationsanfrage übermittelt. Sie gibt an, welche Attribute der Verifier anfordern darf, analog zum eIDAS-2.0-Relying-Party-Registration-Certificate.

Das in EBSI verwendete Zwei-Policy-Modell entspricht konzeptionell den vom Aussteller kontrollierten und von der RP erklärten Autorisierungsmechanismen von eIDAS 2.0. EBSI arbeitet jedoch in einem dezentralen, Blockchain-gestützten Identitätsökosystem, während eIDAS 2.0 einem Top-down-Modell auf Basis von Trust Lists folgt. Dennoch deuten die Entwurfsmuster auf künftige Harmonisierungsmöglichkeiten zwischen den Frameworks hin.

6.2. ISO/IEC 18013-5 („ISO mDL/mDOC“)

Der Standard ISO/IEC 18013-5, insbesondere seine zweite Ausgabe, die von ISO WG10 entwickelt wird, enthält verwandte Funktionen. Ein zentrales Konzept in der Diskussion (Task AP97.06) ist, Relying Parties zu ermöglichen, ihre beabsichtigte Datennutzung zu erklären. Das wird im Konzept der PurposeHints umgesetzt, mit denen die RP den Zweck signalisiert, für den Daten angefordert werden (z. B. Altersprüfung, Adressbestätigung).

PurposeHints sind zwar an sich kein Zugriffskontrollmechanismus, sollen aber datenschutzfreundlichere Interaktionen ermöglichen und es den Credential-Inhabenden (Nutzenden) oder ihrer Software (Wallets) erlauben, informierte Entscheidungen über die Offenlegung zu treffen. Das ähnelt dem Modell der informierten Einwilligung der Nutzenden in eIDAS 2.0 und könnte als ergänzende oder alternative Strategie zu vom Aussteller auferlegten EDPs dienen. Der ISO-Ansatz ist besonders relevant, weil ISO mDOC und eIDAS 2.0 durch standardübergreifende Credential-Kompatibilität (z. B. ISO mDL als Format für EAA) zunehmend zusammenwachsen.

6.3. Deutsche „Berechtigungszertifikate“

Einige nationale Systeme (z. B. der aktuelle deutsche eID) verwenden RP-Zertifikate („Berechtigungszertifikate“) und Register, konzeptionell ähnlich den Access- und Registrierungszertifikaten in eIDAS 2. Das EUDI-Modell lässt sich als gesamteuropäische Verallgemeinerung dieser vertrauensbasierten Schemata sehen. Anders als unternehmensinterne Single-Sign-On-(SSO-) oder OAuth-Systeme betont die EUDI Wallet rechtliche Vertrauensrahmen und die Zustimmung der Nutzenden statt zentralisierter Autorisierungsserver.

7. Schlussfolgerungen

Embedded Disclosure Policies (EDPs) führen eine neuartige, vom Aussteller definierte Ebene der Privatsphärenkontrolle in das EU-Framework für digitale Identitäten ein. Durch eIDAS 2 und seine Durchführungsrechtsakte rechtlich vorgeschrieben, verpflichten EDPs europäische Wallets dazu, vom Aussteller festgelegte Beschränkungen für die Weitergabe von Attributen einzuhalten. In der Praxis muss die Wallet-Software die EDP jeder eingehenden Bescheinigung gegen die authentifizierte Relying Party prüfen und die Nutzenden warnen, wenn die Partei nicht berechtigt ist. Das ergänzt die integrierten Funktionen der Wallet für Selective Disclosure und Pseudonyme und stärkt die Datenminimierung.

Der derzeitige EDP-Mechanismus ist jedoch im Umfang begrenzt. Es werden nur drei grundlegende Regelungstypen unterstützt (keine Regelung, Allow-List von RPs, Allow-List von CA-Roots). Feingranulare oder dynamische Bedingungen fehlen. Die Abhängigkeit von Trust Lists und Zertifikaten erhöht die Komplexität in grenzüberschreitenden Szenarien, und der Widerruf von Regelungen wird nicht direkt behandelt. Die Forschung legt nahe, dass künftige Erweiterungen die Registrierungszertifikate der RPs für eine differenziertere Autorisierung nutzen könnten.

Zusammenfassend sind EDPs ein wichtiger Schritt hin zu einer datenschutzbewussten Weitergabe von Credentials unter eIDAS 2. Sie spiegeln ein Gleichgewicht zwischen Kontrolle der Nutzenden und Vertrauen der Aussteller wider: Nutzende sind informiert und legen nur gegenüber vertrauenswürdigen Parteien offen, während Aussteller darauf vertrauen können, dass ihre Daten nicht missbraucht werden. Mit dem Ausrollen der Implementierungen muss besonderes Augenmerk auf Benutzbarkeit (klare Warnungen), Standardisierung (Trust Lists, Kennungen) und mögliche Erweiterungen (reichhaltigere Regelungen, Unterstützung für Widerruf) gelegt werden. Die Architektur der EUDI Wallet (die europäische Vertrauensrahmen mit modernen VC-Standards verbindet) bietet eine solide Grundlage. Die Weiterentwicklung und Wirksamkeit von EDPs hängt von laufender Verfeinerung der Regelungen und technologischer Innovation ab.

Literaturverzeichnis

[*] OpenAI. ChatGPT (o3) [Large language model] was used to edit the text.

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[3] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets.

[4] European Digital Identity: Architecture and Reference Framework (https://eu-digital-identity wallet.github.io/eudi-doc-architecture-and-reference-framework).

[5] More, S., Heher, J., Fasllija, E., & Mathie, M. (2024). Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems. In ARES 2024 - 19th International Conference on Availability, Reliability and Security, International Workshop on Emerging Digital Identities. Association for Computing Machinery (ACM).

[6] Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties.

[7] Fasllija, E., & More, S. Guardians of the Registry: Certificate Transparency for Relying Party Authorization in eIDAS 2. In ARES 2025 - 20th International Conference on Availability, Reliability and Security, International Workshop on Emerging Digital Identities. Springer.

[8] OpenID for Verifiable Presentations - draft 29 (https://openid.net/specs/openid-4-verifiable presentations-1_0.html).

[9] Verifiable Credentials Data Model v2.0 (https://www.w3.org/TR/vc-data-model-2.0/).