

Leistungsbeschreibung

Beschaffung eines EUDI-Wallet-Adapters
für den Testbetrieb

~~Version 1.0~~ Version 6.0

Inhalt

1	Aufbau des Dokuments	4
2	Gegenstand und Ziel der Ausschreibung.....	5
2.1	Öffentlicher Auftraggeber.....	5
2.2	Gegenstand und Ziele der Ausschreibung	5
3	Rahmenbedingungen	8
3.1	Rechtliche und organisatorische Rahmenbedingungen	8
3.2	Laufzeit.....	8
3.3	Projektsprache	8
3.4	Übergreifende Compliance Anforderungen	9
3.5	Weiterführende Informationen	9
3.6	Ökologische Nachhaltigkeit.....	9
3.7	Mitwirkungsleistungen des AG und technische Ausstattung	10
4	Anforderungen an die Leistung	11
4.1	Funktionale und nicht-funktionale Anforderungen.....	11
4.2	Mengengerüst.....	13
4.3	Bereitstellung und Unterstützung beim Deployment und der Konfiguration des Wallet-Adapters in den Umgebungen des Auftraggebers	14
4.4	Betrieb des Wallet-Adapters beim Auftraggeber	14
4.5	Integrationsunterstützung und Support bei der Anbindung des Wallet-Adapters an interne Systeme des Auftraggebers.....	14
4.6	Unterstützung bei der Erstellung, Pflege und Ausstellung von Test-Nachweisen in den zulässigen Protokollen.....	15
5	Technische Rahmenbedingungen und infrastrukturelle Anforderungen an das Softwareprodukt	16
5.1	Managed-Kubernetes-Testumgebung und Ressourcen-Korridor.....	16
5.2	Infrastrukturelle Anforderungen an das Softwareprodukt.....	18
6	Nachweis der Funktionsfähigkeit	22
6.1	Allgemeine Anforderungen an das eingesetzte Personal.....	23
7	Vertragliche Rahmenbedingungen.....	24

Abkürzungsverzeichnis

AG	Auftraggeber
AN	Auftragnehmer
BFV	Bundesfinanzverwaltung
BMF	Bundesfinanzministerium
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
DK	IT-Dienstekonsolidierung
DSGVO	Datenschutzgrundverordnung
IT	Informationstechnik
ITZBund	Informationstechnikzentrum Bund
o. Ä.	oder Ähnliches
vgl.	vergleiche
VSA	Verschlusssachenanweisung

1 Aufbau des Dokuments

Diese Leistungsbeschreibung stellt in ihrer Gesamtheit die für den Bieter notwendigen Informationen zur Erstellung eines Angebots innerhalb des Vergabeverfahrens "Beschaffung eines EUDI-Wallet-Adapters für den Testbetrieb" dar. Dabei referenziert die Leistungsbeschreibung auf die als Anlagen zur Leistungsbeschreibung geführten Dokumente.

Alle vom Bieter im Angebot zu berücksichtigenden Rahmenbedingungen und Anforderungen sind in dieser Leistungsbeschreibung zusammengefasst.

Mit den Kapiteln 1 und 2 sind einleitende Informationen zu der Ausschreibung und zu den Vergabeunterlagen gegeben.

Kapitel 3 umfasst die Darstellung der organisatorischen und technischen Rahmenbedingungen der Leistungserbringung. Es enthält grundsätzliche Informationen für den Bieter zur geplanten Durchführung der ausgeschriebenen Leistungen.

Das zentrale Kapitel 4 enthält die Beschreibung der Leistung sowie Angaben, inwieweit der Auftragnehmer diese erfüllen muss oder soll.

Kapitel 5 enthält die technischen Rahmenbedingungen, die im ITZBund vorherrschen und an denen sich die angebotene Lösung orientieren muss.

Kapitel 6 enthält die Angaben, wie das ITZBund im Rahmen des Vergabeverfahrens die Funktionsfähigkeit des angebotenen Produkts vor Zuschlag testen wird.

Kapitel 7 erhält einen Verweis auf den EVB-IT Systemvertrag, welcher die vertragliche Grundlage darstellt.

2 Gegenstand und Ziel der Ausschreibung

2.1 Öffentlicher Auftraggeber

Auftraggeber (AG) ist das Informationstechnikzentrum Bund (ITZBund) als zentraler IT-Dienstleister der Bundesverwaltung.

Das ITZBund ist ein zentraler IT-Dienstleister der Bundesverwaltung. Mit vielfältigen Services unterstützt es die Geschäftsbereiche des Bundesministeriums der Finanzen, des Bundesministeriums des Innern, des Bundesministeriums für Verkehr und digitale Infrastruktur und auftragsorientiert ebenfalls die gesamte Bundesverwaltung. Mit seinem umfassenden Leistungsspektrum positioniert sich das ITZBund als Shared-Service-Center für IT-Dienstleistungen innerhalb der öffentlichen Verwaltung.

2.2 Gegenstand und Ziele der Ausschreibung

Das ITZBund möchte eine Software beschaffen, mit der die Entgegennahme, Verarbeitung und Ausstellung von EUDI-Wallet Nachweisen möglich ist (nachfolgend „Wallet-Adapter“). Damit kommt das ITZBund den Anforderungen seiner Bedarfsträger nach, eine Erprobung in einer nicht-produktiven Testumgebungen zu ermöglichen. Dadurch sollen die notwendigen Anforderungen an einen späteren Wirkbetrieb, sowie organisatorischen und prozessualen Veränderungen sowohl für das ITZBund als auch für die Bedarfsträger, antizipiert und vorbereitet werden. Dies zählt direkt auf die Umsetzung und verpflichtende Einführung der Europäischen Digitalen Identität (EUDI-Wallet) gemäß eIDAS 2.0 ab 2027 ein.

Rahmenbedingungen und Ziele des Testbetriebs

Für den initialen Testbetrieb des Wallet-Adapters verfolgt das ITZBund das Ziel einer wirtschaftlichen, testbetriebsangemessenen und nachvollziehbaren Dimensionierung.

Der initiale Testbetrieb des Wallet-Adapters ist als funktionaler, kampagnenbasierter Testbetrieb auszulegen. Ziel ist der Nachweis der vorgesehenen Wallet-Adapter-Funktionen, die Erprobung ausgewählter Integrationsszenarien sowie das Sammeln technischer, fachlicher und organisatorischer Erfahrungen für einen späteren Wirkbetrieb.

Ziel ist der Aufbau einer Umgebung durch das ITZBund, die den initialen funktionalen Testbetrieb stabil unterstützt, ohne produktionsnahe Nutzungsszenarien oder unnötige Infrastrukturreserven zugrunde zu legen. Gleichzeitig soll die Umgebung nicht so knapp dimensioniert sein, dass Testkampagnen, parallele Wallet-Sessions, grundlegende Fehleranalyse oder spätere Erweiterungen nur durch grundlegende Neuarchitektur möglich wären.

Der ITZBund-seitige Zielkorridor für die initiale Testbetriebslandschaft deckt den funktionalen Testbetrieb, die vorgesehenen Testkampagnen, die geringe bis moderate Parallelität, die zu berücksichtigenden fachlichen Systemkontexte sowie grundlegende Monitoring-, Logging- und Fehleranalyseanforderungen ab.

Produktionsnahe Last- oder Performancetests sind in modellierter Form Bestandteil des initialen Testbetriebs. Vorgesehen sind funktionale Tests unter begrenzter Parallelität, um z. B. Race Conditions, Session-/State-Verhalten, gleichzeitige Wallet-Flows, Wiederholungen und Fehlerfälle im Rahmen des funktionalen Testbetriebs prüfen zu können. Außerdem wird die Skalierbarkeit und Performance unter Last im Hinblick auf die Zielvorgabe von bis zu 10 Mio. EUDI-Wallet-Nutzenden in 2027 geprüft.

Die Nutzung erfolgt voraussichtlich in zeitlich begrenzten Testkampagnen über Tage bis Wochen. Die Anzahl paralleler Testnutzenden bzw. Testläufe ist niedrig bis moderat und richtet sich nach dem für den jeweiligen Funktionsnachweis erforderlichen Umfang. Die Anbindung der beteiligten fachlichen Systemkontexte erfolgt voraussichtlich sequenziell und nicht vollständig parallel.

Fachliche Systemkontexte und Testdatenvorgaben

Im initialen Testbetrieb werden einschlägige, fachliche Systemkontexte simuliert und der Einsatz der EUDI-Wallet getestet.

Dies bezieht sich ausschließlich auf für den Testbetrieb vorgesehene Nachbildungen, nicht auf Produktivsysteme oder Produktivdaten. Die Nutzung erfolgt ausschließlich mit synthetischen Testdaten, die die erforderlichen Datenfelder und Attribute realitätsnah abbilden, jedoch keine produktiven personenbezogenen Daten, echten Identifikatoren oder produktiven Nummernkreise enthalten. Eine Verarbeitung personenbezogener Daten i. S. d. Art. 4 Nr. 1 DSGVO findet nicht statt.

Die für den Testbetrieb erforderlichen Testsysteme, Testdatenbestände, Schnittstellen, Fachverfahrensanbindungen und Umsysteme werden grundsätzlich durch den Auftraggeber bzw. die jeweils zuständigen fachlichen Stellen bereitgestellt oder koordiniert. Eine Verpflichtung des Auftragnehmers zur Bereitstellung vollständiger fachlicher Testregister oder vollständiger fachlicher Testdatenbestände besteht insoweit nicht; hiervon unberührt bleiben etwaige vom Auftragnehmer bereitzustellende technische Testkomponenten, Mock-Services oder für die Inbetriebnahme und Integration erforderliche Testartefakte.

Der EUDI-Wallet-Adapter soll als vollständig containerisierte Backend-Lösung inkl. benötigter Dokumentation und Konfiguration bereitgestellt werden, so dass das ITZBund die Lösung automatisiert und ohne weitere Entwicklungsarbeiten in seiner bestehenden Kubernetes/OpenShift-Infrastruktur ausrollen und betreiben kann. Der Betrieb, das Monitoring und die Wartung erfolgen durch das ITZBund selbst.

Die Dokumentation umfasst eine Beschreibung der Architektur sowie der eingesetzten Open-Source- bzw. proprietären Komponenten.

IT-Barrierefreiheit

Der Auftraggeber ist über das Behindertengleichstellungsgesetz (BGG) und die Barrierefreie-Informationstechnik-Verordnung (BITV2.0) dazu verpflichtet, Informationstechnik in barrierefreier Form anzubieten und zu nutzen. Der Auftraggeber nimmt diese Verpflichtung zur IT-Barrierefreiheit sehr ernst, um allen Menschen die Teilhabe an den digitalen Angeboten für Bürger:innen und für Beschäftigte zu ermöglichen. Daher wird die IT-Barrierefreiheit in zukünftigen Ausschreibungen zu diesem Leistungsgegenstand als Kriterium verankert werden. Die Anforderungen an die IT-Barrierefreiheit beziehen sich unter anderem auf die Benutzeroberflächen der Anwendungen, auf die von der Anwendung produzierten Dokumente und auf die Dokumentation der Anwendung sein. Einen vollständigen Überblick über die zu erfüllenden Anforderungen bietet der Anforderungskatalog auf dem Portal Barrierefreiheit. ([Link zum Anforderungskatalog](#))

3 Rahmenbedingungen

3.1 Rechtliche und organisatorische Rahmenbedingungen

Die Leistung dient der Erprobung und Evaluation eines Wallet-Adapters im nicht-produktiven Testumfeld des ITZBund. Sämtliche Tests erfolgen mit vollständig synthetischen oder anonymisierten Testdaten. Wie in Kapitel 2.2 beschrieben, wird davon ausgegangen, dass im Rahmen des Testbetriebs keine personenbezogenen Daten im Sinne des Art. 4 Nr. 1 DSGVO verarbeitet werden. Da sich dies im Laufe der Vertragslaufzeit ändern kann sowie aufgrund der Tatsache, dass im Rahmen des Supports ggf. personenbezogene Daten der Mitarbeitenden des Auftraggebers gespeichert werden, ist ggf. der Abschluss eines Auftragsverarbeitungsvertrags (AVV) gemäß Art. 28 DSGVO gemäß beigefügtem Muster erforderlich.

3.2 Laufzeit

Unmittelbar nach Zuschlagserteilung hat der Auftragnehmer den Wallet-Adapter betriebsbereit zur Verfügung zu stellen und beim Deployment und der Konfiguration des Wallet-Adapters in den Umgebungen des Auftraggebers zu unterstützen.

Der Beginn der Teststellung soll spätestens vier Wochen nach Zuschlagserteilung erfolgen. Der Testbetrieb hat eine Laufzeit bis zum 31.12.2027.

3.3 Projektsprache

Die Projektsprache ist deutsch. Alle Leistungen werden in deutscher Sprache erbracht. Die Dokumentation und das Angebot erfolgen in deutscher Sprache.

3.4 Übergreifende Compliance Anforderungen

- Der Auftragnehmer muss sicherstellen, dass alle Cloud-Infrastrukturen und -Dienste, einschließlich der operativen Kontrolle, des administrativen Zugriffs und des Supports, ausschließlich unter der Gerichtsbarkeit der EU oder der Mitgliedstaaten betrieben und von Einrichtungen verwaltet werden, die der Gerichtsbarkeit und Eigentumskontrolle der EU unterliegen.
- Der Auftragnehmer muss sicherstellen, dass keine Gesetze von Drittländern, einschließlich des US-amerikanischen CLOUD Act oder ähnlicher Gesetze, auf die Verarbeitung von Daten oder den Betrieb von Systemen angewendet werden können.
- ~~Das Betriebs- und Servicepersonal muss seinen Sitz innerhalb der Europäischen Union haben und der Support muss in deutscher Sprache erfolgen können.~~
- Das Betriebs- und Servicepersonal muss seinen Sitz innerhalb der Europäischen Union, des EWR oder der Schweiz haben und der Support muss in deutscher Sprache erfolgen können
- Der Auftragnehmer muss sicherstellen, dass alle Infrastrukturdienste und Daten mit Ausnahme von sensiblen Schlüsselmaterialien, die in HSMs gespeichert sind, vollständig portabel bleiben und ohne Herstellerabhängigkeit über System- und Organisationsgrenzen hinweg migriert werden können.
- Der Auftragnehmer muss eine Software-Stückliste (SBOM) erstellen und kontinuierlich pflegen, die die Infrastruktur und andere operative Komponenten und Dienste umfasst, für die der Auftragnehmer verantwortlich ist.

3.5 Weiterführende Informationen

eIDAS-Verordnung - <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>

EUDI Wallet Implementing Acts - <https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-european-digital-identity-wallets>

EUDI Wallet Architecture and Reference Framework - <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.4.0/>

3.6 Ökologische Nachhaltigkeit

Der Auftragnehmer hat alle Arbeiten so umzusetzen, dass der hierdurch entstehende Ressourcenverbrauch in allen eingebundenen Bereichen jederzeit minimal ist.

3.7 Mitwirkungsleistungen des AG und technische Ausstattung

Der Auftraggeber verpflichtet sich, bei der Erbringung der Leistungen wie folgt mitzuwirken:

- Der Auftraggeber stellt alle erforderlichen Informationen und Unterlagen rechtzeitig und vollständig zur Verfügung.
- Der Auftraggeber stellt die zur Leistungserbringung auf seinem Betriebsgelände notwendigen Voraussetzungen der IT- und Kommunikationsinfrastruktur, und Räumlichkeiten.
- Der Auftraggeber stellt die zur Leistungserbringung notwendigen Systemzugänge (z.B. User-Kennungen) zur Verfügung.

Für sämtliche Arbeiten, die zur konkreten Auftragsabwicklung erforderlich sind, wird der jeweils im Einzelabruf tätigen externen Person ein namentlich zugewiesener Arbeitsplatzcomputer (SINA-Notebook) mit personifizierter Signaturkarte vom ITZBund zur Verfügung gestellt. Es ist kein Remote-Zugriff auf die Technik des ITZBund über bieter eigene Systeme möglich. Der Remote-Zugriff auf die Entwicklungsumgebungen und die damit verbundene Infrastruktur erfolgt über eine namentlich zugewiesene begrenzte Anzahl an Hardware des ITZBund (SINA-Boxen) nur innerhalb Deutschlands. Für die Nutzer von IT-Komponenten des ITZBund gelten [Allgemeine Sicherheitsvorgaben des ITZBund für externe Unterstützungskräfte](#).

4 Anforderungen an die Leistung

4.1 Funktionale und nicht-funktionale Anforderungen

Der Wallet-Adapter ist eine server-seitige Backend-Komponente, die als zentrale technische Schnittstelle zwischen internen Systemen des Auftraggebers (Digitalisierungsplattformen, Gateways, Register, Fachanwendungen) und beliebigen, eIDAS-konformen EUDI-Wallets dient.

Der Wallet-Adapter hat folgende Kernaufgaben eigenständig zu erfüllen:

- Entgegennahme und Überprüfung von Nachweisen aus EUDI-Wallets (insbesondere die von der Bundesrepublik Deutschland entwickelte), kryptographische Verifikation sowie Bereitstellung der extrahierten Daten in standardisierter Form.
- Bereitstellung der für die Wallet-Interaktion erforderlichen technischen Artefakte (QR-Code, Deep-/Universal-Link) als Datenstruktur zur Weiterverarbeitung durch das anbindende System.
- Vollständige Übernahme der technischen Kommunikation mit den EUDI-Wallets, so dass die anbindenden Systeme keine EUDI-spezifischen Protokolle implementieren müssen.
- Die Erzeugung signierter, elektronischer Nachweise, die in eine EUDI-Wallet ausgestellt werden können.
- Anbindung von Fachverfahren, Registern, Datenquellen oder Testsystemen.

Folgende technische Anforderungen sind durch den Wallet-Adapter zu erfüllen:

- Unterstützung der ARF-Protokolle (OID4VP, OID4VCI)
- Unterstützung der ARF-Formate (SD-JWT VC/JWT-VC, mdoc)
- Sichere Prüfung und Verifikation eingehender verifizierbarer Nachweise aus der EUDI-Wallet (Signatur, Vertrauensanker, Gültigkeit)
- Ausstellung und Präsentation von Electronic Attestations of Attributes (EAA)
- ~~Ausstellung von zu EAA vergleichbaren, signierten Nachweisen~~ Ausstellung von EAA Nachweisen
- Ausstellung und Präsentation von Person Identification Data (PID) auf Basis der Onlineausweisfunktion des Personalausweises
- Schnittstelle zur Anbindung eines (Q)TSP an den Wallet-Adapter

- Bereitstellung einer REST-Schnittstelle zur Anbindung der internen Systeme des Auftraggebers (wie bspw. Low-Code-Plattformen, Register oder Fachanwendungen) an den Wallet-Adapter
- Der Adapter wandelt die erhaltenen Daten aus der EUDI-Wallet in die Formate JSON und XML um und leitet sie an die internen Systeme (bspw. Testverfahren, Datenquellen, etc.) des Auftraggebers weiter
- Unterstützung von Same-Device- und Cross-Device-Flows
- Bereitstellung der für die Wallet-Interaktion erforderlichen technischen Artefakte (QR-Code, Deep-/Universal-Link)
- Nahtlose Integration in das deutsche Wallet-Ökosystem

Für den Testbetrieb insbesondere vorgesehen sind:

- Deutschland-Tests mit den genannten fachlichen Systemkontexten,
- EU-/Cross-Border-Tests, soweit hierfür im Testbetrieb geeignete Wallets, Testumgebungen oder Testpartner verfügbar sind,
- QES-/QTSP-nahe Tests mit Test-PKI bzw. Test-Vertrauensankern, soweit hierfür geeignete Testdienste, Testzertifikate oder Test-Vertrauensanker bereitgestellt werden,
- grundlegende Monitoring-, Logging- und Trace-Fähigkeiten sowie basale Nachvollziehbarkeit fehlgeschlagener Testflüsse zur Fehleranalyse.

Das ITZBund greift **ausschließlich über dokumentierte, versionsgeführte Schnittstellen** auf den Dienst zu:

- Primäre Schnittstelle: REST-API gemäß bereitgestellter OpenAPI-3.1-Spezifikation (YAML + ReDoc/Swagger-UI)
- Alle relevanten OpenID4VP-, OpenID4VCI- und eIDAS-2.0/ARF-Flows (PID-, EAA-, SCA- und QES-Flows)
- Optionale Callback-/Webhook-Endpunkte für asynchrone Benachrichtigungen

Bei der Umsetzung der Anforderungen sind die Vorgaben der eIDAS-Verordnung, der dazugehörigen Durchführungsrechtsakte, des ARF sowie der einschlägigen ISO-, ETSI- und CEN-Standards zu gewährleisten.

Folgende nicht-funktionale Anforderungen sind durch den Wallet-Adapter zu erfüllen:

- Sicherstellung der Informationssicherheit nach Stand der Technik
- Der Wallet-Adapter muss vollständig On-Premise betrieben werden können
- Der Wallet-Adapter muss in einer containerisierten Umgebung betrieben werden können
- Lasttoleranz in einem für eine Testumgebung angemessenen Maß
- Schnittstellen für Monitoring und Logging

Eine detaillierte Beschreibung der technischen Rahmenbedingungen und infrastrukturellen Anforderungen, die das Softwareprodukt erfüllen muss, sind in Kapitel 5 zu finden.

4.2 Mengengerüst

Für die initiale Dimensionierung des Testbetriebs gelten folgende zugrunde gelegte Werte zu den Nutzungsszenarien der Testbetriebslandschaft.

Tabelle 1: Dimensionierung/Mengengerüst für initialen Testbetrieb

Dimension	Dimensionierungswert	Zweck/Einordnung
Gleichzeitige aktive Testnutzende aus funktionaler Sicht	Bis ca. 40 über die initiale Testbetriebslandschaft hinweg	Abdeckung funktionaler Tests durch kleine Testgruppen aus Projekt-, Betriebs- und Fachseite
Gleichzeitige aktive Testnutzende aus Lasttest	Abhängig vom Use Case und im Projektverlauf zu bestimmen; entsprechend Zielstellung EUDI-Wallet-Nutzende bis zu 10 Mio. in 2027	Abdeckung von Lasttests zur Modellierung produktionsnaher Szenarien
Kurzzeitige parallele Wallet-Sessions	Bis ca. 60	Puffer für Testkampagnen, Demonstrationen, funktionale Parallelitätstests und parallele Wiederholungen einzelner Testfälle
Wallet-Flows pro Testtag	Typisch 150–600	Abbildung normaler funktionaler Testtage mit mehreren Use Cases,

Umgebungsinstanzen und
Wiederholungen

4.3 Bereitstellung und Unterstützung beim Deployment und der Konfiguration des Wallet-Adapters in den Umgebungen des Auftraggebers

Der Auftragnehmer stellt den Wallet-Adapter betriebsbereit zur Verfügung. Die Software muss in installationsfertigen Paketen übergeben werden (vgl. Abschnitt 5.2).

Der Auftragnehmer muss bei dem Deployment bzw. bei der Konfiguration des Wallet-Adapters unterstützen.

4.4 Betrieb des Wallet-Adapters beim Auftraggeber

Der Auftraggeber betreibt den Wallet-Adapter für die Dauer der Vertragslaufzeit.

Während des gesamten Leistungszeitraumes pflegt der Auftragnehmer die Software und stellt gegebenenfalls Patches bereit.

Leistungen des Auftragnehmers:

- Sicherstellung der Informationssicherheit nach dem Stand der Technik
- Unterstützung bei Betrieb, Monitoring, Logging und Alarmierung
- Regelmäßige Security Patch Management und Release-Updates

4.5 Integrationsunterstützung und Support bei der Anbindung des Wallet-Adapters an interne Systeme des Auftraggebers

Der Auftragnehmer stellt während der gesamten Projektlaufzeit Ansprechpersonen bereit, die, wenn nötig, bei der Integration und Anbindung des Wallet-Adapters unterstützen. Des Weiteren stellt der Auftragnehmer einen Support bereit, der während der gesamten Projektlaufzeit bei Fragen zum Wallet-Adapter zur Verfügung steht.

Leistungen des Auftragnehmers:

- Service-Level-Agreement (SLA) mit definierten Reaktions- und Lösungszeiten gem. vom Bieter einzureichenden Supportkonzept

- Dedizierte technische Ansprechpersonen und 2nd-Level-Support
- Anlassbezogenes Reporting über Verfügbarkeit, Performance und Sicherheitsvorfälle unter Beachtung der infrastrukturellen Vorgaben

4.6 Unterstützung bei der Erstellung, Pflege und Ausstellung von Test-Nachweisen in den zulässigen Protokollen

Der Auftragnehmer unterstützt bei der Erstellung und Pflege von Nachweisen, die für Testzwecke zwischen einer Wallet-Applikation und dem Testsystem ausgetauscht und verarbeitet werden. Weiterhin sollen Nachweise zu Testzwecken aus Fachanwendungen in die Wallet in Form von signierten Nachweisen ausgestellt werden.

Leistungen des Auftragnehmers:

- Technische und inhaltliche Unterstützung bei der initialen Erstellung von Nachweisen in den korrekten Schemata und Protokollen
- Bereitstellung einer GUI und/oder eines Templates zur eigenständigen Erstellung und Befüllung von Test-Nachweisen

5 Technische Rahmenbedingungen und infrastrukturelle Anforderungen an das Softwareprodukt

5.1 Managed-Kubernetes-Testumgebung und Ressourcen-Korridor

Der initiale Testbetrieb des Wallet-Adapters soll in einer durch das ITZBund bereitgestellten Managed-Kubernetes-/OpenShift-Betriebsumgebung betrieben werden. Der Auftragnehmer liefert den Wallet-Adapter als containerisiertes Softwareprodukt. Die nachfolgenden Ressourcen- und Infrastrukturangaben beziehen sich auf diese ITZBund-seitige Testbetriebslandschaft.

Der Komponentenrahmen berücksichtigt sowohl die fachlich aus den vorgesehenen Use Cases abgeleiteten Wallet-Adapter-Funktionen als auch die für einen kampagnenbasierten Testbetrieb erforderlichen technischen Betriebsfunktionen.

Der nachfolgende Hardware- und Ressourcenrahmen bildet den vom ITZBund vorgesehenen Zielkorridor für den Aufbau der initialen Testbetriebslandschaft. Er ist vom Auftragnehmer als Planungsgrundlage zu berücksichtigen. Er setzt bewusst einen wirtschaftlichen und technischen Rahmen für den beschriebenen Testbetrieb. Die Lösung des Auftragnehmers soll innerhalb dieses Rahmens lauffähig betrieben werden können. Dadurch wird sichergestellt, dass die Lösungsarchitektur testbetriebsangemessen, ressourceneffizient und nicht produktionsnah überdimensioniert ausgelegt wird.

Tabelle 2: Hardware- und Ressourcenrahmen für initiale ITZBund-seitige Testbetriebslandschaft

Ressource/ Dimension	Ressourcen-Korridor initialer Testbetrieb	Zweck / fachlich-technische Begründung
Gesamt-vCPU	ca. 8–16 vCPU	Dient der Verarbeitung funktionaler Wallet-Flows einschließlich kryptografischer Prüfungen, Signaturvorgänge, API-Kommunikation, Session-/Flow-Verarbeitung, Persistenzzugriffen und Fehleranalyse
Gesamt-RAM	ca. 24–48 GB RAM	Dient der stabilen Verarbeitung paralleler Test-Sessions, Protokollverarbeitung, Nachweisvalidierung, Laufzeitumgebung, Datenbank-/Persistenzanteilen und

		unmittelbar	erforderlichen
		NebenkompONENTEN	
Initialer Speicherbedarf	ca. 250–500 GB	Dient der Speicherung von Konfigurationen, synthetischen Testdaten, Persistenzdaten, technischen Logs sowie begrenzten Trace-, Fehler- und Testkampagnendaten; der konkrete Bedarf hängt insbesondere vom Umfang der Protokollierung und Trace-Erhebung ab.	
Erweiterbarer Speicherrahmen	mindestens 1 TB	Dient der Aufnahme zusätzlicher Testdatenstände, längerer Testkampagnen, erhöhter Log-/Trace-Volumina, Backups oder späterer Erweiterungen ohne kurzfristige Neuplanung	
Log-/Trace- Retention	sicherheits- und betriebsrelevante Protokollierungsdaten bis zu 30 Tage; umfangreiche Trace- /Debugdaten bedarfsgerecht und konfigurierbar	Dient der Nachvollziehbarkeit, Fehleranalyse, Testauswertung und Sammlung repräsentativer Betriebserfahrungen, ohne eine produktionsnahe SIEM-Auswertung vorauszusetzen	

Die konkrete Bereitstellung der Ressourcen erfolgt durch den Auftraggeber im Rahmen der vorgesehenen Betriebsumgebung. Darüber hinaus gehende Anforderungen des Auftragnehmers an seine Lösung sind im Rahmen einer Bieterfrage zu adressieren.

5.2 Infrastrukturelle Anforderungen an das Softwareprodukt

Grundanforderung an die Betriebsfähigkeit:

Der Wallet-Adapter muss als containerisierte Backend-Lösung in einer durch den Auftraggeber bereitgestellten Managed-Kubernetes-/OpenShift-Betriebsumgebung lauffähig betrieben werden können.

Die vorgesehenen Anforderungen der Managed-Kubernetes-/OpenShift-Betriebsumgebung an das Softwareprodukt werden in diesem Kapitel beschrieben. Der Auftragnehmer hat als Teil der Lieferung exemplarische Softwarekonfigurationen, Deployment- und Konfigurationsartefakte sowie Build- und Beispiel-CI/CD-Pipelines bereitzustellen, aus denen hervorgeht, wie die Lösung diese Anforderungen erfüllt und welche Einstellungen für Deployment, Konfiguration, Ressourcenbedarf, Persistenz, Schnittstellen, Routing/Ingress, API-Gateway-Anbindung, Zertifikate, Trust-Anker, Truststores, Secrets, Storage, Netzwerkkommunikation sowie Monitoring, Logging und Tracing vorgesehen sind.

Die mitzuliefernde exemplarische Softwarekonfiguration für den initialen Testbetrieb muss mit dem in der technischen Leistungsbeschreibung definierten Ressourcen-Korridor vereinbar sein.

Namespace-Betrieb und Berechtigungen:

Die Lösung muss innerhalb bereitgestellter Namespaces ohne Cluster-Admin-Rechte betreibbar sein.

Die mitzuliefernde exemplarische Softwarekonfiguration muss die für den Betrieb erforderlichen Security-Kontext-, ServiceAccount-, Namespace-Rollen- und Berechtigungseinstellungen enthalten, insbesondere in Helm Values, Kubernetes-/OpenShift-Manifests oder vergleichbaren Konfigurationsartefakten.

Die Lösung muss mit restriktiven Security-Kontexten bzw. den durch die Betriebsumgebung vorgegebenen Sicherheitsmechanismen betreibbar sein.

Für die Installation und den Betrieb benötigte Operatoren, Custom Resources und clusterweite Ressourcen:

Clusterweite Installations- oder Administrationsrechte dürfen durch die Lösung nicht vorausgesetzt werden.

Soweit die Lösung Operatoren, Custom Resources, Custom Resource Definitions oder vergleichbare Kubernetes-/OpenShift-Erweiterungen nutzt, müssen die hierfür erforderlichen

Ressourcen und Konfigurationsbestandteile in den mitzuliefernden Deployment- und Konfigurationsartefakten erkennbar sein.

Erreichbarkeit, Routing und Netzwerkkommunikation:

Der Auftragnehmer hat als Teil der mitzuliefernden exemplarischen Softwarekonfiguration alle für den Testbetrieb erforderlichen internen und externen Endpunkte, Ports, Protokolle, Redirect-/Callback-URLs, Deep-Link-/Universal-Link-Anforderungen sowie ausgehenden Verbindungen auszuweisen.

Dies umfasst insbesondere Verbindungen zu Wallets, Testsystemen, Fachverfahren, Registern, Vertrauensdiensten sowie TSP-/QTSP-Komponenten.

Konfiguration, Secrets und Umgebungsparameter:

Der Auftragnehmer hat als Teil der mitzuliefernden exemplarischen Softwarekonfiguration auszuweisen, wie Konfigurationen, Secrets und Umgebungsparameter über Kubernetes-übliche Mechanismen wie ConfigMaps, Secrets oder vergleichbare Mechanismen (z. B. SCC) eingebunden werden.

Secrets dürfen nicht fest in Images, Helm Charts, Values-Dateien, Manifests oder sonstigen Konfigurationsartefakten kodiert sein.

Zertifikate, Trust-Anker und Truststores:

Die mitzuliefernde exemplarische Softwarekonfiguration muss die für den Testbetrieb erforderlichen Einstellungen zu Zertifikaten, Trust-Ankern, Truststores, TLS/mTLS sowie Signatur- und Verifikationsmaterial vorsehen.

Die Einbindung dieser Einstellungen muss über Konfigurationsartefakte bzw. Kubernetes-übliche Mechanismen wie Secrets, ConfigMaps oder vergleichbare Mechanismen erfolgen können.

Storage und Persistenz:

Persistente Speicher-, Datenbank-, Volume-, PVC-, Objekt- oder Dateispeicherbedarfe sind als Teil der mitzuliefernden exemplarischen Softwarekonfiguration auszuweisen, insbesondere über Helm Values, Kubernetes-/OpenShift-Manifests, PVC-Definitionen, Labels, Annotations, Datenbank-Migrationsskripten (Flyway/Liquibase) oder vergleichbare Konfigurationsartefakte.

Zweck, Kapazität, Retention-relevante Einstellungen sowie etwaiger Backup-/Restore-Bedarf müssen daraus für den initialen Testbetrieb nachvollziehbar hervorgehen.

Container-Images und Deployment-Artefakte:

Der Auftragnehmer hat als Teil der Lieferung signierte, versionierte, prüfbare und updatefähige Container-Images sowie die zugehörigen Deployment- und Konfigurationsartefakte bereitzustellen.

Die Images müssen für die Nutzung in einer Container Registry und für automatisierte Image-Prüfungen geeignet sein.

Sie dürfen keine hart kodierten Secrets enthalten, müssen mit eindeutig versionierten Basis-Images erstellt sein, dürfen nur erforderliche Laufzeitbestandteile enthalten und müssen mit nicht privilegiertem Laufzeitnutzer betreibbar sein.

Technische Vorgaben zu Monitoring, Logging und Tracing:

Monitoring, Logging und Trace-Fähigkeiten sowie eine basale Nachvollziehbarkeit fehlgeschlagener Testflüsse sind vorzusehen, um Testflüsse nachvollziehen, Fehler analysieren und Betriebserfahrung sammeln zu können. Dies umfasst insbesondere folgende Aspekte:

- Health-, Readiness- und Liveness-Prüfungen,
- technische Logs für relevante Wallet-Adapter-Flows,
- strukturierte Fehlercodes und Fehlerklassen,
- technische Korrelationskennungen,
- Nachvollziehbarkeit fehlgeschlagener Testflüsse,
- relevante Metriken sowie
- Integration in die vorgesehenen Logging- und Monitoring-Strukturen der ITZBund-Testumgebung, soweit diese bereitgestellt werden

Die mitzuliefernde exemplarische Softwarekonfiguration muss für alle wesentlichen Komponenten Health-, Readiness- und Liveness-Prüfungen enthalten, die als Kubernetes-/OpenShift-Probes nutzbar sind.

Die hierfür erforderlichen Endpunkte, Ports, erwarteten Statuscodes, Timeouts und relevanten Abhängigkeiten müssen in den mitzuliefernden Deployment- und Konfigurationsartefakten enthalten sein.

Die mitzuliefernde exemplarische Softwarekonfiguration muss einen Prometheus-kompatiblen Metrik-Endpunkt für relevante technische Betriebsmetriken enthalten.

Die Bereitstellung von Metriken muss mindestens Status, Verfügbarkeit, Fehlerzähler, Request-/Flow-Zähler, Antwortzeiten und technische Fehlerzustände wesentlicher Komponenten abdecken.

Die mitzuliefernde exemplarische Softwarekonfiguration muss Einstellungen für strukturierte technische Logs relevanter Wallet-Adapter-Flows sowie für technische Korrelationskennungen zur Nachvollziehbarkeit zusammengehöriger Flow-Schritte enthalten. Dies umfasst insbesondere Logformat, Logausgabe, Log-Level, Korrelations-/Request-IDs, Header zur Korrelationsweitergabe sowie die Maskierung sensibler Inhalte.

Vollständige Nachweisinhalte, Attribute, Schlüsselmaterialien, Tokens, Secrets oder vergleichbare sensitive Inhalte, deren Kenntnis unberechtigten Nutzern Zugriff auf das System gewährleisten würden, dürfen nicht regulär protokolliert werden.

Debug-/Trace-Ausgaben mit solchen Inhalten dürfen nur testkonzeptkonform, minimiert und konfigurierbar erfolgen. Debug-/Trace-Ausgaben müssen in der mitzuliefernden exemplarischen Softwarekonfiguration standardmäßig deaktiviert oder gezielt konfigurierbar sein.

Die Dauer der Vorhaltung von Sicherheits- und betriebsrelevante Protokollierungsdaten muss im Testbetrieb konfigurierbar sein.

6 Nachweis der Funktionsfähigkeit

Der Auftraggeber ist daran interessiert, eine bereits am Markt bestehende und funktionsfähige Lösung einzukaufen. Der Bieter muss im Rahmen der Angebotsabgabe nachweisen, dass die Anforderungen der Ausschreibung erfüllt werden. Der Nachweis erfolgt in zwei Schritten:

1) Nachweis im Rahmen der Angebotslegung

Bei Bietern, die in der SPRIND Funke Challenge „Funke EUDI WALLET Prototypes“ die Stufe 2 erreicht haben, gilt der Nachweis bereits als erbracht.

Ebenfalls als erbracht gilt der Nachweis, wenn der Bieter in der Openwallet Foundation unter „Wallets und Agents“ ([Wallet and Agent Overview](#)) aufgeführt ist und Anforderungen der in Abschnitt 3.1 definierten Protokolle und Formate erfüllt.

Erfüllt der Bieter keine der beiden Möglichkeiten, muss er anderweitig den Nachweis erbringen. Die Art und Weise des Nachweises ist dem Bieter überlassen.

2) Nachweis im Rahmen der verifizierenden Teststellung

Der Bieter, der für den Zuschlag vorgesehen ist (d. h. der Bieter, der nach Abschluss der Angebotswertung auf Rang 1 ist) muss im Rahmen einer zu präsentierenden Teststellung den technischen Beweis erbringen, dass alle Anforderungen erfüllt werden. Eine Demo-Vorstellung wird ausdrücklich als nicht ausreichend anerkannt.

Erfüllt der Bieter die Teststellung, wird der Zuschlag auf das Angebot erteilt. Erfüllt der Bieter die Teststellung nicht, wird sein Angebot ausgeschlossen und der nächstbeste Bieter zur Teststellung aufgefordert.

6.1 Allgemeine Anforderungen an das eingesetzte Personal

Der Auftragnehmer ist verpflichtet, die Leistungserbringung ausschließlich durch ausreichend qualifiziertes Personal durchführen zu lassen.

Um die Erbringung der Unterstützungsleistungen durch das angegebene Personal sicherzustellen, müssen alle zur Leistungserbringung eingeplanten bzw. eingesetzten Personen mindestens die folgenden allgemeinen Anforderungen erfüllen:

- Das seitens des Auftragnehmers eingeplante Personal muss, in entsprechender Personenzahl und Verteilung der Anforderungen, die Fähigkeiten für die aufgeführten Aufgaben besitzen.
- Die Bereitschaft zur Teilnahme an Projektsitzungen zwischen dem Auftraggeber und dem Auftragnehmer bzw. mit Kunden des ITZBund am Sitz des Auftraggebers bzw. des jeweiligen Kunden des ITZBund muss gegeben sein. Eine grundsätzliche Bereitschaft zu Reisen muss daher gewährleistet sein.
- Hilfsbereitschaft und eine klare Bereitschaft zur Kooperation mit den ITZBund-Beschäftigten sowie ein methodisches Vorgehen werden vorausgesetzt.
- Sicherer Umgang mit den Microsoft Office-Produkten und Skype.
- Das vom Auftragnehmer für die Leistungserbringung vorgesehene Personal muss fließend die mündliche und schriftliche Kommunikation in Deutsch (Niveau C2) beherrschen.
- Hinsichtlich des seitens des Auftragnehmers eingeplanten Personals wird die Bereitschaft zur Verpflichtung gemäß Verpflichtungsgesetz vorausgesetzt.
- Hinsichtlich des seitens des Auftragnehmers eingeplanten Personals wird die Bereitschaft zur Verpflichtung auf das Datengeheimnis gemäß § 53 Bundesdatenschutzgesetz (BDSG) vorausgesetzt.
- Hinsichtlich des seitens des Auftragnehmers für die Leistungserbringung innerhalb des Vertrags eingeplanten Personals wird die Bereitschaft vorausgesetzt, sich auf Anforderung des Auftraggebers einer Sicherheitsüberprüfung Niveau Ü2 (Sabotage- und Geheimschutz) gemäß § 9 Sicherheitsüberprüfungsgesetz (SÜG) zu unterziehen. Für diesen Fall müssen Personen, die noch nicht sicherheitsüberprüft sind, zunächst beim Auftraggeber ein behördliches Führungszeugnis vorlegen. Etwaige für die Durchführung der Sicherheitsüberprüfung bzw. die Einholung des behördlichen Führungszeugnisses anfallenden Kosten werden vom Auftraggeber nicht erstattet. Eine eingeleitete, aber noch nicht abgeschlossene Sicherheitsüberprüfung ersetzt das behördliche Führungszeugnis nicht.

7 Vertragliche Rahmenbedingungen

Die Leistungserbringung erfolgt auf Grundlage des EVB-IT Systemvertrags nebst Anlagen.