

VERTRAG ÜBER UNTERSTÜTZUNGSLEISTUNGEN IM BEREICH INFORMATIONSSICHERHEIT FÜR EUDI-WALLET

zwischen

Common Codes GmbH

Zionskirchstraße 73a, 10119 Berlin

(im Folgenden: „Common Codes“ oder „Auftraggeber“)

und

[...]

(im Folgenden: „Auftragnehmer“)

Auftraggeber und Auftragnehmer gemeinsam die „Parteien“

Präambel

Der Auftraggeber führt im Auftrag des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) das Projekt „EUDI Wallet Infrastruktur“ durch und entwickelt in diesem Rahmen die nationale EUDI Wallet für Deutschland sowie das zugehörige Ökosystem. Gegenstand des Projekts ist unter anderem die Sicherstellung eines hohen Niveaus an Informationssicherheit, Datenschutz und Nutzbarkeit der EUDI-Wallet-Lösungen für Endnutzerinnen und Endnutzer.

Vor diesem Hintergrund schreibt der Auftraggeber im Wege eines öffentlichen Vergabeverfahrens einen Dienstvertrag aus über Unterstützungsleistungen im Bereich Informationssicherheit für sichere mobile Apps. Der Auftragnehmer erbringt Beratungs-, Analyse-, Konzeptionierungs- und Unterstützungsleistungen entlang des gesamten Entwicklungs- und Einführungszyklus der App und ihres Ökosystems.

Dieser Vertrag wird als Rahmenvereinbarung geschlossen. Der geschätzte Auftragswert beträgt 3.200.000 EUR (netto); zugleich wird ein Höchstwert in Höhe von 3.500.000 EUR (netto) vereinbart, bis zu dem Leistungen aus dieser Rahmenvereinbarung beauftragt werden können. Eine Überschreitung dieses Höchstwertes ist ausgeschlossen. Einzelabrufe, abweichende Abrufaufträge oder gesonderte Leistungsverträge werden nicht vereinbart; sämtliche Leistungen werden auf Basis dieser Rahmenvereinbarung und der jeweils abgestimmten Leistungspakete erbracht.

Vor diesem Hintergrund schließen die Parteien folgenden Vertrag.

1. Vertragsgegenstand; Geltungsreihenfolge; Ausschreibungsbezug

- 1.1 Gegenstand dieses Vertrages sind Unterstützungsleistungen im Bereich Informationssicherheit für die Entwicklung, Einführung und den Betrieb der EUDI-Wallet-Infrastruktur des Auftraggebers. Der Auftragnehmer erbringt für die Common Codes insbesondere Leistungen in den Bereichen Informationssicherheit, Schwachstellenmanagement, Sicherheitsarchitektur, kryptografische Konzepte, Unterstützungsleistungen bei Sicherheits- und Zertifizierungsprozessen sowie Nutzer:innen-, Akzeptanz- und Barrierefreiheitsstudien für sichere mobile Apps.
- 1.2 Der Vertrag kommt nach Durchführung eines öffentlichen Vergabeverfahrens des Auftraggebers zustande. Abrufberechtigt aus diesem Rahmenvertrag sind die Common Codes, ihre bestehenden und zukünftigen verbundenen Unternehmen (Mutter-, Tochter- und Schwestergesellschaften) so wie das Bundesministerium für Digitales und Staatsmodernisierung. Die im Vergabeverfahren bekannt gemachten Unterlagen, insbesondere die Leistungsbeschreibung „Unterstützungsleistungen im Bereich Informationssicherheit für EUDI-Wallet“ sowie das Angebot des Auftragnehmers, sind Bestandteil dieser Rahmenvereinbarung. Im Falle von Widersprüchen gelten die nachfolgend aufgeführten Vertragsbestandteile in der folgenden Reihenfolge:
 - die Leistungsbeschreibung „Unterstützungsleistungen im Bereich Informationssicherheit für EUDI-Wallet“ einschließlich etwaiger Bieterfragen und Antworten des Auftraggebers;
 - die Bestimmungen dieses Vertrages (Rahmenvereinbarung);
 - die sonstigen dem Vergabeverfahren zugrunde liegenden Vergabeunterlagen;
 - das Angebot des Auftragnehmers mit seinen Anlagen, einschließlich Preisblatt und Mitarbeiterprofilen;
 - die „Verdingungsordnung für Leistungen, Teil B – Allgemeine Vertragsbedingungen für die Ausführung von Leistungen (VOL/B)“, Fassung 2003;
 - die gesetzlichen Regelungen des Bürgerlichen Gesetzbuches (BGB).
- 1.3 Die Regelungen dieses Vertrages gelten ausschließlich. Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Auftragnehmers finden keine Anwendung, auch wenn ihnen nicht ausdrücklich widersprochen wird.
- 1.4 Dieser Vertrag begründet eine Rahmenvereinbarung ohne Mindestabnahme. Der Auftraggeber ist zu keinem Zeitpunkt verpflichtet, ein bestimmtes Leistungsvolumen abzunehmen oder abzurufen. Ein Anspruch des Auftragnehmers auf Abnahme einer bestimmten Leistung oder auf Ausschöpfung des Schätz- oder Höchstwertes besteht nicht.
- 1.5 Sämtliche Einzelbeauftragungen und Konkretisierungen der im Rahmen dieser Rahmenvereinbarung geschuldeten Leistungen erfolgen ausschließlich über das vom Auftraggeber bereitgestellte Ticketsystem. Ein Ticket im Ticketsystem, das (i) die zu erbringende Leistung (Leistungsbaustein, Arbeitspaket), (ii) den voraussichtlichen Leistungsumfang (z. B. geschätzte Stundenanzahl bzw. Budgetrahmen) und (iii) einen fachlich verantwortlichen Ansprechpartner des Auftraggebers ausweist, gilt als verbindliche Beauftragung (Einzelabruf) auf Grundlage dieser Rahmenvereinbarung. Die im Ticketsystem eingestellten und vom

Auftraggeber freigegebenen Tickets erfüllen die Anforderungen an die Textform und gelten als schriftliche Beauftragung im Sinne dieses Vertrages. Einer zusätzlichen Auftragsbestätigung in Papierform bedarf es nicht.

- 1.6 Der Auftraggeber ist berechtigt, Leistungen im Sinne dieser Rahmenvereinbarung ganz oder teilweise auch durch Dritte erbringen zu lassen. Hieraus folgt insbesondere kein Anspruch des Auftragnehmers auf ausschließliche Beauftragung oder auf Beauftragung eines bestimmten Leistungsumfangs.

2. Rechtsnachfolge, Übergang auf verbundene Gesellschaft

- 2.1 Sollte der Auftraggeber in seiner jetzigen Rechtsform nicht mehr fortbestehen, tritt – soweit gesetzlich zulässig – sein Rechtsnachfolger in sämtliche Rechte und Pflichten aus diesem Vertrag ein. Die jeweiligen Pflichten der Parteien gelten unverändert fort.
- 2.2 Der Auftragnehmer ist verpflichtet, im Falle eines Übergangs auf die vorgenannte Gesellschaft seine Leistungen so fortzuführen, dass eine Unterbrechung der Leistungserbringung vermieden wird. Die Parteien werden hierzu eine geordnete Übergabe planen und durchführen.

3. Leistungsumfang und Leistungsbausteine

3.1 Allgemeiner Leistungsumfang

Der Auftragnehmer erbringt Beratungs-, Analyse-, Konzeptionierungs- und Unterstützungsleistungen im Bereich der Informationssicherheit sowie der Nutzbarkeit für sichere mobile Identitäten zur Unterstützung der Konzeption, Entwicklung, Absicherung und kontinuierlichen Weiterentwicklung der EUDI-Wallet und ihres Ökosystems. Die Leistungen werden bedarfsgerecht und ohne Mindestabnahme von den relevanten Projektteams des Auftraggebers über das vom Auftraggeber bereitgestellte Ticketsystem beauftragt. Die konkrete Ausgestaltung der Leistungen erfolgt jeweils durch Tickets, in denen der zugehörige Leistungsbaustein, die Aufgabenstellung sowie etwaige Lieferobjekte festgelegt werden. Die Leistungsbeschreibung „Unterstützungsleistungen im Bereich Informationssicherheit für EUDI-Wallet“ konkretisiert die nachfolgenden Leistungsbausteine und ist integraler Bestandteil dieses Vertrages.

3.2 Sichere Systementwicklung für mobile Identitäten

3.2.1 Fortlaufende Risikoanalyse und Sicherheitskonzept

Der Auftragnehmer begleitet und moderiert eine entwicklungsbegleitende Risikoanalyse der System- und Sicherheitsarchitektur der EUDI-Wallet und ihres Ökosystems und leitet, bewertet und priorisiert daraus Maßnahmen zur Erreichung der relevanten Schutzziele in Form eines Sicherheitskonzepts. Risikoanalyse und Sicherheitskonzept werden als lebende Dokumente mit geeigneter Versionierung und Änderungsdocumentation gepflegt und bei Bedarf an formelle Vorgaben angepasst.

3.2.2 Technischer Entwurf für die Architektur des Schwachstellenmanagements

Der Auftragnehmer unterstützt den Auftraggeber beim Entwurf einer technischen Zielarchitektur für das Schwachstellenmanagement auf mobilen Endgeräten (Android/iOS), einschließlich Quellen- und Feed-Integration, Risikobewertung, Remediation-Prozessen und SLA-Definitionen. Die Zielarchitektur ist in das Sicherheitskonzept, die Betriebsprozesse sowie in die Monitoring- und Telemetrie-Landschaft des Auftraggebers zu integrieren.

3.2.3 Dokumentation der Sicherheitsarchitektur und der kryptografischen Methoden

Der Auftragnehmer unterstützt fortlaufend bei der Strukturierung und Weiterentwicklung des Architekturkonzept der EUDI-Wallet (funktionale und nicht-funktionale Anforderungen, Komponenten, Schnittstellen, Datenflüsse) und arbeitet die Sicherheitsarchitektur aus. Er bewertet und beschreibt die eingesetzten kryptografischen Verfahren (einschließlich Algorithmen, Protokolle, Schlüsselmanagement, Nutzung sicherer Hardware und Trustmodelle) in einer Form, die als Grundlage für Prüfungen, Zertifizierungen und Sicherheitsbewertungen durch Dritte dienen kann.

3.2.4 Begleitung der Entwicklung der technischen EUDI-Wallet-Architektur

Der Auftragnehmer begleitet die Refinement- und Design-Phasen der Entwicklungsteams des Auftraggebers und unterstützt bei der sicherheits- und datenschutzgerechten Ausgestaltung der EUDI-Wallet-Architektur. Er bewertet und empfiehlt Umsetzungsoptionen insbesondere zu Build- und Runtime-Sicherheit, Hardening, Secure Storage, Secure Channel, Trusted UI, Anti-Tamper-Maßnahmen und Jailbreak-/Root-Detection sowie zu sicherheitstechnischen Funktionen wie Key Attestation, App Attestation, Plattform-/Device Attestations und Remote Integrity Checking.

3.3 Compliance zu eIDAS 2.0 und nationaler eIDAS-Umsetzung

3.3.1 Fortlaufende Konformitätsanalyse der Architektur

Der Auftragnehmer unterstützt bei der fortlaufenden Konformitätsanalyse der Ziel- und Ist-Architektur gegen die Anforderungen der einschlägigen Technischen Richtlinien und weiteren relevanten Vorgaben durch. Er erstellt und pflegt ein Konformitätsanalyse-Dokument einschließlich Evidenzen, GAP-Analyse und Maßnahmenplan und unterstützt die Vorbereitung der Bewertung durch zuständige Stellen, insbesondere durch Erstellung von Unterlagen, Nachweisen, Testkonzepten und durch die Zusammenarbeit mit beauftragten Prüflaboren.

3.3.2 Begleitung und Unterstützung beim Austausch mit sicherheits- und datenschutzrelevanten Stakeholdern

Der Auftragnehmer unterstützt den Auftraggeber strukturiert beim Austausch mit sicherheits- und datenschutzrelevanten Stakeholdern, insbesondere mit zuständigen Behörden und Aufsichtsstellen. Er erstellt Entscheidungs- und Freigabeunterlagen, wirkt an Bewertungs- und Abstimmungsprozessen mit und nimmt an Reviews und Workshops mit den genannten Stakeholdern teil.

3.3.3 Begleitung von Bewertungs- und Zertifizierungsprozessen

Der Auftragnehmer begleitet Bewertungs- und Zertifizierungsprozesse einschließlich der Erstellung und Pflege von Evaluierungs- und Zertifizierungsunterlagen wie Security Targets und weiteren sicherheitsrelevanten Profilen und stimmt diese mit den zuständigen Stellen ab.

3.4 Nutzbarkeit für sichere mobile Identitäten

3.4.1 Durchführung qualitativer und quantitativer Nutzer- und Akzeptanzstudien

Der Auftragnehmer führt qualitative und quantitative Nutzer- und Akzeptanzstudien zur EUDI-Wallet und ihren Nutzungsszenarien durch und bringt einschlägige Erkenntnisse aus vergleichbaren Projekten ein. Er ist sicher in der Anwendung von plattformspezifischen Design-Bibliotheken und -Systemen und der Erstellung eigener Wireframes, Prototypen und Beiträgen. Er führt Expertenreviews und Validierungen von Wireframes und Screendesigns nach relevanten Normen und Standards hinsichtlich Verständlichkeit, Nutzungsbereitschaft und Nutzervertrauen durch und bereitet, dokumentiert und evaluiert entsprechende Nutzerstudien.

3.4.2 Analyse von Barrierefreiheit in den Endnutzeranwendungen

Der Auftragnehmer prüft und bewertet die Barrierefreiheit der EUDI-Wallet für die Plattformen iOS und Android durch Expertenreviews und Validierung nach einschlägigen Standards zur digitalen Barrierefreiheit. Er bereitet Nutzerstudien zur Barrierefreiheit vor, führt sie durch, wertet sie aus und stellt die Ergebnisse in Form geeigneter Dokumentationen und Handlungsempfehlungen zur Weiterentwicklung der App bereit.

3.5 Sonstige IT-Security-bezogene Anforderungen

Über die vorstehend beschriebenen Leistungsbausteine hinaus kann der Auftraggeber den Auftragnehmer bei Bedarf mit weiteren Beratungs- und Unterstützungsleistungen im Bereich Informationssicherheit beauftragen, sofern der Auftragnehmer über die hierfür erforderliche fachliche Expertise verfügt und die Leistungen mit geeignetem Personal erbringen kann. Mögliche Themenfelder sind insbesondere:

- Unterstützung des Security Operations Centre (SOC) bei der Reaktion auf und Eindämmung von Cybersicherheitsvorfällen sowie bei der Ausarbeitung von Strategien zur Schadensbegrenzung, ggf. auch kurzfristig,
- Analyse, Bewertung und Einführung moderner Sicherheits-, Datenschutz- und Kryptografietechnologien, einschließlich Differential Privacy, Zero-Knowledge-Verfahren, Zero-Trust-Architekturen, quantenresistenter Kryptografie, Maßnahmen zur Kryptoagilität sowie Konzeption, Bewertung und Absicherung von Machine-Learning-Verfahren mit Fokus auf Informationssicherheit, Datenschutz und Schutz sensibler Daten.
- Die Beauftragung solcher zusätzlichen Leistungen erfolgt ebenfalls über das Ticketsystem auf Grundlage dieser Rahmenvereinbarung; Art, Umfang, Zielsetzung und erwartete Lieferobjekte sind im jeweiligen Ticket zu konkretisieren.

4. Lieferobjekte, Dokumentation und Qualität

- 4.1 Der Auftragnehmer erstellt die in der Leistungsbeschreibung definierten Lieferobjekte, insbesondere:
- Risikoanalysebericht und aktualisiertes Sicherheitskonzept (laufend),
 - Konformitätsmatrix zur TR-03107-1 inkl. GAP- und Maßnahmenplan,
 - Architektur- und Kryptodokumentation (inkl. Datenfluss- und Sequenzdiagrammen),
 - Zielbild Vulnerability-Management (Mobile) und Betriebs-/SLA-Konzept,
 - technische Design-Reviews, Attestations-Guides, Hardening-Guidelines,
 - Protokolle und Unterlagen aus Behörden-/Stakeholder-Terminen,
 - Security Targets und weitere Sicherheitsprofile.
- 4.2 Der Auftragnehmer übergibt die Lieferobjekte in den mit dem Auftraggeber abgestimmten Formaten. Die Übergabe umfasst einen Handover-Workshop, ein Betriebs- und Wartungskonzept sowie Unterlagen zur Wissenssicherung (Runbooks, Playbooks, Onboarding-Guides).
- 4.3 Die Qualität der Lieferobjekte muss mindestens die folgenden Kriterien erfüllen:
- Vollständigkeit und Nachvollziehbarkeit,
 - Prüfbarkeit gegen die einschlägigen technischen Richtlinien (insbesondere TR-03107-1),
 - Nachweis implementierter Controls in Design- und Code-Artefakten (evidenzbasiert),
 - Bestehen definierter Security-Gates (z.B. vollständiges Threat-Model, SAST/DAST-Befunde innerhalb definierter Schwellwerte, vorhandene SBOM, Remediation kritischer Schwachstellen).
- 4.4 Der Auftraggeber prüft die Lieferobjekte innerhalb angemessener Frist (höchstens fünf Werktage) und kann die Abnahme von Teilergebnissen erklären oder begründete Mängel rügen. Der Auftragnehmer ist verpflichtet, gerügte Mängel unverzüglich und unentgeltlich zu beheben.
- 4.5 Der Auftragnehmer räumt dem Auftraggeber an sämtlichen im Rahmen dieses Vertrages entstehenden Arbeitsergebnissen und Lieferobjekten ausschließliche, zeitlich, räumlich und inhaltlich unbeschränkte Nutzungsrechte ein, einschließlich des Rechts zur Vervielfältigung, Bearbeitung, Verbreitung, öffentlichen Zugänglichmachung sowie zur Übertragung und Unterlizenzierung; umfasst ist insbesondere die Weitergabe und Nutzung gegenüber beauftragten Dritten, zuständigen Behörden, Aufsichtsstellen und Prüflaboren für Bewertungs-, Zertifizierungs- und Projektzwecke. Die Rechte können im Einklang mit Ziff. 2 auf eine benannte Tochter- oder Schwestergesellschaft übertragen werden. Rechte an vorbestehendem, nicht projektspezifisch geschaffenem Know how, Methoden, Templates und Tools (Hintergrundrechte) verbleiben beim Auftragnehmer. Soweit Hintergrundrechte in Arbeitsergebnissen enthalten sind, räumt der Auftragnehmer dem Auftraggeber eine einfache, unentgeltliche, zeitlich, räumlich und inhaltlich unbeschränkte Lizenz ein, diese Hintergrundrechte in dem zur bestimmungsgemäßen Nutzung, Bearbeitung und Verwertung der Arbeitsergebnisse erforderlichen Umfang zu nutzen.

5. Zusammenarbeit, Governance und Arbeitsweise

- 5.1 Der Auftraggeber arbeitet in einem agilen Projektrahmen mit zweiwöchigen Sprints. Der Auftragnehmer fügt sich in diesen Arbeitsrhythmus ein und nimmt bedarfsgerecht an den zugehörigen Terminen (insbesondere Sprint-Refinement, Planning, Review, Retrospektiven sowie weiteren Regelterminen) aktiv teil.
- 5.2 Die Erfassung, Beschreibung und Nachverfolgung von Arbeitspaketen sowie die Dokumentation von Arbeitsfortschritten erfolgen ausschließlich über das vom Auftraggeber vorgegebene Ticketsystem. Der Auftragnehmer nutzt dieses System vollständig, zeitnah und hält den Bearbeitungsstand der ihm zugewiesenen Aufgaben fortlaufend aktuell. Ergebnisse aus Abstimmungsgesprächen, Beratungssitzungen und Workshops, die Auswirkungen auf Umfang, Inhalt, Fristen oder Budget eines Tickets haben, werden vom Auftragnehmer im Ticketsystem dokumentiert und vom Auftraggeber freigegeben. Nur die im Ticketsystem dokumentierten und freigegebenen Anpassungen sind für die Parteien verbindlich.
- 5.3 Zur Sicherstellung einer effizienten Zusammenarbeit vereinbaren die Parteien ein Mindestmaß an Kooperationsformaten, insbesondere:
- regelmäßige Abstimmungsgespräche zwischen Auftragnehmer, Product Owner und weiteren Teammitgliedern des Auftraggebers zur Bewertung von Status, wesentlichen Problemen und Auswirkungen auf Zeitplan und Budget,
 - Beratungssitzungen auf Anfrage der Projektmitglieder des Auftraggebers,
 - bei Bedarf Workshops vor Ort im Zusammenhang mit Sicherheitsbewertungen und Entscheidungsprozessen.
- 5.4 Der Auftragnehmer stellt die Verfügbarkeit seiner Leistungen auf Stundenbasis jeweils für den Folgemonat sicher; der Umfang wird im Voraus mit dem Auftraggeber abgestimmt. Die Arbeitszeiten sind transparent zu halten.
- 5.5 Der Auftragnehmer erfasst seine Arbeitszeiten und fügt den monatlichen Rechnungen eine detaillierte Stundenaufstellung bei. Zur Einhaltung des Budgetrahmens stimmt sich der Auftragnehmer regelmäßig mit der hierfür benannten Ansprechperson des Auftraggebers ab. Abgerechnete Arbeitsstunden, die über den vereinbarten budgetierten Betrag hinausgehen, werden nicht vergütet, sofern der Auftraggeber nicht vorab schriftlich eine Budgeterhöhung freigegeben hat.
- 5.6 Für das Vergabeverfahren ist Deutsch die maßgebliche Sprache. Im Projekt sowie im Austausch mit externen Stakeholdern wird vom Auftragnehmer ein Austausch in deutscher und englischer Sprache erwartet.
- 5.7 Der Auftragnehmer benennt zu Beginn der Zusammenarbeit einen Single-Point-of-Contact für administrative Themen. Der Auftraggeber bevorzugt ein schlankes Kernteam auf Seiten des Auftragnehmers; die Durchführung ausgewählter Aufgaben durch weitere Teammitglieder im

Backoffice ist möglich. Referenzen und Stundensätze sämtlicher im Projekt eingesetzten Teammitglieder sind anzugeben.

6. Vergütung, Rahmenwert und Preisstruktur

- 6.1 Die Vergütung erfolgt auf Grundlage der im Angebot des Auftragnehmers und im beigefügten Preisblatt „Unterstützungsleistungen im Bereich Informationssicherheit für EUDI-Wallet“ vereinbarten Stundensätze, Tagessätze und ggf. Pauschalen. Das Preisblatt ist Bestandteil dieses Vertrages.
- 6.2 Der geschätzte Auftragswert dieser Rahmenvereinbarung beträgt 3.200.000 EUR netto. Zugleich vereinbaren die Parteien einen Höchstwert in Höhe von 3.500.000 EUR netto. Der Auftraggeber ist nicht verpflichtet, diesen Höchstwert auszuschöpfen. Der Auftragnehmer hat keinen Anspruch auf Abruf oder Vergütung über die tatsächlich beauftragten und erbrachten Leistungen hinaus.
- 6.3 Die Rahmenvereinbarung begründet keine Mindestabnahme. Ein Anspruch des Auftragnehmers auf Beauftragung eines bestimmten Mindestvolumens besteht nicht. Die Vergütung richtet sich nach den im jeweiligen Ticket bezeichneten Leistungsbausteinen und dem dort angegebenen Budgetrahmen. Abgerechnet werden ausschließlich Arbeitsstunden, die einem durch den Auftraggeber freigegebenen Ticket zugeordnet sind. Für die in 3.4 der Leistungsbeschreibung genannten Themenbereiche wird der Tagessatz des Leistungsbausteins „Sichere Systementwicklung für mobile Identitäten“ zugrunde gelegt.
- 6.4 Die Vergütung umfasst sämtliche für die vollständige Leistungserbringung erforderlichen Kosten, einschließlich üblicher Reise-, Transport- und Nebenkosten, sofern nicht im Preisblatt ausdrücklich abweichende Regelungen getroffen sind.
- 6.5 Rechnungen sind monatlich nachträglich auf Basis der tatsächlich erbrachten und im Ticketsystem dokumentierten Leistungen zu stellen und müssen eine prüffähige Aufstellung der geleisteten Stunden nach Personen, Leistungsbausteinen und Arbeitspaketen enthalten.

7. Laufzeit, Verlängerungsoptionen und Sonderkündigung

- 7.1 Dieser Vertrag tritt mit Zuschlagserteilung in Kraft und wird zunächst befristet für zwei (2) Jahre geschlossen.
- 7.2 Der Auftraggeber ist berechtigt, den Vertrag zweimal um jeweils ein Jahr zu verlängern. Übt der Auftraggeber eine Verlängerungsoption aus, teilt er dies dem Auftragnehmer mindestens drei Monate vor Ablauf der jeweiligen Vertragslaufzeit schriftlich mit. Erfolgt keine fristgerechte Mitteilung, endet der Vertrag mit Ablauf der jeweiligen Vertragslaufzeit.
- 7.3 Jede Partei kann den Vertrag aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist kündigen. Ein wichtiger Grund liegt insbesondere vor, wenn:

- über das Vermögen der anderen Partei ein Insolvenzverfahren beantragt, eröffnet oder mangels Masse abgelehnt wird;
- die andere Partei erklärt, zur Leistungserbringung innerhalb der vereinbarten Fristen dauerhaft nicht in der Lage zu sein;
- die andere Partei trotz Abmahnung wiederholt oder schwerwiegend gegen wesentliche Vertragspflichten verstößt;
- die Fortsetzung des Vertrages dem Kündigenden unzumutbar ist.

7.4 Ungeachtet Ziffer 7.3 hat der Auftraggeber ein Sonderkündigungsrecht, diesen Vertrag mit Wirkung zum 31. Dezember 2026 zu kündigen, indem er dem Auftragnehmer spätestens bis zum 30. November 2026 eine schriftliche Kündigungserklärung zukommen lässt. Dieses Sonderkündigungsrecht kann ausschließlich aus Gründen in Anspruch genommen werden, die auf haushaltsbedingte Einschränkungen in Bezug auf den dem Auftraggeber genehmigten Haushalt für das betreffende Haushaltsjahr (Haushaltsmittel) zurückzuführen sind, und bedarf keiner weiteren Begründung über eine schriftliche Erklärung hinaus, in der die haushaltsrechtliche Grundlage der Kündigung bestätigt wird. Im Falle einer Kündigung gemäß dieser Ziffer 9.5 haftet der Auftraggeber nicht für dem Auftragnehmer entgangenen Gewinn oder Honorare, die nach dem Kündigungszeitpunkt angefallen wären; für die bis einschließlich des Wirksamwerdens der Kündigung aufgelaufene Vergütung haftet der Auftraggeber weiterhin.

8. Informationssicherheit, Compliance und Audit

- 8.1 Der Auftragnehmer und seine Unterauftragnehmer verfügen über eine Zertifizierung nach ISO/IEC 27001, SOC-2 Typ 2 oder über ein gleichwertiges Informationssicherheits-Managementsystem, gestaltet seine internen Verfahren und Prozesse so, dass sie mit den Anforderungen der ISO/IEC 27001 nicht in Widerspruch stehen, und ist verpflichtet die entsprechenden Zertifikate sowie Management Summaries von Überwachungsaudits dem Auftraggeber unaufgefordert jährlich in Textform bereitstellen.
- 8.2 Der Einsatz von Unterauftragnehmern, die nicht bereits im Angebot des Auftragnehmers benannt und vom Auftraggeber zugelassen wurden, bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Alle Unterauftragnehmer sind vertraglich dazu zu verpflichten, denselben Sicherheits- und Datenschutzstandards zu genügen wie der Auftragnehmer.
- 8.3 Der Auftraggeber betreibt ein ISO-27001-konformes Informationssicherheits-Managementsystem (ISMS). Der Auftragnehmer unterstützt die Einhaltung dieser Compliance durch geeignete organisatorische und technische Maßnahmen sowie durch Bereitstellung der für Prüfungen und Nachweise erforderlichen Informationen.
- 8.4 Dem Auftraggeber oder einem von ihm beauftragten, zur Verschwiegenheit verpflichteten Dritten steht nach angemessener vorheriger Ankündigung das Recht zu, die Einhaltung der Sicherheitsanforderungen sowie der technischen und organisatorischen Maßnahmen des Auftragnehmers (einschließlich derjenigen von Unterauftragnehmern, soweit diese die Leistungserbringung betreffen) zu auditieren. Der Auftragnehmer wirkt an solchen Audits angemessen mit. Das Auditierungsrecht umfasst neben der Prüfung der Sicherheitsanforderungen auch die

Überprüfung der Einhaltung weiterer vertraglicher Vorgaben, soweit diese mit Informationssicherheit, Datenschutz oder Compliance in Zusammenhang stehen. Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage regelmäßig, mindestens jedoch einmal jährlich, strukturierte Performance- und Compliance-Reports zur Verfügung, die insbesondere den Stand der Informationssicherheit, Ergebnisse interner und externer Audits sowie den Status wesentlicher Maßnahmen zur Risikominderung dokumentieren. Der Auftraggeber beauftragt für Audits keine direkten Wettbewerber des Auftragnehmers. Die Auditrechte werden nur im rechtlich zulässigen Umfang und unter Wahrung berechtigter Geheimhaltungsinteressen des Auftragnehmers ausgeübt; sie beschränken sich auf abgrenzbare Räumlichkeiten sowie auf solche Unterlagen und Informationen, deren Einsicht zur Prüfung der vertraglich vereinbarten Sicherheits-, Datenschutz- und Compliance-Anforderungen erforderlich ist. Ein unmittelbarer Zugriff auf produktive IT-Systeme des Auftragnehmers oder seiner Unterauftragnehmer ist nicht geschuldet. Audits erfolgen grundsätzlich anlassbezogen; daneben kann höchstens einmal innerhalb von zwölf Monaten ein planmäßiges Audit durchgeführt werden. Die Pflicht des Auftragnehmers zur regelmäßigen Bereitstellung von Performance- und Compliance-Reports nach dieser Ziffer bleibt unberührt.

- 8.5 Der Auftragnehmer unterstützt sonstige Compliance-, Sicherheitsbewertungs- und Prüfprozesse durch Bereitstellung geeigneter Dokumentationen, Reports und technischer Informationen, die für unabhängige Prüfungen oder Zertifizierungen erforderlich sind.
- 8.6 Der Auftragnehmer hat bei der gesamten Leistungserbringung die Prinzipien von Privacy by Design und Privacy by Default zu berücksichtigen und aktiv in seine Architektur-, Sicherheits- und Prozesskonzepte einzubetten. Datenschutzerfordernisse sind integraler Bestandteil der jeweiligen Lösungskonzepte und nicht nachgelagerte Zusatzanforderungen.
- 8.7 Der Auftragnehmer ist verpflichtet, sicherheitsrelevante Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit der Systeme, Daten oder Dienste des Auftraggebers beeinträchtigen oder voraussichtlich beeinträchtigen können, dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach erstmaliger Kenntnisnahme zu melden. Die Meldung hat mindestens eine Beschreibung des Vorfalls, der betroffenen Systeme und Daten, bekannte oder vermutete Ursachen sowie zunächst ergriffene Maßnahmen zu enthalten. Der Auftragnehmer kooperiert vollumfänglich und transparent mit dem Auftraggeber bei der Untersuchung, Eindämmung und Behebung des Vorfalls und stellt alle hierfür erforderlichen Informationen sowie fachkundiges Personal zur Verfügung.

9. Gewährleistung der Beratungsleistungen

- 9.1 Der Auftragnehmer gewährleistet, dass er über die für die Erbringung der Leistungen erforderliche Fachkunde, Erfahrung und Leistungsfähigkeit verfügt und die Leistungen nach dem jeweils aktuellen Stand der Technik sowie unter Berücksichtigung anerkannter Standards und Best Practices (insbesondere BSI-Richtlinien, einschlägige ISO-Normen, OWASP-Standards) erbringt.

- 9.2 Der Auftragnehmer erbringt seine Beratungsleistungen so, dass sie die Ziele des Projekts, insbesondere hohe Informationssicherheit, Datenschutz, Barrierefreiheit und Nutzbarkeit der EUDI Wallet-Lösungen, unterstützen und nicht beeinträchtigen.
- 9.3 Stellt der Auftraggeber Mängel in den Beratungsleistungen fest – etwa unzutreffende, widersprüchliche oder unvollständige Empfehlungen –, ist der Auftragnehmer verpflichtet, diese nach entsprechender Rüge und innerhalb einer angemessenen Frist unentgeltlich zu korrigieren.

10. Qualifikation, Einsatz und Wechsel des Personals

- 10.1 Der Auftragnehmer setzt für die Erbringung der Leistungen ausschließlich solches Personal ein, das die im Vergabeverfahren für dieses Projekt definierten Eignungs-, Qualifikations- und Erfahrungsanforderungen erfüllt, insbesondere die in den Zuschlags- und Eignungskriterien (Teil A und Teil C der Vergabeunterlagen, einschließlich der dort beschriebenen Leistungsbausteine „Sichere Systementwicklung für mobile Identitäten“, „Compliance zu eIDAS 2.0 und nationale eIDAS-Umsetzung“ und „Nutzbarkeit für sichere mobile Identitäten“, der jeweils geforderten Mitarbeiterprofile, der Fachkenntnisse und der Referenzanforderungen) festgelegten Mindestanforderungen an Berufserfahrung, Fachpraxis und Spezialisierung. Diese Anforderungen gelten als vertraglich vereinbarter Mindeststandard für alle vom Auftragnehmer eingesetzten Personen. Der Auftraggeber kann innerhalb des vertraglichen Höchstwertes zusätzliches qualifiziertes Personal des Auftragnehmers über das Ticketsystem abrufen; Gegenstand, Qualifikation und Vergütung richten sich unverändert nach Ziff. 3, 6 und 10. Der Abruf dient ausschließlich der Erfüllung der vereinbarten Leistungsbausteine und ändert den Gesamtcharakter des Auftrags nicht. Der Auftragnehmer stellt angefragtes, qualifiziertes Personal innerhalb angemessener Frist bereit; Ziff. 10.3–10.8 gelten entsprechend. Der Auftragnehmer gewährleistet, dass die als Schlüsselpersonal benannten Personen die ihnen zugewiesenen Leistungen persönlich erbringen und nicht lediglich nominal als Projektverantwortliche fungieren. Eine überwiegende Delegation der operativen Aufgaben auf nicht benanntes, weniger qualifiziertes Backoffice-Personal ist unzulässig.
- 10.2 Der Auftragnehmer stellt sicher, dass die mit dem Angebot eingereichten und in der Wertung berücksichtigten Profile („Schlüsselpersonal“) tatsächlich in dem im Angebot und in den Vergabeunterlagen vorgesehenen Umfang im Projekt eingesetzt werden. Abweichungen hiervon bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers.
- 10.3 Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf dessen Verlangen jederzeit geeignete Nachweise zur Qualifikation und Erfahrung des eingesetzten Personals vorzulegen (z. B. Lebensläufe, Projektlisten, Referenzbestätigungen, Zertifikate, Schulungsnachweise), aus denen die Erfüllung der in den Vergabeunterlagen definierten Anforderungen hervorgeht. Der Auftragnehmer hat diese Nachweise aktuell zu halten und wesentliche Änderungen unverzüglich mitzuteilen. Der Auftragnehmer darf die in den Vergabeunterlagen bewerteten Qualifikationen nicht dadurch umgehen, dass die benannten Schlüsselpersonen lediglich sporadisch oder in untergeordnetem Umfang im Projekt mitwirken und die laufende Leistungserbringung überwiegend durch im Vergabeverfahren nicht berücksichtigtes oder geringer qualifiziertes

Personal erfolgt. Soweit zur Unterstützung Backoffice-Personal eingesetzt wird, erfolgt dies nur ergänzend; fachliche Verantwortung, Steuerung der Arbeitspakete und wesentliche operative Aufgaben verbleiben bei den benannten Personen. Ein entsprechender Einsatz- und Verantwortungszuschnitt ist dem Auftraggeber auf Verlangen in geeigneter Form nachzuweisen.

10.4 Ein Wechsel von Schlüsselpersonal ist nur zulässig, wenn

- die zu ersetzende Person aus Gründen, die nicht auf ein vertragswidriges Verhalten des Auftragnehmers zurückzuführen sind, dauerhaft nicht mehr zur Verfügung steht oder der Austausch aus sachlichen Gründen erforderlich ist, und
- die ersetzende Person mindestens gleichwertige Qualifikationen und Erfahrungen aufweist, die den im Vergabeverfahren definierten Anforderungen entsprechen und diese im Hinblick auf die für die Wertung maßgeblichen Kriterien mindestens erreichen.

10.5 Der Auftragnehmer hat beabsichtigte Personalwechsel des Schlüsselpersonals dem Auftraggeber vorab schriftlich anzuzeigen. Mit der Anzeige sind alle erforderlichen Nachweise zur Qualifikation und Erfahrung der Ersatzperson vorzulegen. Der Auftraggeber kann innerhalb einer angemessenen Frist begründet widersprechen, wenn die vorgelegten Nachweise die Gleichwertigkeit der Qualifikation und Erfahrung nicht belegen. Bis zur Einigung über eine Ersatzperson bleibt der Auftragnehmer zur ordnungsgemäßen Leistungserbringung mit geeignetem Personal verpflichtet.

10.6 Der Auftraggeber ist berechtigt, den Austausch einzelner Mitarbeiter zu verlangen, wenn objektive Gründe vorliegen, insbesondere wenn diese trotz Abmahnung wiederholt oder schwerwiegend gegen wesentliche Vertragspflichten verstoßen, die geforderte fachliche Qualität nachhaltig verfehlen oder die vertraglich vereinbarten Qualifikationsanforderungen nicht (mehr) erfüllen. Der Auftragnehmer hat in diesem Fall innerhalb einer vom Auftraggeber gesetzten angemessenen Frist geeignetes Ersatzpersonal mit gleichwertiger Qualifikation und Erfahrung zu stellen.

10.7 Verletzt der Auftragnehmer schuldhaft die Verpflichtungen aus dieser Klausel, insbesondere indem er nicht ausreichend qualifiziertes Personal einsetzt, geforderte Nachweise trotz Fristsetzung nicht oder nicht vollständig vorlegt oder Personalwechsel ohne vorherige Anzeige bzw. ohne Zustimmung des Auftraggebers vornimmt, ist der Auftraggeber nach erfolgloser Abmahnung und angemessener Fristsetzung zur Abhilfe berechtigt,

- die Vergütung für von nicht ausreichend qualifiziertem Personal erbrachte Leistungen angemessen zu kürzen oder deren Vergütung zu verweigern,
- Ersatz der durch den Pflichtverstoß entstandenen Mehrkosten zu verlangen (z. B. für erforderlich werdende Nacharbeiten oder zusätzliche Prüfungen), sowie
- den Vertrag aus wichtigem Grund außerordentlich zu kündigen, wenn dem Auftraggeber ein Festhalten am Vertrag unter Berücksichtigung der Schwere oder Wiederholung der Verstöße unzumutbar ist.

- 10.8 Weitergehende gesetzliche und vertragliche Rechte des Auftraggebers, insbesondere Rechte aus Gewährleistung, Schadensersatz und Kündigung aus wichtigem Grund, bleiben unberührt.

11. Haftung und Versicherung

- 11.1 Der Auftragnehmer haftet unbeschränkt für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung beruhen, sowie für sonstige Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung beruhen.
- 11.2 Für Schäden, die auf einer leicht fahrlässigen Pflichtverletzung des Auftragnehmers beruhen, ist die Haftung auf 500.000 EUR je Schadensfall begrenzt. Übersteigt der zweifache Auftragswert (bezogen auf den jeweiligen Einzelauftrag zum Zeitpunkt der Beauftragung) den Betrag von 500.000 EUR, ist die Haftung auf den zweifachen Auftragswert begrenzt.
- 11.3 Die Haftung nach dem Produkthaftungsgesetz, aus ausdrücklich übernommenen Garantien sowie in Fällen zwingender gesetzlicher Haftung bleibt unberührt.
- 11.4 Der Auftragnehmer ist verpflichtet, für die gesamte Laufzeit dieses Vertrages eine den in der Ausschreibung vorgegebenen Anforderungen entsprechende Versicherung zu unterhalten und dies dem Auftraggeber auf Nachfrage nachzuweisen. Kommt der Auftragnehmer dieser Pflicht trotz angemessener Fristsetzung nicht nach, ist der Auftraggeber berechtigt, den Vertrag aus wichtigem Grund zu kündigen.

12. Vertragsstrafe bei Verstößen gegen Tariftreuepflichten nach dem BTTG

- 12.1 Der Auftragnehmer ist verpflichtet, sämtliche sich aus dem Bundestariftreuegesetz (BTTG) ergebenden Pflichten, insbesondere das Tariftreueversprechen gemäß § 3 BTTG sowie die Nachweis- und Mitwirkungspflichten gemäß § 9 BTTG, für die zur Leistungserbringung eingesetzten Arbeitnehmerinnen und Arbeitnehmer einzuhalten und dies auch bei von ihm eingesetzten Nachunternehmern und Verleihern sicherzustellen.
- 12.2 Der Auftraggeber und der Auftragnehmer vereinbaren für schuldhafte Verstöße des Auftragnehmers gegen die in Ziffer 12.1 genannten Pflichten eine Vertragsstrafe. Die Vertragsstrafe beträgt je festgestelltem Verstoß höchstens ein (1) Prozent des Nettoauftragswertes dieses Vertrages; die Summe aller Vertragsstrafen aus diesem Vertrag ist auf höchstens zehn (10) Prozent des Nettoauftragswertes begrenzt. Maßgeblich ist die Nettoauftragssumme in ihrer objektiv richtigen Höhe unter Berücksichtigung etwaiger nachträglicher Verringerungen des Auftragswertes.
- 12.3 Die Vertragsstrafe ist verwirkt, wenn die Prüfstelle Bundestariftreue einen Verstoß des Auftragnehmers im Sinne von § 13 BTTG durch bestandskräftigen oder nicht mehr anfechtbaren Verwaltungsakt festgestellt hat. Bei der Festsetzung der konkreten Höhe der Vertragsstrafe innerhalb des Rahmens nach Ziffer 12.2 sind insbesondere die Schwere des Verstoßes, die

Anzahl der betroffenen Arbeitnehmerinnen und Arbeitnehmer, die Dauer und das Ausmaß der Abweichung von den zu gewährenden Arbeitsbedingungen sowie der Grad des Verschuldens zu berücksichtigen.

- 12.4 Der Auftraggeber ist berechtigt, die verwirkte Vertragsstrafe nach Abschluss der Auftragsausführung geltend zu machen; weitergehende gesetzliche Fristen und Verjährungsregelungen bleiben unberührt. Der Auftraggeber kann verwirkte Vertragsstrafen insbesondere durch Aufrechnung gegen Vergütungsansprüche des Auftragnehmers oder durch Einbehalt von noch offenen Vergütungsbeträgen geltend machen.
- 12.5 Die Geltendmachung der Vertragsstrafe lässt das Recht des Auftraggebers unberührt, Schadensersatz zu verlangen sowie den Vertrag aus wichtigem Grund, insbesondere im Falle eines nach § 13 BTTG festgestellten Verstoßes, außerordentlich fristlos zu kündigen.
- 12.6 Eine gezahlte oder einbehaltene Vertragsstrafe wird auf einen weitergehenden Schadensersatzanspruch des Auftraggebers wegen desselben Verstoßes angerechnet.

13. Vertraulichkeit

- 13.1 Die Parteien verpflichten sich, alle im Rahmen dieses Vertrages erhaltenen vertraulichen Informationen der jeweils anderen Partei streng vertraulich zu behandeln und ausschließlich für Zwecke der Durchführung dieses Vertrages zu verwenden. Die Vertraulichkeitsverpflichtung gilt für einen Zeitraum von fünf (5) Jahren ab Beendigung dieses Vertrages. Unberührt bleiben strengere gesetzliche Pflichten sowie der Schutz von personenbezogenen Daten und von Informationen, die von der offenlegenden Partei ausdrücklich schriftlich als Geschäftsgeheimnis bezeichnet wurden; für diese gilt die Vertraulichkeitsverpflichtung zeitlich unbefristet, solange die jeweiligen Schutzvoraussetzungen bestehen. Die Ausnahmen nach Ziff. 13.2 bleiben unberührt.
- 13.2 Von der Vertraulichkeitsverpflichtung ausgenommen sind Informationen, die:
- der empfangenden Partei bereits vor der Offenlegung nachweislich bekannt waren,
 - ohne Verletzung dieses Vertrages allgemein bekannt werden,
 - von einem dazu berechtigten Dritten ohne Vertraulichkeitsverpflichtung offenbart werden oder
 - aufgrund gesetzlicher Vorschriften oder behördlicher bzw. gerichtlicher Anordnungen offenzulegen sind.

Soweit rechtlich zulässig, informiert die zur Offenlegung verpflichtete Partei die andere Partei vorab über die beabsichtigte Offenlegung und gibt ihr Gelegenheit, gegen die Offenlegung vorzugehen.

- 13.3 Die Parteien stellen sicher, dass ihre Mitarbeiterinnen und Mitarbeiter sowie beauftragte Dritte, die Zugriff auf vertrauliche Informationen erhalten, mindestens in dem Umfang zur Verschwiegenheit verpflichtet werden, wie es dieser Vertrag vorsieht.

14. Sprache, anwendbares Recht und Gerichtsstand

- 14.1 Die deutsche Sprachfassung dieses Vertrages ist die rechtlich verbindliche Fassung. Übersetzungen dienen ausschließlich der Verständlichkeit.
- 14.2 Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).
- 14.3 Soweit gesetzlich zulässig, vereinbaren die Parteien als ausschließlichen Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag den Sitz des Auftragnehmers.

15. Schlussbestimmungen

- 15.1 Mit Beendigung des Vertrages hat der Auftragnehmer sämtliche vom Auftraggeber erhaltenen Unterlagen, Hilfsmittel, Materialien oder Gegenstände, die ihm zum Zwecke der Vertragsausführung überlassen wurden und nicht dauerhaft beim Auftragnehmer verbleiben sollen, unverzüglich und unaufgefordert an den Auftraggeber zurückzugeben. Elektronische Daten, die vertrauliche Informationen oder personenbezogene Daten des Auftraggebers enthalten, sind – soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen – sicher zu löschen. Auf Verlangen weist der Auftragnehmer die Löschung in geeigneter Weise nach.
- 15.2 Änderungen und Ergänzungen dieses Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Änderung dieses Schriftformerfordernisses.
- 15.3 Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder undurchführbar sein oder werden, so berührt dies die Wirksamkeit der übrigen Bestimmungen nicht. An die Stelle der unwirksamen oder undurchführbaren Bestimmung tritt eine wirksame Bestimmung, die dem mit der unwirksamen Bestimmung verfolgten wirtschaftlichen Zweck am nächsten kommt. Entsprechendes gilt im Falle einer Regelungslücke.
- 15.4 Nebenabreden bestehen nicht. Sämtliche Anlagen sind Bestandteil dieses Vertrages.

_____	_____	_____
(Ort)	(Datum)	(Unterschrift Auftragnehmer)

_____	_____	_____
(Ort)	(Datum)	(Unterschrift Auftraggeber)