Framework Agreement for Development Support

Award number: EINCC-256

Service Description

1. Objectives and Context

COMMON CODES GmbH (Common Codes, hereinafter “the Client”) intends to conclude a framework agreement with up to three contractors for software development support services for the national European Digital Identity Wallet (EUDI Wallet) in Germany and its surrounding ecosystem. This document describes the required services and roles.

The EU Digital Identity Wallet is an initiative of the European Commission that will provide EU citizens, residents and businesses with a digital identity and a personal digital wallet (EUDI Wallet). It allows them to prove their identity securely and easily when accessing digital services. The wallet app enables users to securely receive, store and share digital documents and credentials, and to sign documents electronically or to seal them. For example, it is intended to make it possible to provide the documents required for opening a new bank account, enrolling at a university abroad or applying for a job. Privacy must be protected at all times; the person concerned must be able to control which data is shared and who has access to it.

Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183 (eIDAS 2.0) enables the digital transformation of the public sector and ensures that more services are accessible digitally, including across borders. For businesses, it will be easier to offer online services throughout Europe, as the EUDI Wallet provides secure authentication and is available to every potential customer in the EU. Each Member State provides at least one version of the EUDI Wallet, built on the same common specifications.

On behalf of the Federal Ministry for Digital Transformation and Government Modernisation (BMDS), Common Codes carries out the project “EUDI Wallet Infrastructure” and, as part of this assignment, develops the national EUDI Wallet for Germany and its ecosystem components.

With this tender, the Client establishes a framework agreement for hands-on development support. The Client seeks specialists with proven, practical experience in the roles described in this Service Description, who support the Client in delivering specific service modules. The tender is not aimed at the delivery of a complete product by an external party.

2. Frameworks, standards and protocols

The EUDI Wallet is developed in a regulated and standards-driven environment. The Client therefore requires personnel with specific technical qualifications and practical experience in the fields of eIDAS, electronic identification and digital identity wallets, mobile applications and secure backend services, specifically:

- Experience with eIDAS 2.0 / Regulation (EU) No 910/2014 framework, Architecture and Reference Framework (ARF), and European Digital Identity Wallet Implementing Acts.
- Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API).
- Experience building secure mobile applications that balance security, privacy, and usability.
- Experience in applying accessibility requirements, including BITV 2.0, EN 301 549 and WCAG.

The bidder demonstrates this experience via the role profiles and the project references within the role profiles. References are assessed for their relevance to the requirements of the respective role description; references with a direct link to digital identity solutions, EUDI wallets, eID systems or comparable projects in the context of eIDAS are considered most relevant. References from other fields are considered only to the extent that they demonstrate the experience described above. The evidence is evaluated in accordance with the *Award Criteria* document.

3. Service modules

The services that can be called off under this framework agreement are grouped into the service modules described below. The service modules describe the scope of services and the expertise the Client expects – invoicing is based on person days delivered, service modules are not ordered separately. A call-off always refers to roles as set out in the section *Roles*, each of which is assigned to one service module. The Client may call off individual roles from one module, roles from several modules, or a cross-functional team combining several modules. The services are provided as capacity within the Client's product and engineering organisation, in accordance with the subsection *Delivery & acceptance model*.

Module #1 - Architecture, security and technical governance

Roles: Software Architect, Security Engineer
Scope: Defining and governing the technical architecture with regard to scalability, security, interoperability and modularity; selecting technologies and integration patterns aligned with open standards and eIDAS 2.0 framework; leading architecture and design reviews; maintaining architecture documentation and decision records; identifying and mitigating architectural risks; threat modelling, security reviews, reproduction and validation of attacks in test environments.

Module #2 - Mobile wallet development

Roles: iOS Developer, Android Developer

Scope: Developing and maintaining native iOS and Android components of the EUDI Wallet; implementing wallet functionality in line with product, UX, security and regulatory requirements; secure handling of credentials and cryptographic material; integration with backend services and standardised APIs; automated testing in CI/CD; accessibility and compatibility across supported platform versions.

Module #3 - Backend and integration development

Roles: Backend Developer, Integration Engineer
Scope: Developing and maintaining backend services supporting the EUDI Wallet ecosystem; designing and implementing secure APIs and integrations with the wallet applications and the Client's own systems; authentication, authorization, encryption, logging and resilience mechanisms; automated quality, security and performance checks in CI/CD; enabling external partners such as issuers and relying parties to integrate technically, including onboarding, integration material, a partner test environment, readiness checks before go-live and technical support during integration.

Module #4 - Product and delivery management

Roles: Product Owner
Scope: Translating priorities and requirements into a testable, traceable and continuously refined backlog; validating sprint outcomes against the Definition of Done and functional, security and accessibility requirements; coordinating development, operations and QA; aligning release planning with programme objectives.

Module #5 - Quality assurance and test automation

Roles: QA/automation Engineer
Scope: Owning QA processes and quality gates; designing and maintaining test automation frameworks; risk-based testing, test data management and traceable test and defect reporting.

Module #6 - Platform and operations engineering

Roles: DevOps/platform Engineer, Operations Engineer
Scope: Building and maintaining CI/CD pipelines for backend services and mobile apps, including code signing and App Store and Google Play release management, infrastructure as code, and monitoring and observability tooling (*DevOps/Platform Engineer*). Operating production services, including service levels, on-call, incident response and root cause analysis, capacity management, backup and restore, patching and recovery, in collaboration with the Client's support team. Both use open standards and non-proprietary technologies (*Operations Engineer*).

Module #7 - UX/UI design and accessibility

Roles: UI/UX Designer
Scope: User research, usability testing and workshops; wireframes, prototypes and design systems; definition of measurable usability and accessibility acceptance criteria; continuous improvement of the user experience based on user feedback.

Module #8 - App analytics

Roles: App Analytics Specialist

Scope: Designing and operating a privacy-preserving analytics concept for the iOS and Android wallet apps, based on data minimisation, purpose limitation and transparency; defining together with product, UX and development which questions analytics should answer, which metrics are needed and which data is deliberately not collected; building and maintaining the data flow from collection to analysis, including event schemas, data models and dashboards; analysing usage, stability and performance data along key user journeys; deriving actionable recommendations for UI/UX, architecture and development and measuring their impact; documenting the analytics concept, data flows and data protection measures for review by security and data protection experts.

4. Roles

In order to fulfil the service modules outlined above, the contractor is expected to offer certain roles. The roles are divided into two groups. The mandatory roles cover the Client's immediate needs in the current phase of the project that focuses on preparing for launch and hyper-care in the months following the go-live.

A bidder must provide all mandatory roles otherwise the tender is not taken into account. The optional roles cover capacities that the Client may require at a later stage, depending on the progress of the project. Bidders are invited to offer them, but are not required to do so. For each role, the Client provides a role description and requirements. The role profiles submitted with the tender must refer to them.

Irrespective of seniority, the submitted role profiles must demonstrate a high level of professional expertise and independence within their discipline. They are expected to independently manage complex tasks, take responsibility for their quality and delivery, resolve challenging problems and make sound professional decisions. They also contribute to the development of the wider team through guidance, reviews and knowledge sharing.

4.1 Group: Mandatory roles

The following roles are considered mandatory to participate in the tender at hand. If a bidder can not provide all roles in the required amount (6 role profiles in total), the bid will not be taken into account. The following roles are considered mandatory - role description and requirements are provided in separate tables below:

- Software Architect
- iOS Developer (2x – must be provided twice)
- Android Developer (2x – must be provided twice)
- Backend Developer

Each named person may be submitted for one role profile only. If the same person is named in more than one role profile of a bid, that person is counted solely for the first of these roles in the order in which the roles are listed in section 4 of the service description (mandatory roles before optional roles, iOS and Android developer #1 before #2). The remaining role profiles of that person are treated as not submitted: a missing mandatory role profile leads to the exclusion of the bid, a missing optional role profile is treated as an optional role that is not offered. The minimum professional experience is set out in Section 4.1 of the *Award Criteria* document.

Software Architect	
Role description	• Defines and governs the technical architecture with focus on scalability, security, maintainability, performance and modularity. • Selects technologies, frameworks and integration patterns aligned with open standards and eIDAS 2.0 framework. • Evolves and governs the wallet architecture, in particular key management and cryptographic devices, the trust model, attestation and revocation concepts, and reviews changes with regard to security and certifiability. • Provides technical leadership and drives secure-by-design engineering practices. • Leads architecture and design reviews and ensures consistency across services, APIs and interfaces. • Maintains architecture documentation, diagrams and architectural decision records (ADRs). • Identifies architectural risks and defines mitigation strategies.
Academic background	• Degree in Computer Science, Software Engineering or comparable technical field, or equivalent practical experience.
Professional Experience	• Experience with eIDAS 2.0 / Regulation (EU) No 910/2014 framework, Architecture and Reference Framework (ARF), and European Digital Identity Wallet Implementing Acts. • Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Experience building secure mobile applications that balance security, privacy, and usability. • Proven experience designing security-critical systems with key management and cryptographic devices (e.g. HSM, secure element), PKI and attestation concepts, preferably in identity or regulated environments. • Demonstrated architectural leadership across multiple teams, vendors or stakeholders.
Key skills	• Security architecture: key management, WSCD/WSCA, PKI and trust lists, attestation, revocation and status mechanisms, threat modelling. • API, integration and event-driven architectures. • Interoperability, secure communication and IAM. • Ability to translate complex requirements into robust, compliant architectures

Android Developer	
Role description	• Develops and maintains native Android components of the EUDI Wallet with focus on security, reliability, accessibility and performance.

	• Implements wallet functionality according to product, UX, security and regulatory requirements. • Applies modular architecture, clean code, dependency management and automated testing. • Implements secure handling of credentials, personal data, cryptographic material and authentication. • Integrates wallet functionality with backend services and standardised APIs. • Implements accessibility in the Android app (e.g. TalkBack support, reading and focus order, font scaling, contrast, keyboard operation) and approved design systems, and verifies it with assistive technologies and automated UI tests. • Integrates unit, integration, UI and security testing into CI/CD. • Participates in code reviews, technical refinement and troubleshooting. • Ensures compatibility across supported Android versions and devices.
Academic background	• Degree in Computer Science, Software Engineering, Mobile Computing or comparable practical experience.
Professional Experience	• Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Proven experience implementing hardware-backed key storage (Android Keystore with StrongBox), key attestation, device integrity checks (Play Integrity API) and biometric key binding (BiometricPrompt) in native Android applications. • Proven experience with proximity presentation according to ISO/IEC 18013-5 (QR, NFC, Bluetooth Low Energy) in native Android applications; experience reading the German identity card (eID) via NFC is an advantage. • Proven experience implementing accessibility in native Android applications according to EN 301 549, WCAG and BITV 2.0, including testing with TalkBack and external keyboards. • Proven experience delivering native Android applications with Kotlin. • Demonstrated experience integrating mobile applications with backend services and APIs.
Key skills	• Kotlin, Android SDK, Jetpack and Jetpack Compose. • Modular architecture and lifecycle management. • Android Keystore (incl. StrongBox), key attestation, Play Integrity API, BiometricPrompt, authentication and cryptography. • REST, JSON, OAuth/OIDC. • Automated unit, integration and UI testing. • Accessibility APIs (Jetpack Compose semantics and the View system), adaptive UI and font scaling. • CI/CD, Git, static analysis and dependency/security scanning. • Privacy-by-design.

iOS Developer	
Role description	• Develops and maintains native iOS components of the EUDI Wallet with focus on security, reliability, accessibility and performance. • Implements wallet functionality according to product, UX, security and regulatory requirements. • Applies modular architecture, clean code, dependency management and automated testing. • Implements secure handling of credentials, personal data, cryptographic material and authentication. • Integrates wallet functionality with backend services and standardised APIs. • Implements accessibility in the iOS app (e.g. VoiceOver support, reading and focus order, Dynamic Type, contrast, keyboard operation) and approved design systems, and verifies it with assistive technologies and automated UI tests. • Integrates unit, integration, UI and security testing into CI/CD. • Participates in code reviews, technical refinement and troubleshooting. • Ensures compatibility across supported iOS versions and Apple devices.
Academic background	• Degree in Computer Science, Software Engineering, Mobile Computing or comparable practical experience.
Professional Experience	• Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Proven experience implementing hardware-backed key storage (Secure Enclave), app and device attestation (App Attest) and biometric key binding (LocalAuthentication) in native iOS applications. • Proven experience with proximity presentation according to ISO/IEC 18013-5 (QR, NFC, Bluetooth Low Energy) in native iOS applications; experience reading the German identity card (eID) via NFC is an advantage. • Proven experience implementing accessibility in native iOS applications according to EN 301 549, WCAG and BITV 2.0, including testing with VoiceOver and external keyboards. • Proven experience delivering native iOS applications with Swift. • Demonstrated experience integrating mobile applications with backend services and APIs.
Key skills	• Swift, iOS SDK, SwiftUI and UIKit. • Modular architecture and application lifecycle. • Keychain, Secure Enclave, App Attest, LocalAuthentication, authentication and cryptography. • REST, JSON, OAuth/OIDC. • Automated unit, integration and UI testing. • Accessibility APIs (UIKit and SwiftUI), adaptive UI and Dynamic Type.

	• CI/CD, Git, static analysis and dependency/security scanning. • Privacy-by-design.

Backend Developer	
Role description	• Develops and maintains backend services supporting the EUDI Wallet ecosystem with focus on security, scalability, reliability and maintainability. • Develops and operates the backend services of the wallet provider (e.g. wallet instance registration, wallet attestation and revocation, status lists, remote key operations, verification of device attestations) and integrations with the wallet applications. • Implements APIs, business logic, data services and integrations according to product, architecture, security and regulatory requirements. • Implements authentication, authorisation, encryption, logging, monitoring and resilience mechanisms. • Ensures defined performance, scalability, availability and operational requirements. • Participates in architecture reviews, code reviews, technical refinement and troubleshooting.
Academic background	• Degree in Computer Science, Software Engineering, IT or comparable practical experience.
Professional Experience	• Proven experience delivering security-critical backend services, preferably identity or trust services with HSM-backed key operations (e.g. PKCS#11), PKI/X.509 and attestation-based authentication. • Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Experience building backend services for secure mobile applications that balance security, privacy, and usability. • Demonstrated experience designing APIs and integrations in complex or regulated environments. • Experience working with frontend, mobile, DevOps, architecture, security and product disciplines.
Key skills	• Application security, IAM, encryption, PKI/X.509, HSM integration and secure API design. • Java, Kotlin, Go, Python or comparable backend technologies. • REST APIs, service/microservice architectures and asynchronous communication. • Databases, data modelling, caching, messaging and distributed systems. • Automated testing and quality gates. • Containers and cloud-native development. • CI/CD, Git, vulnerability and supply-chain scanning.

4.2 Group: Optional roles

The following roles are considered optional. If a bidder cannot provide some or all of the optional roles, the bid will be taken into account, yet a minimum of one role needs to be provided in order to earn points in the category for optional roles under the *Price* or *Quality* award criteria. Please refer to the *Award Criteria* document for details. The following roles are considered optional - role description and requirements are provided in separate tables below:

- App Analytics Specialist
- DevOps/ Platform Engineer
- Integration Engineer
- Operations Engineer
- Product Owner
- QA/ Automation Engineer
- Security Engineer
- UI/UX Designer

App Analytics Specialist	
Role description	• Designs and implements a privacy-preserving self-hosted (and no third-party tracking SDKs) analytics concept for the iOS and Android wallet apps, based on data minimisation, purpose limitation and transparency. • Defines together with product, UX and development which questions analytics should answer, which metrics are needed and which data is deliberately not collected. • Builds and maintains the data flow from collection to analysis, including event schemas, data models and dashboards. • Analyses usage, stability and performance data, for example along key user journeys such as onboarding, issuance and presentation, and identifies friction points. • Turns findings into clear, actionable recommendations for UI/UX, architecture and development and measures the impact of the changes. • Monitors app quality indicators such as crash and error rates and performance together with the mobile developers. • Documents the analytics concept, data flows and data protection measures so that security and data protection experts can review them.
Academic background	• Degree in Computer Science, Data Science, Statistics, Engineering or a comparable field, or equivalent practical experience.
Professional Experience	• Experience designing and operating analytics collection for mobile apps on iOS and Android, ideally under privacy constraints. • Experience building data ingestion pipelines, event schemas and app instrumentation, including crash and performance monitoring. • Experience with server-side privacy measures such as removing IP addresses and other identifiers, log hygiene, pseudonymisation and retention limits.

	• Proven knowledge of data protection requirements, in particular GDPR and § 25 TDDDG (consent for storing and accessing information on the user's device), and of privacy-preserving techniques. • Demonstrated ability to turn data into recommendations and to explain them to designers, developers and non-technical stakeholders. • Experience working in cross-functional teams with product, UX, mobile development, architecture and security. • Experience with self-hosted or open-source analytics tooling for mobile apps without third-party tracking SDKs.
Key skills	• SQL, Python or R. • Statistics, funnel and cohort analysis. • Data modelling and dashboards. • Crash and performance monitoring with self-hosted tooling. • Server-side data processing with removal of identifiers and retention limit. • Privacy-preserving data collection (aggregation, anonymisation, pseudonymisation) and GDPR.

DevOps/ Platform Engineer	
Role description	• Builds and maintains deployment, monitoring and automation infrastructure for reliable software delivery. • Develops CI/CD pipelines for backend services and the native iOS and Android apps covering build, test, security scanning, code signing and release, and manages the app release process to the App Store and Google Play • Applies Infrastructure as Code, automated provisioning, configuration management and security-by-design. • Implements monitoring, observability and automated alerting. • Supports incident reviews with automation and tooling improvements, configuration/code reviews and continuous improvement. • Uses open standards and non-proprietary technologies to support interoperability and vendor independence. • Improves automation, resilience and operational reliability within agile delivery.
Academic background	• Degree in Computer Science or comparable technical field, or equivalent practical experience.
Professional Experience	• Experience building secure mobile applications that balance security, privacy, and usability. • Proven experience building and operating CI/CD for mobile apps (e.g. code signing, Fastlane or comparable, App Store and Google Play release management) and for backend services in distributed or regulated environments.

	• Demonstrated delivery of reliable, automated and secure software deployment processes.
Key skills	• GitLab CI, GitHub Actions, Jenkins or comparable tooling, including mobile build and release tooling (Xcode, Gradle, Fastlane or comparable). • Terraform, Ansible, Docker and Kubernetes. • Monitoring and observability with tools such as Prometheus, Grafana or ELK/EFK. • Secure configuration, automated testing and security scanning. • Bash, Python, Go and Git. • DevSecOps, policy enforcement and audit-ready automation.

Integration Engineer	
Role description	• Designs, develops and maintains tools that make it easier for relying parties and credential issuers to integrate with the EUDI Wallet ecosystem and that raise implementation quality across it (e.g. test and validation tools, libraries, sample code, developer utilities). • Builds prototypes and reference implementations that serve as blueprints for typical ecosystem scenarios (e.g. credential issuance and presentation). • Turns specification and regulatory requirements into working code and developer-ready documentation.
Academic background	• Degree in Computer Science, Software Engineering, Information Systems or a comparable field, or equivalent practical experience.
Professional Experience	• Proven hands-on software development experience; able to design and ship developer tools independently. • Experience with OAuth 2.0 and OpenID Connect. • Experience building or integrating distributed systems, ideally in identity, security or other regulated environment. • Demonstrated ability to write clear technical documentation for developers • Familiarity with eIDAS 2.0 (Regulation (EU) 2024/1183) and the Architecture Reference Framework (ARF) • Experience with open-source projects or developer communities
Key skills	• TypeScript, Java, Kotlin, Go, Python or comparable programming language for developer tools • API design and testing (REST, OpenAPI), test and validation tooling. • Technical writing for developers: integration guides, API documentation, sample code. • Git, CI/CD and open-source workflows.

Operations Engineer	
Role description	• Ensures the reliability, security, performance and availability of the production services of the EUDI Wallet ecosystem throughout their operational lifecycle.

	• Operates the production environments: monitors service health, handles alerts, manages capacity and performance, and maintains runbooks. • Resolves complex production incidents, performs root cause analysis, implements lasting corrective measures and leads post-incident reviews. • Plans, executes and validates rollbacks, backup and restore and recovery mechanisms to ensure service continuity, including regular recovery tests. • Handles operational security together with the Security team: least-privilege access, patching, vulnerability management and the lifecycle of certificates and keys. • Defines and tracks service levels (e.g. SLOs) and reports on availability and incidents. • Feeds operational requirements and lessons learned back to Development and to the DevOps/platform team. • Provides on-call service for critical periods, releases and incidents when called off.
Academic background	• Degree in Computer Science, IT Engineering, Systems Engineering, or a comparable field, or equivalent practical experience.
Professional Experience	• Experience building secure mobile applications that balance security, privacy, and usability. • Extensive experience operating complex production systems in cloud-native, distributed, or comparable environments, including incident, problem and change management. • Proven track record in resolving complex incidents, including on-call duty, and improving reliability in multi-stakeholder or regulated environments. • Experience with backup, recovery and business continuity for security-critical services.
Key skills	• Production operations, incident response and root cause analysis. • Backup, restore, disaster recovery and rollback procedures. • Capacity and performance management, service-level-based operations. • Secure operations: least-privilege access, patching, vulnerability management. • Runbooks and post-incident reviews.

Product Owner	
Role description	• Supports delivery alignment for software, security and design within assigned teams. • Translates priorities, user needs and requirements into a clear, actionable product backlog in coordination with the Client Product Owner. • Ensures backlog items are testable, traceable and continuously refined.

	• Prepares for review against the Definition of Done and functional, security and accessibility requirements. • Coordinates development, operations and QA and ensures transparent delivery tracking. • Prepares options for decisions
Academic background	• Degree in Computer Science, Business/Media Informatics, Software Engineering, Product/Digital Design, or comparable practical experience.
Professional Experience	• Experience with eIDAS 2.0 / Regulation (EU) No 910/2014 framework, Architecture and Reference Framework (ARF), and European Digital Identity Wallet Implementing Acts. • Experience building secure mobile applications that balance security, privacy, and usability. • Proven experience as a product owner in agile software development, preferably in complex, multi-stakeholder or regulated environments. • Demonstrated experience in managing product backlogs and translating requirements into testable, traceable backlog items for development teams. • Experience in coordinating development, operations and QA and in working with client-side stakeholders. • Experience with security-sensitive, privacy-relevant or public sector products is advantageous.
Key skills	• Agile delivery, stakeholder management and cross-functional collaboration. • Requirements engineering and backlog management. • Product design, user journeys and usability. • Ability to manage multiple topics and structured handovers. • Strong adaptability in dynamic delivery environments.

QA/ Automation Engineer	
Role description	• Owns QA processes, ensuring functional, technical and compliance requirements are met before release. • Designs and maintains scalable test automation frameworks, reusable test components and reliable test execution across environments. • Develops automated tests, manages test data and integrates automated quality gates into CI/CD pipelines. Performs exploratory manual testing where needed. • Embeds measurable acceptance criteria into user stories and ensures traceable test results, defect reports and quality metrics. • Applies risk-based testing and improves test coverage, automation reliability and maintainability. • Plans and executes interoperability tests against reference implementations and other wallets and relying parties

Academic background	• Degree in Computer Science, Quality Engineering, Software Testing or a related field, or equivalent practical experience.
Professional Experience	• Experience with protocols and standards for digital credential issuance, presentation, and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Experience building secure mobile applications that balance security, privacy, and usability. • Proven experience in test automation, automation framework development and CI/CD integration and regulated or safety-critical systems experience is an advantage. • Experience with accessibility testing of mobile applications according to EN 301 549, WCAG and BITV 2.0, including testing with screen readers (VoiceOver, TalkBack), is an advantage • Experience with native mobile test automation (e.g. XCUITest, Espresso, Compose testing, Appium or comparable), security testing and interoperability and conformance testing for digital credential protocols (e.g. OpenID conformance suite, ISO/IEC 18013-5 test tooling, cross-wallet and relying party interoperability tests) is an advantage
Key skills	• Hands-on expertise with automated testing tools and structured testing methods. • Ability to design reusable test components, maintain test coverage and integrate automated tests into CI/CD pipelines. • Experience with test data, test environments, defect management and test reporting. • Accessibility testing with assistive technologies (VoiceOver, TalkBack) and, where available, automated accessibility checks

Security Engineer	
Role description	• Performs threat modelling for the EUDI Wallet apps, backend services and interfaces and derives security requirements. • Reproduces and validates attacks against the Client's systems in designated test environments to confirm findings, assess exploitability and verify fixes. • Reviews architecture, key management, cryptography and authentication designs and documents findings. • Prepares evidence for certification and security audits (controls, test reports, documentation). • Supports the security analysis of incidents together with other members of wallet development or security teams.
Academic background	• Degree in Computer Science, IT Security, Software Engineering or comparable practical experience.
Professional Experience	• Proven hands-on experience in offensive application and mobile security, including reproducing and exploiting vulnerabilities in a controlled environment.

	• Experience with protocols and standards for digital credential issuance, presentation and verification (e.g. IETF SD-JWT VC, ISO/ IEC 18013-5/-7 mdoc, OpenID4VCI, OpenID4VP, W3C DC API). • Experience with threat modelling, secure design reviews and vulnerability management. • Experience preparing evidence for security certifications or audits is an advantage. • Recognised offensive security qualifications (e.g. OSCP, OSWE or comparable) are an advantage. • Experience with eIDAS 2.0 / Regulation (EU) No 910/2014 framework, Architecture Reference Framework (ARF) and security requirements for European Digital Identity Wallets is an advantage.
Key skills	• Threat modelling and attack reproduction (mobile and web/API). • Applied cryptography, secure key storage, mobile platform security (iOS, Android). • Security documentation, reporting and audit evidence.

UI/UX Designer	
Role description	• Designs and continuously improves user-centred digital experiences aligned with usability, accessibility and functional requirements. • Applies human-centred design principles based on ISO 9241-210 and relevant accessibility standards. • Conducts user research, usability testing and workshops and translates findings into intuitive interfaces. • Creates wireframes, prototypes and design systems for consistent implementation. • Works closely with Product Owners, Client UX/UI teams and developers throughout design and validation. • Defines measurable usability and accessibility acceptance criteria. • Uses user feedback and testing to continuously improve the user experience.
Academic background	• Degree in UX/UI, Interaction Design, HCI, Media Informatics or comparable practical experience.
Professional Experience	• Experience building secure mobile applications that balance security, privacy, and usability, by designing in particular: consent and selective-disclosure flows, trust/verifier indicators (who is asking for what), onboarding at high assurance, error and recovery states, and plain language. • Experience in applying accessibility requirements, including BITV 2.0, EN 301 549 and WCAG. • Proven experience delivering UX/UI solutions with a strong focus on accessibility, research and prototyping. • Demonstrated experience working and testing with diverse user groups (incl. users with disabilities), preferably in security-sensitive or regulated environments.
Key skills	• User research, usability testing, prototyping and accessibility.

	• Wireframes, prototypes and design systems. • Figma, UXPin or comparable tools. • Agile product development.

5. Collaboration & Governance

The contractor supports the Client in the continuous development of Germany's EUDI Wallet and its supporting digital infrastructure. Its personnel work in close collaboration with the Client's product and engineering teams. This chapter sets out the general terms of the collaboration, the call-off procedure, the availability and replacement of personnel, and the delivery and acceptance model. Transparent processes, flexible staffing and close collaboration ensure high-quality delivery and the long-term success of the EUDI Wallet ecosystem.

5.1 General

- **Billing**: Monthly based on person days/ hours delivered and accepted by the client. No fees shall be charged for securing availability or for on-call standby time, if not agreed otherwise upfront.
- **On-call:** Upon request in a call-off, the Contractor provides on-call service outside the Client's regular working hours (Monday to Friday, 9:00 a.m. to 6:00 p.m. German time, excluding public holidays in Berlin]) for selected roles and limited periods, in particular for critical positions, releases or incidents. On-call service is not required permanently or for all personnel. Standby time is not remunerated separately. Hours actually worked during on-call service are remunerated at the hourly rate plus a surcharge of 20 %. The Contractor determines which of its personnel provide the on-call service and ensures compliance with working time law.
- **Location**: Remote work; regular on-site workshops are expected
- **Workshops**: Upon client's request, in Germany, Berlin or other large city, every 2 months expected
- **Travel and expenses**: Travel expenses are the responsibility of the contractor
- **Working language**: English, German optional
- **Tools and hardware**: The contractor remains responsible for ensuring that assigned personnel have the skills, equipment and organisational support required to perform the contracted services. However, the Client may require that the services or parts of them are performed exclusively on devices and systems provided by the Client. In this case, the Contractor's personnel will use these devices in accordance with the Client's security and usage requirements.
- **Access**: The Client will provide access to all Client-controlled tools required for the performance of the services.

5.2 Call-off procedure

Individual call-offs under the framework agreement are placed without a renewed competition, strictly in the order of the ranking determined in the evaluation. If a Contractor has not provided an optional role that is called off, this Contractor will be skipped in the call-

off procedure. For each call-off, the Client submits a written e-mail request to the Contractor ranked first, specifying

- the service module(s),
- the role profile(s),
- the required start and end dates of availability,
- the duration and (if applicable) daily hours and
- whether and for which periods on-call service is required.

The Client may request multiple role profiles at the same time. The procedure below applies separately to each requested role profile.

- **(1)** First, the role profile submitted by the Contractor with its tender for the requested role is called off. Within 5 working days, the Contractor confirms the availability of the named person as of the required date (a minimum of 10 working days in advance).
- **(2)** If the person named in the role profile(s) are already deployed or otherwise unavailable, the Contractor may submit comparable role profile(s) for the requested role(s) within the same period. A role profile is comparable if it meets the minimum requirements pursuant to section 4.1 of the Award Criteria document and this service description and is at least equivalent to the role profile originally submitted. The Client accepts a comparable role profile that meets these requirements.
- **(3)** The Client may proceed to the next-ranked Contractor only if
    a. the Contractor does not respond within the deadline,
    b. the named person is not available and the Contractor does not submit a comparable role profile that meets the requirements pursuant to step 2 above,
    c. the Contractor declares that the requested role(s) are not available, or
    d. the selected personnel is not available as of the required date (a minimum of 10 working days in advance),
    e. the Client rejects the role profile as not comparable and gives reason,
    f. the Contractor declines the call-off or states that it is not available for the requested period.

The same procedure applies to the Contractors ranked second and third. This list is exhaustive. If no Contractor offers suitable role profile(s), the Client may procure the requested service outside this framework agreement. The framework agreement does not oblige the Client to purchase any minimum quantity.

Note: If a Contractor has not provided an optional role that is called off, this Contractor will be skipped in the call-off procedure

5.3 Availability and replacement of personnel

By submitting a role profile as part of this tender, the contractor confirms that the availability of the named person is secured as indicated in the role profile submitted as part of the tender. If a person is not available at the start of the project, the Contractor shall indicate the date from which the person will be available as part of the role profile.

The replacement of personnel assigned after a call-off is possible by mutual agreement. The Contractor shall notify the Client in writing at least 15 working days in advance of any planned replacement and shall coordinate the replacement with the Client. Any replacement personnel must meet the minimum requirements for the respective role pursuant to the requirements in Part B_Service Description and Part C_Award Criteria and must be at least equivalent in qualification to the person originally offered. The Client may reject a proposed replacement that does not meet these requirements. In the event of unplanned unavailability (e.g. illness or termination of employment), the Contractor shall inform the Client without delay. The Contractor must also offer an equivalent or better replacement within 10 business days. If this does not occur, the Client reserves the right to recast the role in a new call-off. In this case, the Contractor is not allowed to participate in the call-off.

5.4 Delivery & acceptance model

- Contractor's personnel will work very closely with the Client's product and engineering organisation where applicable, including the Client's 14-day sprint cadence and established delivery processes. This may include:
    - Sprint Planning, Backlog Refinement, Reviews and Retrospectives
    - Daily collaboration and technical design/refinement
    - Code reviews
    - Incident and problem-solving activities, where applicable
- All work shall follow the Client's established development, collaboration and delivery processes. By submitting a tender, the bidder undertakes to ensure that its services are provided in accordance with the Client's agile delivery process.
- Instructions by the Client relate exclusively to the content, prioritisation and quality requirements of the services, in particular through the backlog, sprint planning and reviews. The Contractor retains the right to direct its personnel as employer, in particular regarding working time, leave, absences and staffing. The Contractor designates a coordinator for personnel matters and escalations. The obligation to participate in agreed meetings and sprint events remains unaffected.
- Engineering work shall be delivered through the Client's pull request/merge request (PR/MR) workflow and reviewed according to the Client's standards.
- Complete and understandable documentation shall be maintained as part of daily engineering activities. This includes: technical, API/interface, security-relevant and test documentation
- All Intellectual Property resulting from the services shall be owned by Common Codes
- Source code will continue to be open sourced

6. Tender Framework

6.1 Contract

The framework contract shall be provided in **German**, an **English** convenience translation will be made available for reference purposes. In the event of any discrepancies, inconsistencies, or interpretation differences between the German version and the English translation, the

German version shall prevail as the legally binding and governing language of the contract. All other tender documents are provided in English.

6.2 Service period and volume

The framework contract runs for 2 years after tender conclusion. There is the option to extend the contract twice for one year at a time. Based on a potential four-year service period, the estimated contract value is 3.960.000 EUR net. A total maximum contract value of 4.752.000 EUR for all individual call-offs applies.

6.3 Overarching compliance requirements

The client has defined the following overarching general compliance requirements to ensure compliance with regulatory, security, and data protection standards:

- The contractor shall be headquartered or have its principal place of business within the **European Union/EEA**
- An **ISO/IEC 27001 certification** or SOC 2 Type 2 (or equivalent information security management certification) is required and shall be evidenced as part of the proposal
- The engineering approach is expected to reflect the fundamental principles of the EUDI Wallet ecosystem:
    - Privacy by Design
    - Security by Design
    - Interoperability by Design
    - Open Standards & Avoidance of Vendor Lock-in
    - Accessibility by Design
    - User Control & Transparency
    - Regulatory & Standards Environment

The contractor must support compliance, security evaluation, and assessment processes by providing appropriate documentation and technical information required for independent security reviews or audits if requested by the Client.