

Procurement procedure  
Runtime Application Self-Protection (RASP)  
of SPRIND GmbH

Award number: EIN-1380

**Part B: Service description**

# 1. Context and objectives

The implementation of the revised eIDAS regulation (electronic Identification, Authentication and Trust Services) requires the creation of a secure and user-friendly ecosystem. As a milestone for Europe's digital sovereignty, its core element is the European Digital Identity Wallet (EUDI Wallet), which serves as the regulation's central instrument. By the start of 2027, all EU citizens and residents should have access to a trustworthy, interoperable, and non-discriminatory digital wallet for identification, attribute attestations, electronic signatures, and more. The EUDI Wallet aims to simplify users' daily lives while enabling companies and administrations to benefit from faster, more secure, and more efficient digital processes.

In Germany, the rollout of the EUDI Wallet is a joint effort by the Federal Ministry for Digital and State Modernization (BMDS) and SPRIN-D – the Federal Agency for Breakthrough Innovation. Since June 2023, the initiative has followed an open architecture and consultation process involving business, civil society, and science, with a focus on security, privacy, user-friendliness, and innovation. Germany's dual strategy supports both a national EUDI Wallet as well as alternative EUDI Wallets. The roadmap includes a sandbox rollout of the identity (PID) function by the end of 2025 and further enhancements and production rollout throughout 2026.

In this tender, the client is seeking a **Runtime Application Self-Protection (RASP)** solution to provide an additional layer of runtime security for its wallet applications on iOS and Android. The objective is to enhance protection against runtime threats, obfuscate the code and support privacy provisioning and telemetry. The scope covers the procurement and integration of the RASP solution with the described functionality.

## 2. Mandatory requirements

The client has defined a specific feature scope for the proposed RASP solution. The solution is expected not only to perform comprehensive runtime threat detection, but also to provide robust code protection capabilities (e.g., obfuscation and anti-tampering mechanisms), dynamic policy provisioning and telemetry.

Further details regarding the functional requirements are outlined below and additionally described in the client's publicly available documentation ([German Architecture Documentation - MDVM concept](#)) - the documentation is currently still work in progress and will be updated regularly.

### 2.1 Functional requirements

The requirements set out in this section constitute the **mandatory minimum scope** of the proposed solution. **All bidders must fully comply with these requirements.**

#### A. Runtime threat detection

The solution must detect and respond to:

- **App Hooking and Debugging**
  - Detection of runtime hooking frameworks (e.g., dynamic instrumentation)
  - Detection of active debugging attempts
  - Protection against runtime manipulation of application logic
- **App Repackaging**
  - Detection of modified or re-signed application packages
  - Integrity verification of distributed application binaries
- **App Tampering**
  - Detection of code modification and unauthorized changes
  - Runtime integrity validation mechanisms
- **Rooting and Emulation Detection**
  - Detection of rooted or jailbroken devices
  - Detection of emulators and virtualized environments
  - Identification of compromised or high-risk device states

## B. Code protection

The solution must provide:

- **Code Obfuscation**
  - Protection of sensitive logic and RASP calls
  - Compatibility with standard build tools

## 2.2 Other technical requirements

In addition to the functional requirements outlined above, the client defines the following non-functional technical requirements to ensure long-term scalability, interoperability, and implementation stability.

- The proposed solution shall provide a mobile SDK supporting both **iOS and Android platforms**. If the provider meets the requirements with a solution that is not implemented via an SDK, this is also acceptable. In the following, the term “SDK” will continue to be used. If the provider supports additional operating systems, these may be listed but will not be considered in the evaluation.
- If a **backend** is required: The component must be capable of operating on infrastructure provided and controlled by the client or its designated subcontractors.
- The SDK must be available as an **out-of-the-box solution** meaning that the solution requires very limited to no programming effort on either side and provides immediate protection based on a proven best-practice configuration.
- The SDK shall fundamentally support **both operating modes**: (i) standalone operation (SDK-only, without backend integration), and (ii) operation in conjunction with a backend component if necessary for full scope. The contractor must clearly state which functionality requires a backend!
- **No transfer of data to servers operated or controlled by the contractor** shall take place unless explicitly agreed in writing. The solution must be capable of operating without transmitting operational or security telemetry to contractor-controlled infrastructure.

- Based on the client's current assessment, little to no **integration or development effort** is anticipated on the client's side (e.g. ramp-up to full functional capacity within 10 work days). Should the contractor foresee material integration complexity or additional implementation requirements, these must be explicitly outlined and commercially reflected in the proposal.
- When delivering the SDK, an SBOM (Software Bill of Materials) must be provided and updated with every update in order to track third-party libraries and OSS licenses.

## 2.3 Non-technical requirements

In addition to the technical and functional requirements, the client defines the following non-technical 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**.
- 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 solution shall adhere to the principles of **privacy by design and by default**.
- The contractor shall disclose all categories of data processed by the SDK and ensure full support for **GDPR compliance** within the client's environment.
- The contractor shall **support compliance, security evaluation, and assessment processes** by providing appropriate documentation and technical information required for independent security reviews or audits.
- The contractor shall provide **evidence of the robustness** of the RASP solution based penetration tests (or similar evidence) conducted within the last two years. This evidence should be quantifiable and demonstrate that the RASP solution is hardened against attacks. The documentation should also indicate the scope and duration of the penetration testing or equivalent efforts, including how extensively attempts were made to compromise the system.

## Open Source & Bug Bounty

The contractor accepts code being published **open source**. Due to the open source nature of the project, the client intends to publish the applications' source codes throughout 2026. Prior to publication, all RASP-related calls will be removed from the publicly released codebase.

Additionally, the contractor shall grant the client the explicit right to include all protected code, including iOS, Android or other OS applications, as well as any integrated RASP components, within the scope of the client's bug bounty program. The client shall retain sole responsibility for the administration, management, and execution of the bug bounty program.

The contractor shall maintain and enforce a documented Vulnerability Disclosure Policy (VDP) and shall further implement appropriate incident handling processes to address security findings in a timely and structured manner.

### 3. Optional functional requirements

The functionalities described in this section are **optional** and **not required** for participation in this tender. Bidders may offer these optional modules on a voluntary basis. Offers without optional modules will be considered fully compliant and will not be excluded from the procurement procedure.

#### 3.1 Optional module: Policy provisioning & telemetry

If a bidder chooses to offer this optional module, all requirements listed below must be fulfilled in full.

- **Dynamic policy provisioning**
  - Centralized runtime configuration without requiring app updates (e.g. device classes) limited to predefined parameter ranges (guardrails)
  - Secure and signed policy distribution to prevent manipulation of the software development kit (SDK)
- **Telemetry**
  - Policy Version Traceability: The solution shall provide telemetry indicating the security policy version applied to each application instance or session, enabling correlation of runtime behavior with the active policy configuration.
  - Security Event and Termination Reporting: The solution shall report all triggered runtime security rules (e.g., tampering or hooking detection) and the resulting enforcement action. Telemetry must clearly indicate if and when the application was terminated by the RASP solution and the reason for such action. Each event shall include the triggered rule, the action taken, and a unique session and/or event identifier to support correlation, operational analysis, and investigation of false positives or anomalies.

The client acknowledges that certain functionalities may be offered by the contractor through backend components. Where such backend components are required to deliver the proposed functionality, they must be capable of operating on infrastructure provided and controlled by the client or its designated subcontractors. The client will not be able to use backend components hosted or operated by the contractor. Any such contractor-hosted backend services, if offered, will not be taken into consideration in the evaluation of the bidder's proposal.

The contractor shall, as part of the commercial offer, clearly describe which functionalities are provided by the proposed solution and indicate how these functionalities address the requirements set out in this tender.

Offers that do not include optional functional requirements will still be considered.

## 4. Operations & support

The contractor shall provide comprehensive operations and support services for the proposed RASP solution throughout the contract term. This includes in particular:

- **24/7 incident intake and support** for critical security incidents (Severity 1), including a maximum initial response time of four (4) hours and provision of mitigation measures or patches within forty-eight (48) hours, where technically feasible.
- **Timely security updates and vulnerability remediation**, within forty-eight (48) hours for critical vulnerabilities and within five (5) business days for high-severity vulnerabilities and proactive notification of newly identified security risks affecting the SDK or backend components.
- **Ongoing compatibility support** for new major releases of iOS and Android, ensuring continued functionality and protection of SDK and backend components.
- **Provision of a dedicated technical contact point** and structured **escalation procedures** for security-relevant incidents.
- **Regular maintenance** releases and **continuous improvement** of detection capabilities, performance, and stability.

The contractor shall clearly describe its support model, severity classification framework, escalation paths, and associated response and resolution times in the solution concept.

## 5. Information on pricing & contract

### Pricing

The wallet applications to be secured under this tender will be provided to German citizens and are intended for broad nationwide adoption. The potential user base comprises all individuals holding a valid German electronic identity document (eID) or electronic residence permit (eAT). The transaction volumes will depend on the evolution and adoption of the surrounding digital ecosystem. During the initial rollout phase starting on January 2nd 2027, transaction frequency per device is expected to be relatively low (e.g., fewer than three transactions per month). However, with the planned functional expansion of the ecosystem in 2027 and onwards, a significant increase in usage intensity is anticipated, potentially resulting in multiple transactions per device per day. This requires **high scalability of the proposed solution both technically and commercially**. A pricing structure that remains predictable and sustainable across varying levels of user adoption and transaction intensity is therefore required.

This dynamic growth trajectory has several implications for this tender, including but not limited to:

1. The client requires a **comprehensive, all-inclusive pricing model** with a defined price cap, independent of Monthly Active Users (MAU), covering both the SDK and the optional backend components. Pricing must be provided separately for (i) the SDK-only scenario and (ii) the backend component on-top of the SDK pricing. Any

underlying assumptions, cost drivers, or pricing mechanics must be transparently explained within a separate commercial offer documentation.

- a. Note: In the price sheet, the contractor shall provide a total price in order to enable a comparable evaluation of the submitted offers.
  - b. Note: The client intends to **integrate the SDK in 2026** and, if required, extend the integration with **backend components in 2027**. Accordingly, charges shall only apply once the respective functionalities are actively available to the client.
2. **Integration support** by the contractor is expected as part of the overall service scope and must be included in the proposed pricing. Based on the client's current assessment, no significant integration or development effort is anticipated. Should the contractor foresee material integration complexity or additional implementation requirements, these must be explicitly outlined and commercially reflected in the proposal.
  3. The client expects **continuous solution improvements** throughout the contract term, including but not limited to compatibility with updated iOS and Android versions, performance optimizations, and reduction of false positives. Ongoing quality assurance measures (e.g., penetration testing, security validation activities) as well as all required licensing fees shall be included in the proposed pricing.
  4. In the event of a **backend implementation**, the client will assume responsibility for provisioning and operating the necessary infrastructure capacity to handle backend load, unless explicitly agreed otherwise.

## Contract

All contractual documentation shall be provided in **German**. An **English** convenience translation may 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.

## 6. Further information on tender framework

It is important to understand that the client for the contractor will be the SPRIND GmbH - Bundesagentur für Sprunginnovationen (SPRIND), a 100% federally owned GmbH. The EUDI Wallet applications and their related artifacts are developed by a project team that will directly be responsible for the collaboration with the contractor.

All other information regarding cooperation, application process and decision making will be provided as part of the tender document bundle.