

Award procedure
Managed Bug Bounty Program
of SPRIND GmbH

Award number: EIN-1464

Part B: Award Criteria

Award Criteria

The tender will be awarded to the most economically advantageous bid based on the following award criteria:

Criteria	Weighting
Pricing	30 %
Quality:	70 %
• Solution Concept	50 %
• CVs	10 %
• Platform Design & Usability	10 %

The bids will be evaluated on the basis of a total of 100 points. Of these, 30 points are allocated to the price component, 50 points to the Solution Concept, 10 points to the CVs (Customer Success Manager and Triage Team Manager), and 10 points to Platform Design U usability.

The points to be awarded will be recorded in “Part B_Evaluation grid template”, which is also attached, and will form the basis for the assessment.

A. Pricing

Bounty-based Pricing Model

Tier	Maximum Annual Bounty To Spend	General Platform Fee (Annual) in Euro net	Triage Service Fee (Annual) in Euro net	Total Fee (= Sum of ‘General Platform Fee (Annual) in Euro net’ and ‘Triage Service Fee (Annual) in Euro net’)
A	Up to €200,000			
B	Up to €300,000			
C	Up to €400,000			
D	Up to €500,000			
E	Up to €600,000			
F	Up to €700,000			
G	Up to €800,000			
H	Up to €900,000			
I	Up to €1,000,000			

Scoring Methodology

For every bidder, the average annual total fee is calculated and evaluated as follows:

$$P_{\text{bidder}} = (P_{\text{Total_Fee_Tier_A}} + P_{\text{Total_Fee_Tier_B}} + P_{\text{Total_Fee_Tier_C}} + P_{\text{Total_Fee_Tier_D}} + P_{\text{Total_Fee_Tier_E}} + P_{\text{Total_Fee_Tier_F}} + P_{\text{Total_Fee_Tier_G}} + P_{\text{Total_Fee_Tier_H}} + P_{\text{Total_Fee_Tier_I}}) / 9.$$

The lowest total annual price submitted among all eligible bidders is determined:

P_{min} : lowest total annual fee.

This ‘total annual fee’ is used as the basis for evaluating the ‘pricing’ award criterion.

The bidder with the lowest total annual fee will receive 30 points. The remaining bids receive proportionally fewer points based on their total annual fee, with the score decreasing linearly and capped at 0 points for any bid that is at least twice as expensive as the lowest-priced offer:

$$\text{Points} = 30 \times [(2 \times P_{\text{min}}) - P_{\text{bidder}}] / P_{\text{min}}$$

SPRIN-D

For the evaluation of the price component, all calculations are performed using the exact numerical values provided by the bidders. The resulting price scores are then rounded to two decimal places for the purpose of comparison and documentation. Rounding is carried out according to standard mathematical rules (values with a third decimal digit of 5 or higher are rounded up; values with a third decimal digit below 5 are rounded down).

Only the prices/fees provided by the tenderer in the form Part C Appendix 01 price sheet shall be decisive.

B. Solution Concept

As part of this tender, each bidder shall submit a written solution concept describing how the bidder intends to provide the Services in accordance with Annex B (Service Description and Requirements). The solution concept shall, for each subsection of Annex B, explain in a clear and sufficiently detailed manner how the bidder will implement the mandatory requirements and, where applicable, to what extent and in what manner the bidder can support the desirable, non-mandatory requirements. The document must not exceed 30 pages (excluding cover pages and table of contents) and must be formatted in font 11 (e.g. Arial or Calibri) or higher with standard margins (e.g. 2cm top/bottom/left/right). Any pages exceeding this limit will be ignored and not evaluated/considered.

It shall have the following structure:

1. Program Setup & Scope of Services (Annex B 1.1, 1.2)
2. Platform Capabilities & Integrations (Annex B 1.3, 1.4, 1.5)
3. Compliance, Governance & Security Management (Annex B 1.6)
4. Managed Triage Services (Annex B 1.7)
5. Researcher & Bounty Management (Annex B 1.8)
6. Analytics, Transparency & Reporting (Annex B 1.9)
7. Onboarding, Communication & Researcher Obligations (Annex B 1.10, 1.11, 2)

The evaluation will be carried out in accordance with this structure. This means that aspects relevant to the evaluation must be included in the relevant section. Consequently, if a tenderer presents, for example, aspects under point 1 that actually belong under point 2, these will not be taken into account under point 2.

Please note: The 'mandatory requirements' set out in the Annex B must always be met if the contract is awarded. Should your proposal deviate from these mandatory requirements, your bid will be rejected. Please therefore ensure that you do not deviate from these mandatory requirements – even inadvertently.

The form "Part C_Appendix 02_Solution concept_template" is to be used for the solution concept.

Overview table

Chapter (Solution Concept)	Annex B Reference	Max Points
Program Setup & Scope of Services	1.1, 1.2	5
Platform Capabilities & Integrations	1.3, 1.4, 1.5	10
Compliance, Governance & Security Management	1.6	10
Managed Triage Services	1.7	10
Researcher & Bounty Management	1.8	5
Analytics, Transparency & Reporting	1.9	5
Onboarding, Communication & Researcher Obligations	1.10, 1.11, 2	5
Total		50

Evaluation Sub-Criteria

Program Setup & Scope of Services (1.1, 1.2 of Annex B) – 5 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 1 point – Only fragments are described; several mandatory elements are absent or unclear. There is no coherent overall model.
- 2 points – All mandatory elements are mentioned, but description is very high-level, generic or not recognisably tailored to the EUDI Wallet context. Important responsibilities or handovers remain vague.
- 3 points – The solution outlines a coherent program model and end-to-end lifecycle aligned with 1.1 and 1.2 of Annex B, but some steps or roles are only briefly described or lack concrete examples.
- 4 points – The solution describes a clear, logically structured program setup, covering all lifecycle stages with understandable responsibilities and flows tailored to the EUDI Wallet use case. Minor details may be missing but do not impair feasibility.
- 5 points – In addition to fulfilling all points for 4, the solution provides concrete practical detail (e.g. process diagrams, role descriptions, examples from similar programs) that demonstrates a high degree of operational maturity and low implementation risk.

Platform Capabilities & Integrations (1.3, 1.4, 1.5 of Annex B) – 10 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 2 points – Some platform features are described, but several core mandatory aspects are not clearly addressed or are left open.
- 4 points – All core mandatory aspects are at least mentioned as being supported; however, explanations are mostly marketing-level, with little technical or procedural detail. It remains unclear how configuration and operation will look in practice.
- 6 points – The solution describes how the platform implements all mandatory features in 1.3–1.5 of Annex B in an understandable way. There is enough information to assume feasibility, but the concept remains partly generic or lacks depth in some areas.
- 8 points – The solution provides a structured, detailed description of platform functions and integrations, including: concrete role model, MFA enforcement, encryption and retention implementation, RoE/Safe Harbor handling, communication flows, and ticketing system integration. Where desirable features are offered, they are clearly explained and integrated into the approach.
- 10 points – In addition to fulfilling all points for 8, all desirable features are offered and the solution convincingly demonstrates platform maturity (e.g. screenshots, reference architectures, proven integration patterns, SLA dashboards) and shows that the technical platform is specifically well suited for the Client's environment and requirements.

Compliance, Governance & Security Management (1.6 of Annex B) – 10 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 2 points – Individual aspects such as ISO certification or incident response are mentioned, but the overall framework is not explained. Personnel screening, data residency, vulnerability management or audit support may be completely absent.

SPRIN-D

- 4 points – The solution addresses most key points of 1.6 of Annex B, but several are treated only with generic statements. No concrete processes or responsibilities are mentioned.
- 6 points – The solution presents a coherent framework that covers all mandatory elements, including personnel qualification and screening, ISO 27001/SOC2 or equivalent, incident/disaster recovery plans with RTO/RPO, vulnerability and patch management, data-location overview and sub-processor lists, audit support, and NDAs. In addition, all Personal Data is stored, processed and effectively controlled in accordance with GDPR within the European Union or a non-EU country that has a fully adequate level of data protection without limitations.
- 8 points – The solution describes concrete processes, roles and artefacts, demonstrates existing certifications, and explains how client-specific requirements will be implemented. The picture indicates a mature but standard enterprise-grade setup.
- 10 points – In addition to fulfilling all points for 8, the solution shows a highly developed security governance model and gives confidence that the provider can transparently and proactively support audits, supervisory requests and complex incident situations.

Managed Triage Services (1.7 of Annex B) – 10 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 2 points – Triage is described in generic terms without clear steps for filtering, verification, severity assessment, reporting or escalation. References to SLAs are missing or unclear.
- 4 points – The solution describes basic triage steps and mentions SLAs, but does not explain how complex cases, duplicates, spam/AI noise or disagreements are handled. Team structure and skills are only briefly described.
- 6 points – The solution outlines a structured triage process including: dedicated team, filtering rules, reproduction or alternative verification, severity/impact methods and triage summaries. It references the SLAs in Annex C and describes how triage times will be monitored. Some practical detail may still be limited.
- 8 points – The solution provides a detailed triage model: clearly defined roles and skills, step-by-step workflow, specific criteria for duplicates/closure, standard format for triage summaries, and explicit procedures for SLA monitoring and escalation of Exceptional/Critical issues. Past experience or examples are used to illustrate capability.
- 10 points – In addition to fulfilling all points for 8, the solution shows robust internal quality assurance and demonstrates that triage is operated as a mature, industrialised service rather than an ad-hoc activity.

Researcher & Bounty Management (1.8 of Annex B) – 5 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 1 point – Only basic statements are made; controls for identity verification/tax/sanctions, Trust Account usage, approvals and returns of funds are not explained.
- 2 points – The solution describes, in outline, how researchers participate and how payouts are made, and mentions some checks or fund management. However, the governance of the bounty pool and handling of edge cases (e.g. return of funds, country restrictions) remain vague.

SPRIN-D

- 3 points – The solution explains how researchers are managed, engaged and bound to program rules, how global payouts with identity verification/tax/sanctions are handled, and how the Trust Account and ledger are managed. Processes appear plausible, but practical detail on controls or exception handling is still limited.
- 4 points – The solution provides a clear, structured description of researcher lifecycle, payout workflow, verification and sanctions checks, real-time balance management and return of unallocated funds, along with a coherent approach to review and update the bounty table. The processes appear well-thought-out and controlled.
- 5 points – In addition to fulfilling all points for 4, the solution demonstrates concrete experience operating similar bounty pools and shows how feedback from researchers and Client is systematically used to adjust the program and bounty table.

Analytics, Transparency & Reporting (1.9 of Annex B) – 5 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 1 point – Only generic statements are included, without specifying which metrics, exports or report types are available.
- 2 points – The solution lists some dashboards or KPIs and mentions structured exports and periodic reports, but without sufficient clarity on scope, formats or how they support Client's governance and reporting duties.
- 3 points – The solution describes specific dashboards, key KPIs, export capabilities and periodic report formats that appear to meet the mandatory requirements. It explains, in principle, how Client can use this information for internal steering and decision-making.
- 4 points – The solution provides a clear and concrete view of analytics and reporting: which KPIs and breakdowns are available, how data can be exported, what regular reports look like, and how these outputs will be integrated into Client's governance processes.
- 5 points – In addition to fulfilling all points for 4, the solution offers advanced or flexible analytics options (e.g. additional KPIs, trend analyses, API access) and explains convincingly how these will be used jointly with Client to monitor, optimise and report on the program.

Onboarding, Communication & Researcher Obligations (1.10, 1.11, 2 of Annex B) – 5 points

- 0 points – The chapter is missing or does not meet any of the criteria listed in the related section of Annex B.
- 1 point – Only very general statements are made; timelines, responsibilities and enforcement of researcher obligations remain mostly undefined.
- 2 points – The solution outlines basic onboarding steps and main communication channels, and notes that Annex E obligations will be reflected on the platform. However, the plan lacks structure and implementation details for researcher terms and enforcement are sparse.
- 3 points – The solution presents a recognisable onboarding plan and a communication setup with named roles and escalation paths. It explains, at least in principle, how researcher obligations from Annex E will be integrated into the platform's terms and flows.
- 4 points – The solution provides a structured onboarding timeline with phases, responsibilities and concrete deliverables, a clear communication and escalation model, and a comprehensible concept for implementing and enforcing Annex E obligations.

SPRIN-D

- 5 points – In addition to fulfilling all points for 4, the solution shows that the bidder has a proven methodology for onboarding similar programs, including risk mitigation for go-live of the program, and describes how the communication and researcher-obligation mechanisms are regularly reviewed and refined during the contract term.

C. CVs

Each CV shall not be longer than 3 pages and must be formatted in font 11 (e.g. Arial or Calibri) or higher with standard margins (e.g. 2cm top/bottom/left/right). Any pages exceeding this limit will be ignored and not evaluated/considered. The bidder must clearly assign each CV to the relevant position (Customer Success Manager or Triage Team Manager). Please submit only these two CVs and no others. However, if more CVs are submitted and/or the assignment is not clear, the CVs will be evaluated in alphabetical order by surname. If the assignment is not clear, the CV will first be evaluated as a Customer Success Manager and the other as a Triage Team Manager, in alphabetical order.

- Customer Success Manager
CV 5 Points
- Triage Team Manager
CV 5 Points

Requirements

Scoring Table/Evaluation

Score	Assessment Criteria for Customer Success Manager
5	The CV shows (a) at least 4 years of experience in managing bug bounty programs for government agencies or operators of critical infrastructure, or (b) shows at least 3 years of experience in managing bug bounty programs for government agencies or operators of critical infrastructure and at least 1 year of experience in managing bug bounty programs for other fields.
4	The CV shows at least 3 years of experience in managing bug bounty programs for government agencies or operators of critical infrastructure.
3	The CV shows (a) at least 2 years of experience in managing bug bounty programs for government agencies or operators of critical infrastructure and at least 1 year of experience in managing bug bounty programs for other fields, or (b) at least 3 years of experience in managing bug bounty programs for other fields.
2	The CV shows at least 1 year of experience in managing bug bounty programs for government agencies or operators of critical infrastructure and at least 2 years of experience in managing bug bounty programs for other fields.
1	The CV shows at least 2 years of experience in managing bug bounty programs for other fields.
0	The CV is missing/incomplete or does not meet any of the criteria listed above.

Score	Assessment Criteria for Triage Team Manager
5	The CV shows at least 4 years of experience in triage. It also shows one year of experience each in the following domains (1) web application security, (2)

SPRIN-D

	authorization and identity protocols, (3) wallet ecosystems, (4) mobile app security and (5) cryptography.
4	The CV shows at least 3 years of relevant experience in triage. It also shows one year of experience each in 4 of the following domains: (1) web application security, (2) authorization and identity protocols, (3) wallet ecosystems, (4) mobile app security and (5) cryptography.
3	The CV shows at least 2 years of relevant experience in triage. It also shows one year of experience each in 3 of the following domains: (1) web application security, (2) authorization and identity protocols, (3) wallet ecosystems, (4) mobile app security and (5) cryptography.
2	The CV shows at least 1 year of relevant experience in triage. It also shows one year of experience each in 2 of the following domains: (1) web application security, (2) authorization and identity protocols, (3) wallet ecosystems, (4) mobile app security and (5) cryptography.
1	The CV shows at least 1 year of relevant experience in triage.
0	The CV is missing/incomplete or does not meet any of the criteria listed above.

D. Platform Design & Usability

The platform will be evaluated based on its user interface, ease of use, and its alignment with the functional requirements described in the service description. For this purpose, bidders are encouraged to provide temporary access including a link and credentials to a non-production or test instance of the platform to allow hands-on evaluation. If test access cannot be provided, bidders shall instead submit comprehensive documentation (e.g. a detailed PDF with representative screenshots) that clearly demonstrates the relevant functionality and workflows.

Scoring Table

Score	Assessment Criteria
10	Highly intuitive interface with advanced UX features; exceeds all expectations with seamless workflows.
8	Modern, user-friendly design; fully meets all expectations with clear navigation.
5	Functional design that meets basic expectations but may have minor usability friction or dated UI elements.
2	Difficult to navigate or missing several key functional features required for efficient program management.
0	The platform is unusable, lacks critical security/functional requirements, or no demo/evidence was provided.
