

Award Criteria – Runtime Application Self-Protection (RASP)

1. Information on overall evaluation

This document describes the evaluation methodology for submitted bids and outlines the documents required as part of the tender. Bidders are required to submit the following documents for the award criteria:

- **Price sheet** (please use the provided form “Part D_Appendix 01_Price sheet”) – forms the basis for the evaluation of the “Price” award criterion
- **Solution concept** (there is no form provided by the Client, however please consider the required content for this concept as described in this document) – forms the basis for the evaluation of the “Quality” award criterion

For each award criterion, this document sets out the relevant evaluation categories, the number of points available, and the applicable weighting. Depending on the criterion, scoring will be based either on the submitted price sheet or on the submitted solution concept.

2. Information on award criterion “Price”

2.1 Preliminary remarks and notes

This price sheet contains all price components related to the requested services in accordance with the service description. All prices are all-inclusive prices (fixed prices) and include all components required for the full provision of the services in line with the service description, including:

- Integration
- Support
- Maintenance
- Upgrades / hardening
- Unlimited number of devices
- Unlimited number of downloads
- All functionalities offered in accordance with the service description

All prices must be stated in EUR (net, excluding VAT) and must include all applicable costs such as transport, travel and any other costs required for complete service delivery and effective cooperation with the Client.

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

The bidder must only complete the grey cells in accordance with the description and may not make any changes to the structure or composition of the price sheet. Otherwise, the offer must be rejected/excluded.

2.2 Categories of the award criterion “Price”

The award criterion “Price” includes both mandatory and optional functionalities. Points will be awarded based on the submitted document *Part D_Appendix 01_Price sheet*.

Category A: Mandatory functionalities

Category	Protected devices [number]
1	0 – 1.000.000
2	1.000.001 – 5.000.000
3	5.000.001 – 10.000.000
4	10.000.001 – 20.000.000
5	From 20.000.001

The bidder is required to provide the monthly costs as all-in prices (fixed prices) and based on the number of protected devices. The contractor must provide the full scope of mandatory functionalities. Please refer to *Part D_Appendix 01_Price sheet* for details.

Category B: Optional functionalities

Category	
6	Optional functionalities

The bidder may, but is not required to, provide monthly costs as an all-in price for optional functionalities. If this category is not included, no total monthly cost are to be entered. In this case, the bid will receive 0 points for category B of this award criterion during the evaluation.

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

If this category is included, that is the bidder offers “Category B: Optional functionalities”, the total monthly cost are to be entered accordingly and the contractor must provide the full scope of optional functionalities if required by the Client. Please refer to *Part D_Appendix 01_Price sheet* for details (please note: If the optional functionalities are provided via the contractor’s backend or if user data leaves the Client’s sphere of influence in any other way, zero points will be awarded for category 6.)

2.3 Scoring for the award criterion „Price“:

A total of 50 points will be awarded for the award criterion. For each of the six total cost categories, **5 points** are awarded based on a scoring scale from 0 to 5:

- 5 points are awarded to the bid with the lowest total costs in the respective category (see above).
- 0 points are awarded to a fictitious bid with twice (200%) the lowest total costs in the respective category (see above).
- All bids with higher total costs also receive 0 points.
- Points for all intermediate prices are calculated using linear interpolation. Rounding is done in a commercial manner.

This results in a **preliminary total score** per bidder as the sum of the 6 categories. A maximum of **6 categories × 5 points = 30 preliminary points** can be achieved. The **total score** achieved for the award criterion is multiplied by a **weighting factor** of **5/3**:

$$\text{Total score} = \text{preliminary total score} \times \text{weighting factor}$$

A maximum of **50 total points** can be achieved in the price evaluation.

2.4 Example calculation “Price”

The following is an exemplary calculation. Please note that the monetary values used are fictitious and were chosen arbitrarily.

Parameters:

- C_{\min} = lowest verified total cost in category (here: EUR 180.000 net)
- C = cost in category of the bid under evaluation (here: EUR 200.000 net)
- $C_{\max} = 2 \times C_{\min}$ (here: EUR 360.000 net)
- Points: meaning points in category

Formula:

$$\text{Points} = 5 * \frac{C_{\max} - C}{C_{\max} - C_{\min}}$$

Exemplary calculation for a category:

$$Points = 5 * \frac{360.000 - 200.000}{360.000 - 180.000} = 4,4$$

3. Information on award criterion “Quality”

3.1 Preliminary remarks and notes

The bidder is required to use the following structure to develop a *solution concept* in response to the service description set out in this call for tenders. The bidder uses its own document, there is no form provided by the Client. However, the bidder’s solution concept shall correspond to the format and category order as stated in this document.

Bidders are encouraged to provide additional information beyond the guiding questions, especially if this contributes to the fulfillment of the service description and highlights the strengths of their proposed solution and service offering. The entire solution concept should not exceed 10 pages (excluding cover pages, table of contents, references and requested appendices) and must be formatted in font 11 (e.g. Arial or Calibri) or higher with standard margins (e.g. 2 cm top/bottom/left/right).

3.2 Categories of the award criterion “Quality”

The award criterion “Quality” includes three categories: solution design, integration and security. Points will be awarded based on the submitted solution concept and its appendices.

Category A: Solution design

As part of the solution concept, the bidder is requested to provide a concise description of the exact scope of the proposed solution in relation to the functional requirements and how these requirements are fulfilled by the bidder’s solution. The concept should address the guiding questions set out below:

- Which optional functional requirements are covered (see service description chapter 3.1)? The bidder is requested to provide a table in checklist form.
- How is each functional requirement – mandatory and if offered optional - implemented, for example via SDK, backend components, or other technologies? The mapping for each functional requirement should be clearly identifiable.
- Which components form part of the overall security solution? How are these components, and in particular the RASP components, implemented? Which operating systems do you offer besides iOS and Android?
- Describe your security concept: How are security functionalities provided by the RASP implemented from a technical perspective, and how do the individual functions interact within the overall solution architecture?
- Describe your support model including severity classification framework, escalation paths, and associated response and resolution times

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

Focus of category A is on clarity, relevance, and structure of the information presented, including the readability and logical structure of the document while answering the guiding questions above. Category A of the solution concept will be evaluated using a scoring scale from **0 to 10 points**:

- 10 points – Excellent: Fully meets or exceeds expectations; comprehensive, well-structured, and highly relevant, providing clear added value.
- 8 points – Very good: Meets expectations with only minor omissions; clear, relevant, and well-structured.
- 6 points - Good: Meets expectations overall, though some details may be missing or could be further clarified.
- 4 points – Average: Generally adequate, but lacks detail or contains some inconsistencies or ambiguities.
- 2 points – Poor: Incomplete, unclear, and fails to address key aspects of the guiding questions.
- 0 points - Not answered: The bidder did not address the guiding questions in this section.

Category B: Integration

As part of the solution concept, the bidder is requested to provide a concise integration concept covering the implementation of the proposed RASP solution from contract award through to productive go-live. The concept should address the guiding questions set out below:

- Which key implementation steps are required for SDK (or equivalent) integration, testing, validation, and final go-live readiness, including any expected tuning of detection mechanisms or reduction of false positives?
- Which technical prerequisites, inputs, or decisions are required from the Client, and at what stage of the implementation are they needed?
- Which activities and responsibilities are expected from the contractor and from the Client during integration and the initial stabilization phase? The concept should include an indicative timeline with key milestones and expected Client input.

Focus of category B is on clarity, relevance, and structure of the information presented, including the readability and logical structure of the document while answering the guiding questions above. Category B of the solution concept will be evaluated using a scoring scale from **0 to 5 points**:

- 5 points – Excellent: Fully meets or exceeds expectations; comprehensive, well-structured, and highly relevant, providing clear added value.
- 4 points – Very good: Meets expectations with only minor omissions; clear, relevant, and well-structured.
- 3 points - Good: Meets expectations overall, though some details may be missing or could be further clarified.
- 2 points – Average: Generally adequate, but lacks detail or contains some inconsistencies or ambiguities.
- 1 point – Poor: Incomplete, unclear, and fails to address key aspects of the guiding questions.

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

- 0 points - Not answered: The bidder did not address the guiding questions in this section.

Category C: Security

The “Security” category consists of two parts: pentest, worth 20 points, and bug bounty, worth 15 points.

Pentest (20 points)

The contractor may submit up to **three pentest reports** as annexes to its bid submission including report and **documented retest**. Each pentest report is required to meet the following criteria on a pass/ fail basis:

- Timeliness: max. 24 months old
- Retest documented: yes
- Report shared as annex: yes
- Testing firm: accredited based on CREST, CHECK or BSI

If the above-mentioned must criteria are met, the following matrix describes the scoring system for Pentest that is only pentests that meet the above-mentioned criteria will be considered for the further evaluation according the below mentioned table. A maximum of 20 points is achievable.

For #3 and #4, only the most recent pentest will be taken into account.

If a bidder submits more than three pentest reports, only the 3 most recent reports will be considered for evaluation.

#	KPI	Max. Points	Logic
1	Number of pentests reports submitted	3	1 point - per test report submitted (retest does not count as test report)
2	Recency of delivered reports	6	Each time frame can be awarded once: - 3 points if report is within ≤6 months old - 2 points if report is within <6 and ≤12 months old - 1 points if report is within <12 and ≤18 months old <u>Note:</u> The maximum number of points can therefore only be achieved when providing pentests that cover a larger period of time/ the full time frame that is: The maximum points will only be awarded if the bidder submits 3 reports so that each report covers the above-mentioned time frame.
3	Platform coverage	3	- 3 points if both platforms covered (iOS + Android) - 1 point if single platform only <u>Note:</u> For #3 and #4, only the most recent pentest will be taken into account
4	Methodology	8	Pentest methodology should follow OWASP ASVS security domains listed below or equivalent – 2 points are awarded for each domain covered in the pentest (max. 8 points achievable): - Encoding and Sanitization (V1) - Validation and Business Logic (V2)

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

			<ul style="list-style-type: none"> - Session Management (7) - Authorization (V8) - Cryptography (V11) - Configuration (V13) - Secure Coding and Architecture (V15) - Security Logging and Error Handling (V16) <p><u>Note:</u> For #3 and #4, only the most recent pentest will be taken into account. If a pentest covers OWASP ASVS domains with an equivalent test approach, the bidder should indicate which domains from the above list are covered with a given test. The bidder can do so within the solution concept. Please visit the official website for details: https://owasp.org/www-project-application-security-verification-standard/</p>
--	--	--	---

Bug Bounty (15 points)

In order to enter scoring, the bidder is required to provide one bug bounty report that indicates participation in a bug bounty program. The scoring system lists the criteria to be achieved for a certain number of points. The bidder will only be awarded points for the highest point level achieved by the bug bounty report, no cumulation. A maximum of 15 points can be achieved.

- 0 points – If no report is available/was submitted 0 points will be awarded
- 5 points – If the contractor provides a report that indicates participation in a bug bounty program within the last **24 months**
- 10 points – If the contractor provides a report that shows
 - participation in a bug bounty program within the last **12 months** and
 - active tester participation (**5 or more payouts** within last 6 months) and
 - quick fixing of findings (average of **60 working days** to fix a finding) by the contractor
- 15 points – If the contractor provides a report that shows
 - participation in a bug bounty program within the last **6 months** and
 - very active tester participation (**10 or more payouts** within last 6 months) and
 - very quick fixing of findings (average of **20 working days** to fix a finding) by the contractor

If a bidder submits more than one bug bounty report, only the most recent report will be considered for evaluation.

3.3 Scoring for the award criterion „Quality“:

The total score is calculated as sum of the points achieved across all three categories. This cumulated score aims to reflect the overall quality of the provided solution and forms part of the bid's final evaluation.

3.4 Example calculation “Quality”

Check table below for an exemplified evaluation (all numbers fictional):

Procurement procedure Runtime Application Self-Protection (RASP) of SPRIND GmbH
Award number: EIN-1380

Category Name			Points (max.)	Points awarded	Comment
A	Solution Design		10	8	"Very good" representation in solution concept
B	Integration		5	4	"Good" representation in solution concept
C	Security				
	Pentest	# of pentest	3	3	3 reports provided
		Recency of reports	6	5	No report within time frame 12-18 months
		Platform coverage	3	3	For iOS & android
		Methodology	8	6	OWASP equivalent covering 6 domains
	Bug Bounty		15	10	Within last 12 months, 7 payouts within last 6 months, average time to fix finding of 32 days
	Summe		50	39	