European Payments Council

Request for Proposal

Service provider to establish and maintain the EPC MISP instance

EPC098-21 / 2021 Version 1.0 / Date issued: 28 April 2021

Public

Request for Proposal

EPC MISP Instance Service Provider

EPC098-21
2021 Version 1.0
Date issued: 28 April 2021

European Payments Council

European Payments Council AISBL,
Cours Saint-Michel 30 B-1040 Brussels
T +32 2 733 35 33
Enterprise N°0873.268.927
secretariat@epc-cep.eu

Table of Contents

0 Introduction

The European Payments Council (EPC), an international non-profit association, offers one focal point and voice for the European payment service provider's sector on all European payment issues. In constant dialogue with other stakeholders and regulators at European level, its role is to support and promote European payments integration and development, and provide Single Euro Payments Area (SEPA) payments schemes facilitating over 43 billion transactions across 36 countries every year.

The EPC's goal is to contribute to harmonised payments across SEPA – a goal which ultimately supports European competitiveness and innovation.

In its role of scheme manager, the EPC develops payment and payment-related schemes and updates them regularly to meet end-users' needs and technology evolution, sets up rules and technical standards for the execution of (or the supporting of) SEPA payment transactions and organises regular change management cycles opened to any stakeholders.

As a scheme manager, the EPC is also responsible for addressing fraud risks in the context of the schemes. To this end the EPC needs to take appropriate action related to fraud data collection and analysis, information sharing and prevention measures.

In addition, the ECB/Eurosystem, as overseer of the SEPA payment schemes, already recommended the EPC (i) to develop an early warning-sharing system for specific fraud cases, towards relevant scheme participants; and (ii) to broadcast fraud-related information towards all scheme participants, for example through the publication of quarterly qualitative dashboards.

In this context, the EPC Scheme Management Board (SMB) approved the EPC Payment Scheme Fraud Prevention Working Group (PSFPWG)'s implementation proposal on the development of a SEPA-wide "Malware Information Sharing Platform" ("MISP") instance for real-time fraud information sharing with direct browser access by all SEPA payment scheme participants.

The EPC intends to outsource the management and the maintenance of the EPC MISP instance. The purpose of this RFP document is to find a reliable independent service provider to which the EPC can outsource the management and the maintenance of the EPC MISP instance.

1 Scope of EPC MISP instance

1.1 Introduction to the EPC MISP instance

With the advent of SEPA instant payments, it became clear that the existing process for prioritising payment blocking requests related to fraud (through a bi-lateral email exchange process) is insufficient for contacting the appropriate persons related to payment blocking requests in case of fraudulent transactions in a timely manner.

In addition, the ECB/Eurosystem, as overseer of the SEPA payment schemes, already recommended the EPC (i) to develop an early warning-sharing system for specific fraud cases, towards relevant scheme participants; and (ii) to broadcast fraud-related information towards all scheme participants, for example through the publication of quarterly qualitative dashboards.

In light of these developments, and upon due consideration also taking into account existing fraud information sharing initiatives, the PSFPWG requested the SMB in September 2020 to be mandated to explore the possible use of the MISP for real-time fraud information sharing amongst SEPA payment scheme participants.

1.2 Use cases

The PSFPWG considers four main use cases:

- General sharing of information/ statistics on fraud (Broadcasting);
- Direct communication between two affected scheme participants[1];
- Sharing of IBAN lists, User Agents, Device IDs, IP-Addresses, websites, etc. (taking into account and subject to all applicable EU legal frameworks);
- Funds blocking and recovery.

The first two use cases (most straightforward) will be prioritised through a phased go-live approach, as these also relate to the use cases recommended by the Overseer. These will be expanded to the other two use cases and potentially further identified use cases along implementation and usage experiences, with the possibility of early adoption through pilots by volunteering participants/ national communities.

The fraud typology documentation and classification (maintenance) for the various use cases is to be aligned/mapped with the ECB payment statistical reporting and the EBA Guidelines on Fraud reporting, and if possible, in sync with the EBA Association's "Fraud Taxonomy" document.

The EPC will regularly report to the SEPA payment scheme's Overseer (the Eurosystem) in the context of the aforementioned use cases. Also, the MISP solution should allow the EPC to gather statistical information on fraud to support its 'broadcasting' role, however, without replacing or duplicating the participants' existing reporting duties pursuant to relevant rules and regulation.

1.3 IT architecture/ implementation

The PSFPWG recommends the following use-case based approaches to IT architecture/ implementation:

[1] Note: From the onset, this use case aims to complement the current SEPA scheme processes, including the SWIFT process for stopping fraudulent transactions by speeding up the processing of the formal recovery request (e.g., ISO 15022 message MT n92 'Request for Cancellation' (in combination with code 'FRAD')). When Participants contact each other on a specific case, reference to the related SWIFT message should be made.

- **Full Usability:** intended as providing easy-to-use platform and full availability of services for the EPC Community Members (i.e. SEPA scheme participants);
- **Full Security**: intended as providing full protection on information and identities of involved actors. SEPA scheme participants will access platform services in a secure way and will use them without any risks on databases protection;
- **Source Protection:** the Traffic Light Protocol (TLP) must always be used and followed;
- **Format and accessibility**: SEPA scheme participants must use the prescribed formats, protocols and taxonomies defined for the EPC purposes to allow the information to be fully utilised, exploited and easily consumed;
- **Responsiveness**: The SEPA scheme participants must be responsive to the needs of other community members to support their needs in a timely manner;
- **Compliant:** The information shared must comply with applicable laws and regulations (e.g. GDPR, Banking Secrecy, other legal/contractual obligations, etc).

Based on its analysis, the PSFPWG recommended a hybrid approach, whereby the EPC Secretariat (through a dedicated service provider) manages the MISP SEPA community on an EPC MISP instance with direct browser access by all SEPA participants, with the alternative possibility for each country to also establish a local MISP instance, whereby the EPC manages a list of all MISP instances' details (e.g. URL and AuthKey). Participants who run their own MISP instance would equally be able to connect with the EPC MISP instance.

Key components for implementation will include the principles to determine what to share and related distribution levels (i.e. with whom to share).

Concerning the principle to determine what to share, the PSFPWG agreed that SEPA scheme participants should endeavour to share as much information and financial indicators which they assess to be accurate, of relevance and which meet the objectives of EPC. Participants will have to follow the following sharing principles (as far as permitted in accordance with relevant internal and external rules and regulations):

- **Should share:** Participants should share financial indicators about confirmed fraud (e.g. Customer confirmed fraud, Analyst detected fraud) in order to counter and prevent further fraud;
- **Could share:** Participants could share financial indicators about "very likely" fraud in order to counter and prevent further fraud.

Participants will share information using the appropriate distribution levels as defined in MISP (i.e. "Your organization only"; "This Community-only"; "Connected communities"; "All communities"; or "Sharing group") and only within the EPC community. Notably, in MISP a community is defined as the set of the local organizations on a MISP server and the remote organizations connected by the sync users. Participants will be able to share fraud information even through restricted sharing groups. Sharing groups in MISP are a more granular way to create re-usable distribution lists for events that allow users to include organizations from their own instance (local organisations) as well as organisations from directly, or indirectly connected instances (external organisations).

Participants will be able to share information directly amongst themselves, in order not to lose time. Additionally, participants will be able to contact each other directly from the MISP.

1.4 Pilot and wider adoption of the EPC MISP instance

As part of the implementation, the PSFPWG recommended launching a 3-month EPC MISP pilot with volunteering Participants/ PSP communities. After a brief evaluation exercise and finetuning of the infrastructure and the governance framework as necessary, the EPC MISP should be fully operational and available to all interested Participants/ PSP communities by February 2022.

Obviously, a SEPA-wide adoption by scheme participants is a must for the EPC MISP to reach its full potential. At the present stage, the PSFPWG nevertheless considers it premature to recommend a mandatory migration by a given end-date, favouring an adoption based on merit and a gentle peer group pressure instead. Indeed, the PSFPWG considers that the current bi-lateral email exchange process is not a sustainable and future-proof pan-European solution in the context of instant payments and that the usage of pilot countries/communities, esp. cross-border, will demonstrate the usefulness and efficiency increase for data exchange/sharing and statistical purposes alike.

2 Defined terms and abreviations

In this document, the designations “we” and “our” are all used for the European Payments Council (EPC) as the party initiating this RFP.

The party answering to the RFP (making the bid) is referred to as 'SP candidate' or ‘SP’.

Term/Abbreviation	Definition
EPC	European Payments Council (in French: Conseil Européen des Paiements), an international non-profit association (in French: Association Internationale Sans But Lucratif, AISBL) established under and governed by Belgian law, having its registered office at Cours Saint-Michel 30, B-1040 Brussels, Belgium, and registered with the Crossroads Database for Enterprises under the enterprise number 0873.268.927 (register for legal entities Brussels)
EPC MISP instance	The central MISP instance which will form the central repository for the EPC MISP Community and which will be serviced by a dedicated Service Provider
Event	Any alert incident (related to fraud, malware, etc.)
GDPR	General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Governing documentation	The document(s) which set out the rules and conditions that regulate the use of, and contribution to, the MISP platform and the EPC MISP Community.
Hosted MISP Instance	A decentralized MISP instance hosted by a MISP Organization.
MISP Member	The MISP Organizations and the MISP Users which have access to the published information.
MISP Community	A MISP Community is composed of the local organizations on a MISP server and the remote organizations connected by the sync users. For further details see https://www.circl.lu/doc/misp/sharing/.
MISP Instance	A MISP Instance is an installation of the MISP software and the connected database. All the data visible to the users is stored locally in the database and data that is shareable (based on the distribution settings) can be synchronised with other instances via the Sync actions. For further details see https://www.circl.lu/doc/misp/general-concepts/#misp-instance.
MISP Organization	An organizational element which is grouping individual users that are maintaining their own events as a single entity. A MISP Organization must not necessarily take the form of a legal entity.

	Event ownership in MISP is organized at the MISP Organizations level.
MISP User	An individual member who has access credentials to the Platform through a MISP Organization.
Participant	An entity accepted to be a party to one or more SEPA Payment Scheme(s) in accordance with the relevant provisions of the Rulebooks.
Platform	The entire MISP system. It is to be understood as synonym of "MISP".
PSP	Payment Service Provider, as defined in Article 1 of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
Publishing party	The Publishing Party is the MISP Organization which is making the information available in the MISP by authorizing its publication via the platform, under the conditions of the relevant Governing documentation.
Remote MISP Instance	The instances that the EPC MISP instance synchronises with will be referred to as "remote instances". For further details see https://www.circl.lu/doc/misp/general-concepts/#misp-instance .
RFP	Request for Proposal
Rulebook	Each of the SEPA Credit Transfer Rulebook, the SEPA Instant Credit Transfer Rulebook, the SEPA Direct Debit Core rulebook and the SEPA Direct Debit Business-to-Business rulebook, as amended from time to time. The Rulebooks consist of a set of rules, practices and standards that make it possible for any eligible Participant to join, participate and operate in the SEPA Payment Schemes.
Payment Scheme	Each of the SEPA Credit Transfer Scheme, the SEPA Instant Credit Transfer Scheme, the SEPA Direct Debit Core Scheme and the SEPA Direct Debit Business-to-Business Scheme, as described in the Rulebooks
SEPA	Single Euro Payments Area The SEPA Payment Schemes are applicable in the countries listed in the EPC list of SEPA Scheme Countries (document EPC409-09, as amended from time to time).
Stakeholder	Within the SEPA context, the key stakeholders include amongst others: governments, authorities and regulators, the payments industry and their suppliers, corporates, small and medium-sized enterprises (SMEs), merchants, consumers, and their associations.

3 Practical Information

This chapter contains all the formalities and practicalities surrounding the RFP process.

3.1 Timeline

This section outlines the deadline for each stage of the RFP process:

Stage	Activity Deadline	Deadline Date
1	Publication of the RFP by the EPC on its website.	30 April 2021
2	Final date for SP candidates to submit written questions concerning the RFP documents.	14 May 2021cob
3	Final date for receipt of RFP responses. (See section Guide for submission of for details on how to submit your RFP response documents.) The EPC will analyse the RFP responses. In case there is a need for clarification as to elements of the response to the RFP the EPC will contact the RFP respondent via email. The respondent will have 5 business days to reply.	28 May 2021 cob
4	The EPC informs SP candidates of the outcome of the RFP process and, subject to that, the process going forward.	25 June 2021

3.2 Formalities

All SP candidates must structure their response to the RFP in accordance with the outline detailed in section 4 “Preparation and outline of RFP” of this document. This is to ensure comparability and that all relevant issues are dealt with. It is also essential that all items, requirements and expressed preferences are dealt with and replied to.

The SP candidate may supplement the outline with matters considered relevant by them. The EPC reserves the right to disregard RFP responses in which the SP candidate deviates from the outline to a significant extent.

If the SP candidate finds that there are unclear items, the SP candidate must specify the conditions on which its response to the RFP is based.

It should be noted that all or parts of the SP candidate’s response, as chosen by the EPC, may form part of a final contract between the parties.

3.3 Terms & Conditions of Response

Every proposal received by the EPC is deemed to have been made subject to these conditions. No other terms will be deemed to be accepted by the EPC or incorporated into any contract between the EPC and any SP candidate unless they are expressly accepted in writing by an authorised signatory of the EPC.

Confidentiality	Responses of SP candidates to the present RFP will be evaluated by the EPC. The final selection of the supplier will be subject to approval by the SMB in accordance with the EPC's established procedures and subject to the relevant provisions of Belgian law. The members of the PSFPWG who will review the responses of SP candidates for recommendation to the SMB shall be bound by a dedicated confidentiality agreement concluded with the EPC.
Examination and explanation of RFP documents	The SP candidate shall be responsible for carefully examining the complete RFP, including any addenda, and making whatever further arrangements as may be required such that the SP candidate is fully informed and acquainted with all the circumstances and matters which might in any way affect the performance or cost of the services which are the subject matter of the SP candidate's response. Failure to do so is at the sole risk of the SP candidate and no relief shall be given for errors or omissions in the response to the RFP in estimating the difficulty or cost of performing the requirements successfully. Should the SP candidate find discrepancies in, or omissions from, the Request for Proposal or relevant documents, or should these appear to be obscure or ambiguous, the SP candidate shall at once contact the EPC for clarification or correction thereof before submitting its proposal. Any SP candidate making a request for clarification or correction will be solely responsible for the timely receipt of such request by the EPC. Replies to such enquiries may be made in the form of written addenda that will be issued simultaneously to all SP candidates.
Unsolicited revisions to proposals	Unsolicited revisions to proposals will not be received favourably unless the SP candidate can substantiate to the EPC's satisfaction that a genuine error occurred during preparation of the original proposal. The EPC is under no obligation to accept such a revision.
Modification to RFP Documents	The EPC reserves the right to revise any provisions of the Request for Proposal. Such revisions, if any, will be in the form of written addenda which will be issued simultaneously to all SP candidates. SP candidates shall immediately acknowledge receipt of the addenda by e-mail.
RFP Expenses	All costs and expenses incurred by the SP candidates in the preparation and submission of their response or in attending subsequent discussions or negotiations with the EPC, are entirely

	for their own account and the EPC shall not be responsible for such expenses.
Currency/ pricing	All amounts will be in euro (EUR), excluding VAT.
Language	All proposals, correspondence and communications shall be in the English language.
Form of proposal	The SP candidate shall base its response on the requirements of the EPC as stated in this Request for Proposal. However, should any SP candidate be unable to fulfil any of these requirements it must state clearly any and all exceptions to such requirements that it may have made with words such as "This response is subject to the following qualifications: ….".
Submission of proposal	Proposals submitted shall be properly executed and completed by a representative of the respondent authorised to commit the SP candidate.
Closing Date	Proposals must be received by the EPC at the email address and no later than the Closing Date mentioned in section 3.1.
Withdrawal	The EPC reserves the right to withdraw the RFP and not to award work or compensation to any party.
Awarding Authority	Once the endorsement of a SP candidate has been decided upon by the SMB, the relevant SP candidate will be informed accordingly and invited to commence contract negotiations.

3.3.1 Duration of offer

The RFP response and related offer shall be irrevocable for a period of up to three (3) months from the closing date of the RFP.

3.3.2 Duration of contract

The RFP response must take into account an expected duration of the contract of three (3) years with the possibility of extension subject to mutual agreement.

3.3.3 Preparation of RFP response

The RFP response shall be prepared according to the instructions given by the EPC in section 4 “Preparation and outline of RFP response”.

3.3.4 Consideration of questions

Questions concerning the RFP documents shall be sent by email as outlined in section “Guide for submission of , queries and questions”. If possible, all questions must refer specifically to an exact reference in the RFP documents. Whenever appropriate, questions and related answers will be made publicly available in an anonymised version on the EPC website.

4 Preparation and outline of the RFP response

4.1 RFP document

The SP candidate must structure their RFP response in accordance with section 3.

4.2 Background and introduction

4.2.1 Introduction of the SP candidate

The SP candidate must provide:

- Key contact name, (e-mail) addresses and telephone number
- Name, legal form and registered address of the company
- Please indicate whether the SP candidate is a part of a corporate group, where its assets or liabilities may be shared with a parent or other group entity, and provide the name of the ultimate holding company (if applicable).
- A solvency statement (e.g., a letter from an external accountant (such as the SP candidate's statutory auditors, where relevant) confirming that the SP candidate is not insolvent and is able to pay its debts as they fall due) and/or a certificate of non-bankruptcy (this certificate can be obtained from the SP candidate's competent commercial court)

The SP candidate must also provide a high-level description of their organisation and key competencies as well as who would be engaged in the activities that are covered by the RFP.

4.2.2 Contact(s)

The SP candidate must specify the name, address, telephone number, email address and any other relevant contact information of the person who is familiar with the RFP response and who can be contacted by the EPC.

4.2.3 Reservations

The SP candidate shall provide the EPC with a copy of its general terms and conditions if available and applicable, and clearly indicate any reservations or limitations of liability regarding the provision of services according to the RFP documents. It is to be noted that the EPC cannot accept any limitation of liability for gross negligence or wilful misconduct.

Moreover, the possible implications of these reservations to the provision of the services must be stated.

4.2.4 Sub-contractor(s)

The SP candidate must provide a declaration that no sub-contractors will be used unless provided for in the contract with the EPC and advised in the submission. In that case sub-contractors need to be listed together with a short description of their specific role in relation to the activities covered by this RFP. Any change of sub-contractors during the project shall be subject to the prior approval of the EPC, which will not be unreasonably withheld. It is to be noted that the EPC will not waive any claim against third parties.

4.3 Description of the service

The SP candidate shall give a general description of the proposed services and how it will fulfil the needs and requirements of the EPC as described in this RFP.

The description should at least include:

- MISP Instance description
- Process flowchart
- Technical setup
- Testing plans and tools
- Maintenance
- Standards used (related to quality, security, ….)
- Other functionalities such as billing, administration etc.

4.4 Project delivery

A high-level planning indicating the various proposed steps to setup the EPC MISP instance (including expected resources needed from the EPC if applicable).

The service must be operational by 1 October 2021, the envisaged date of the launch of the 3-month pilot/ proof of concept.

4.5 Conditions

4.5.1 Licences

The SP candidate must include a description of any licences included in the offered solution as well as the specific conditions under which these licenses are valid. This should include information on the need for registered single user licenses and/or concurrent user licenses. Furthermore, the SP candidate must describe included functionalities/user rights under each license type(s).

It is expected however that no licenses will be required for the hosting of the EPC MISP instance as such, as the code of MISP is made available, free of charge on https://github.com/MISP/MISP, as part of the MISP installation package provided to any MISP Member who wants to host an instance of MISP.

4.5.2 Quality

The SP candidate's quality policy and practices must be outlined.

4.5.3 Accreditations

Formal recognition by an independent body, that the SP candidate operates according to international standards (e.g., ISO standards).

4.5.4 References

Experience of the SP candidate in providing a similar kind of service.

4.5.5 Risk-analysis

The SP candidate must include a description of the most significant risks to which it would be exposed in offering the service covered by the RFP, as well as the corresponding mitigating measures.

4.6 Requirements

The SP candidate must provide an answer to each individual requirement detailed in:

- Appendix A: Eligibility Requirements
- Appendix B: MISP Instance Requirements

4.7 Miscellaneous

Here, the SP candidate may describe other aspects that are considered by the candidate SP relevant to the EPC's evaluation of the RFP response such as datasheets, brochures, certifications, standards, etc.

4.8 Guide for submission of proposal, queries and questions

All RFP response documents, including correspondence and questions, must be submitted to EPC electronically. Emails must be sent in the format:

To: gert.heynderickx@epc-cep.eu

CC:

Subject EPC MISP Instance [SP *candidate name*] – [*brief description of email content]*

Files must be attached to the email in the following format:

Document	Filename	File Format
RFP document	EPC MISP Instance [SP *candidate name]* RFP version [#]	.docx or .pdf
Appendix A: Eligibility Requirements	EPC MISP Instance [SP *candidate name]* appendix A version [#]	.docx or .pdf
Appendix B: MISP Instance Requirements	EPC MISP Instance [SP *candidate name]* appendix B version [#]	.docx or .pdf
Other documents relevant to the RFP as determined by the SP candidate	EPC MISP Instance {SP *candidate name*] [*relevant file name*]	as applicable

The only email address to be used for submission of the response and other communication as part of the RFP process is: gert.heynderickx@epc-cep.eu

SP candidates must ensure that any emails sent to gert.heynderickx@epc-cep.eu are free from any virus or other malware. In consideration of their participation in the RFP process, each SP candidate agrees to indemnify the EPC from and against all costs, expenses, losses or damages that may result from the electronic copy being infected by a virus or other malware.

5 Requirements

The requirements are comprised of two elements:

- The eligibility requirements (EL)
- The MISP Instance requirements (MI)

Remark: in this RFP, the assumption is made that one single SP will be in charge of establishing and maintaining the EPC MISP instance. The SP candidate could however decide to outsource some parts of the requirements temporarily or permanently, but in this case, the conditions mentioned in section 4.2.4 of this document must be respected. In addition, it is necessary to specify that the SP will remain fully accountable for the servicing of the EPC MISP instance.

5.1 Eligibility requirements

In order to be eligible the SP must at all times fulfil the below requirements.

Reference	Requirement
EL-R1	The SP must operate the EPC MISP instance in a way that does not conflict with the interest of the schemes.
EL-R2	The SP must have a BCP in place.
EL-R3	The SP must comply with applicable rules and regulations. The regular place of business of the SP shall be established in the SEPA geographical area.
EL-R4	The SP must comply with applicable rules and regulations in the context of data protection and privacy.

5.2 MISP Instance requirements

The SP candidate must be able to meet all requirements detailed below and is invited to describe their solution for each requirement.

Reference	Requirement
MI-R1	The MISP software is an open source and free software released under the AGPL (Affero General Public License) and available on https://github.com/MISP/MISP, as part of the MISP installation package provided to any MISP Member who wants to host an instance of MISP.
MI-R2	Set up an instance of MISP on behalf of the EPC and based on the requirements provided by the EPC.
MI-R3	The SP should detail its general business requirements and range of service level agreements, e.g., availability in %, specified downtimes, reaction times, number of max. simultaneous users, recovery from failure, full daily back-up and retention time, etc.
MI-R4	Security: In order to maximize protection of data, identity information of involved actors and services exposed the SP must implement firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) perimeter measures. The channel to access the web portal will use secure protocols (HTTPS) to prevent the interception of the exchanged information.

Reference	Requirement
	In addition, the SP should evaluate the right integration of an external authentication mechanism to provide multi-factor authentication, for further details see https://www.circl.lu/doc/misp/appendices/.
MI-R5	All aspects of "hosting a MISP Instance" (hardware, support & maintenance, operations, user assistance, …) are the sole responsibility of the SP.
MI-R6	The EPC must be able to consult at any time an up-to-date list of entities having access to the EPC MISP instance.
MI-R7	The SP must nominate a MISP Technical POC.
MI-R8	In order to guarantee full compatibility between all MISP Instances of the EPC MISP Community, platform upgrades are to be done in full synchronization with all the other members hosting a MISP Instance.
MI-R9	Any security related patch and bug fix to MISP is to be installed by the SP as a matter of priority.
MI-R10	Data synchronization arrangements and configuration have to be agreed between the SP and the EPC.
MI-R11	The SP should ensure disaster recovery in Europe in maximum 48 hours.
MI-R12	The SP must ensure that all staff involved in operating the EPC MISP instance are adequately trained. Therefore, the staff training process must be documented.
MI-R13	The SP should ensure an audit trail is in place.
MI-R14	Prior to the implementation of every new system update affecting the EPC MISP instance, the SP must conduct and document all necessary tests to validate that all concerned procedures and systems function properly.
MI-R15	The SP must provide a yearly service level reporting to the EPC.
MI-R16	The SP candidate is invited to describe in detail the envisaged pricing structure (e.g., fixed vs variable elements, ….).
MI-R17	The SP should ensure that all aspects of "hosting a MISP Instance" follows the OWASP Web Security Testing Guide.
MI-R18	The SP agrees that the EPC can carry out own security tests on the MISP instance in order to guarantee a secure platform for all members.
MI-R19	Regarding platform functionalities: MISP Members will be able to access the platform from the internet with a web browser (using secure protocols - HTTPS) and the provided access credentials; MISP Members will be able to synchronize their own MISP instance with the EPC MISP instance.

6 Evaluation process

Responses of SP candidates to the present RFP will be evaluated by the EPC. The final selection of the EPC MISP Instance service provider will be subject to endorsement by the PSFPWG and the SMB. The members of the PSFPWG are bound by a dedicated confidentiality agreement. Notably, the SMB may not be provided with individual, non-anonymised confidential information related to the submitter of a response to this RFP, and/or the services or products offered by such submitter.

The EPC will evaluate the proposals based on, but not limited to, the following criteria: which are not listed in a prioritised order:

- Fulfilment of the eligibility requirements.
- Capability to set up the EPC MISP instance and be ready to launch the 3-month pilot within the expected timing.
- Capability to onboard scheme participants based on the Set up an instance of MISP on behalf of the EPC and based on the requirements provided by the EPC.
- Capability to suggest appropriate tailored processes and procedures.
- Experience with operating a similar type of MISP hosting services.
- The pricing model.
- The timing in which the SP candidate can perform the services.
- The capability of the SP candidate to maintain/update the EPC MISP instance process requirements within defined delays.
- Presence of efficient and user-friendly consultation and tracking systems.
- The general terms and conditions governing the SP candidate’s services.

7 Appendix A – Eligibility Requirements

Reference	Candidate response
EL-R1	
EL-R2	
EL-R3	
EL-R4	

8 Appendix B – MISP Instance Requirements

Reference	Candidate response	Solution description
MI-R1		
MI-R2		
MI-R3		
MI-R4		
MI-R5		
MI-R6		
MI-R7		
MI-R8		
MI-R9		
MI-R10		
MI-R11		
MI-R12		
MI-R13		
MI-R14		
MI-R15		
MI-R16		
MI-R17		
MI-R18		
MI-R19		