Q&A

EPC128-21
Version 1.0
Date issued: 26 May 2021
GHx

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

Public

Approved

EPC MISP Instance Service Provider RFP – Questions and answers

1 Scope of EPC MISP instance (RFP Section 1)

- RFP Section 1.2: Whether EPC can broadcast information which is relevant but NOT based on the data provided by participants?

  The EPC should indeed have the possibility to also access the EPC MISP instance and share certain relevant information via the EPC MISP Instance.

- RFP Section 1.2: It is mentioned that the shared information has to be aligned/mapped with 1) ECB payment statistical reporting 2) EBA Guidelines and 3) EBA Association's "Fraud Taxonomy" document.
  Can these documents be shared, so that we can understand the data formats?

  The documents mentioned in the RFP (ECB payment statistical reporting (link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1409), EBA guidelines (link: https://www.eba.europa.eu/sites/default/documents/files/document_library/960425/Final%20Report%20on%20EBA%20GL%20on%20fraud%20reporting%20-%20Consolidated%20version.pdf), EBA Association's Fraud Taxonomy (not yet publicly available)) are related to the taxonomy used to tag MISP events.

  Related to data formats, the MISP core format is a simple JSON format used by MISP and other tools to exchange events and attributes. The MISP format is described as Internet-Draft in misp-rfc. https://github.com/MISP/MISP-rfc. In addition, MISP events can be exported in several formats such as JSON, XML, CSV (https://www.circl.lu/doc/misp/automation/)

- RFP Section 1.3: What is the shelf life of the shared information? What are the purging requirements? What is the data archival policy?

  The purging / erasure of data must always comply with legal obligations (e.g., GDPR).

  The exact requirements are to be further defined.

- RFP Section 1.3: Which format will be used for sharing the fraud data by PSPs, banks and EPC? Whether ISO 20022/15022 will be used? If so what message?

  - import: bulk-import, batch-import, import from OpenIOC, GFI sandbox, ThreatConnect CSV, MISP standard format or STIX 1.1/2.0

  - export: OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools), Cache format (used for forensic tools), STIX (XML and JSON) 1 and 2, NIDS export (Suricata, Snort and Bro/Zeek) or RPZ zone

- RFP Section 1.3: What is the data curation policy? how data de-duplication will be handled? For example, how data curation / aggregation of the same fraud reported by many participants will be (need to be) handled? Do we have guidelines for this? Do we give equal weightage to each FI reported information independently or de-duplicate?

  There is no data curation policy at present. It is foreseen that de-duplication should be managed at the participant level (e.g., to be handled in the user manual), not at the level of the service provider.

- RFP Section 1.3: Is there a need of support to help design these policies and procedures as for participant users as a part of the engagement?

  Not foreseen.

- RFP Section 1.3: What is the purpose of Region level physical instances? Why are they required? Can you please elaborate the purpose of this segregation?

  The possibility of synchronizing two MISP instances is an important requirement as other PSP/PSP communities may already have one MISP instance running. This is mainly to avoid the burden of having to connect and share information on two instances separately.

- RFP Section 1.3: 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).
  Question: SP will own the EPC MISP Instance. Will the local MISP instances deployed in local countries also be managed by SP (including central infrastructure)?

  No, (local) MISP instances already in place will not be managed by the SP.

- RFP Section 1.3: Will EPC community MISP Instance be a private/logical one? Yes.
  Are you going to gather MISP events from other communities? Yes.
  Are you going to publish events to external communities? Yes, according to a policy still to be defined.

- RFP Section 1.3: Scope for EPC MISP pilot: What is scope for EPC Pilot solution within 3-month timeline?

  The purpose of the pilot is to fully understand the potential of the MISP instance in the context of the EPC and in the prevention of fraud as well as to find possible flaws in the governance model to correct it. The pilot simultaneously serves as 'proof of concept' (POC) of the MISP instance, aiming to demonstrate its feasibility and practical potential.

- RFP Section 1.3: Given the sensitivity of the data stored in the MISP instance (IBAN and payment information of EU citizens), potentially for only specific recipients, is the expectation on the SP that the level of data protection is equivalent to that of banking platforms?

  Yes, indeed. Note however that the decision and responsibility to publish information on the EPC MISP Instance rests exclusively with the relevant Participant acting as Publishing party, who will act as Data Controller in the context of the GDPR. Specific rules are set out in the

Terms of Use/ user manual for participants to the EPC MISP Instance (not yet available), but this is not to be controlled by the SP.

- RFP Section 1.3: Is there a planned method for geographical limitation of shared data? Currently not all countries in the SEPA region are deemed equivalent from a data protection stand-point.

  This is currently not foreseen at the level of the EPC MISP Instance itself, but will be the responsibility of the relevant Participant acting as Publishing party, who will act as Data Controller in the context of the GDPR.

- RFP Section 1.3: Is the intention to share PII based on consent or legitimate interest, and what is the defined acceptable usage of the data?

  If any personal data would be processed in the context of the EPC MISP instance, it would be processed in a secure manner with the aim of preventing fraud and as such to contribute to ensuring the safe and trustworthy processing of SEPA payments.

  The legal basis for the processing is covered under the “Legitimate interest” (Article 6(1)(f) GDPR):

  “[where] processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.”

  Furthermore, under GDPR Recitals 47, 49 and 50, certain expressed purposes of processing of personal data may constitute a legitimate interest. These purposes are:

  - Fraud prevention;
  - Ensuring network and information security;
  - Identifying possible criminal activity or threats to public security.

- RFP Section 1.3: Given the hybrid scenario described on chapter 1.3. Could you confirm that only the EPC MISP instances is in scope?

  Yes, indeed.

- RFP Section 1.4: Could you clarify if the 3 moths of POC are included in the 36 months of service or the service will start once the POC is finished?

  The 36 months of service will start after the “POC”, subject to the successful completion of the POC/ pilot phase.

- RFP Section 1.4: What is the expected/estimated volume of MISP information sharing transactions flowing through the instance per year in 5 years’ time?

  This is difficult to assess.

- Who defines, implements and monitors the rules for sync?

  To be included with the Terms of Use/ user manual for participants to the EPC MISP Instance (not yet available).

- Is there a defined content update workflow?

  The tasks that each participant needs to perform in order to create/update and publish MISP events will be defined in the workflow in the user manual.

- Is there a defined template in place for rollout of additional MISP instances?

  No.

- The EPC is responsible for addressing fraud risks in the context of the schemes. The SP is not in charge of these risks?

  No, this is not the responsibility of the SP.

- "The assumption is made that one single SP will be in charge of establishing and maintaining the EPC MISP instance”. Please clarify?

  The EPC intends to engage one (and only one) SP to perform the services of establishing and maintaining the EPC MISP instance.

- Who defines taxonomy and tag list?

  The EPC.

- Who is responsible if there is a negative impact of sharing data?

  The decision and responsibility to publish information on the EPC MISP Instance rests exclusively with the relevant Participant acting as Publishing party.

- Is there a clear Point of Service definition, so consequences of errors could be assigned?

  N/A

- How many partners, users and clicks per minute are you expecting for central MISP instance?

  It is at present not possible to evaluate those parameters.

- What is the roadmap for horizontal scaling to additional MISP instances?

  N/A

- Is anonymization of data under the responsibility of EPC?

  No, the Publishing party, who will act as Data Controller in the context of the GDPR, is responsible for data anonymization, if and when relevant.

- What kind of information will be shared? Could you please provide some more details?

  The Platform is limited to the sharing of fraud-related information (including incidents, trends, modus operandi and statistics).

- How will the created events be managed? Are there any available examples of events?

  Yes, through https://www.circl.lu/doc/misp/.

- What kind of feeds will be used by the MISP instances?

  No external feeds should be used. See the MISP training material available at https://github.com/MISP/misp-training and https://www.circl.lu/doc/misp/ for details.

- Which kind of integration is expected to be implemented by the participants? Are there any examples of integration?

  There are no external tools to integrate.

- Is there any automation required?

  No, not needed.

- Could you please provide some more details about the mentioned pre-described formats, protocols and taxonomies? Which taxonomies should be active? Would it be possible to have some documentation about them?

  Documentation is available in the MISP github repository.

2 Preparation and outline of the RFP response (RFP Section 4)

- RFP Section 4.4: Could you clarify the expectation on the 1st of October 2021? On this date the service will need to be fully operational (POC completed) or is this the planned pilot start date?

  No, the platform will not be fully operational by that time. The pilot phase is intended as POC, limited to a single use case. After the pilot, taxonomies will have to be further implemented, etc.

3 Requirements (RFP Section 5)

- RFP Section 5: In this RFP, given the assumption that a SP shall establish and maintain the EPC MISP instance, could you confirm that currently no EPC MISP instance is in place?

  That is correct, no EPC MISP instance is currently in place.

- Should the SP provide a service management system for tickets, requests?

  Not sure yet. The SP is requested to spell out in its response whether this can be accommodated. If this would be the case, it is expected that tickets would be opened with a moderate frequency only (for example for implementing Firewall rules).

- Who will be responsible for user support and installation/distribution support?

  The SP for the EPC MISP Instance will be responsible for user support. No software installation is foreseen.

- Who is organizing blocklists? Is there any responsibility for the provider?

  If blocklists would be used, the EPC would be accountable, and the SP would be the responsible to manage this blocklist.

- Is it expected that every data access is monitored?

  Access is automatically logged in the MISP Instance. The SP should guarantee the connection to and from the Internet of the customer VLAN through the perimeter protection system in place providing NGFW and IPS. The traffic flows and the IPS rules will be agreed with the EPC before the services are put into production, in any case the EPC can request changes to the rules by reporting to the SP technical support.

- Who will manage Sharing Groups?

  The EPC – the management of sharing groups should be included in the user manual.

- There is no co-management planned from EPC side. Therefore, it is expected that we will provide fully managed MISP Platform. Is this assumption correct?

  Yes, indeed.

- Necessary communication changes for new MISP members will be managed by the SP?

The EPC – through the user manual.

- Are the MISP contents provided by EPC and ready to implement? Do we (SP) have the task to formulate or check MISP contents?

  No, this is not required of the SP.

- EPC MISP instance process requirements: Do we need to implement new instances as part of the service or will this be done by separate projects?

  The SP will have to establish the EPC MISP Instance as a new MISP instance. No other instances are to be established.

- EL-R1 What do you mean with the following sentence: The SP must operate the EPC MISP instance in a way that does not conflict with the interest of the schemes.

  The schemes provide a set of interbank rules, practices and standards to be complied with by Participants who adhere to the schemes, allowing payment service providers in SEPA to offer SEPA-wide euro (instant) credit transfer and/or direct debit products to customers. The EPC MISP instance aims at facilitating the exchange of fraud-related information through the provision of a platform that allows the sharing of financial fraud indicators within a trusted community of scheme Participants, thus contributing to the safety and the interests of the scheme. Safeguarding the interests of the scheme can thus be considered - albeit indirectly - at the heart of the services requested from the SP. The due management of potential situations of conflict of interest and/or the need for “Chinese walls”/confidentiality undertakings are equally part of this requirement.

- MI-R1 Is the SP responsible for issues and bugs in the MISP software at https://github.com/MISP/ ? Does this include an obligation to maintain the software?

  There are no SP responsibilities for issues and bugs. The SP must commit to applying relevant patches and updates when available.

- MI-R1 If the SP is not responsible for the maintenance of the MISP software, what is the expected frequency of updates by the Github community to the MISP software, and what is the lead-time by the Github community to fix a critical issue?

  Please refer to https://www.circl.lu/.

- MI-R1 How will one classify the particular file/IP address(new) as Malware/threat (Any pre-defined format)?

  Through predefined tags.

- MI-R1 Is there any limitation for sharing Threat information.

  No, the decision and responsibility to publish information on the EPC MISP Instance rests exclusively with the relevant Participant acting as Publishing party. Specific rules are set out in the Terms of Use/ user manual for participants to the EPC MISP Instance (not yet available), but this is not to be controlled by the SP.

- MI-R2 To setup an instance of MISP by SP - what will be the hardware/software requirements?

  Requirements based on the ones from CIRCL.LU (link: https://www.circl.lu/doc/misp/).

- MI-R3 What is the projected number of participating MISP data sharing organisations in the next 5 years?

  This is difficult to assess.

- MI-R3 Please confirm the expected monthly volumes & % hit rate?

  N/A

- MI-R3 Are there monthly / Quarterly volume spikes?

  Not excluded.

- MI-R3 Please confirm the average handling time at a Maker & Checker level

  No such logic foreseen.

- MI-R3 What is the Recovery Time Objective (RTO), Volumes to be processed under the BCP scenario?

  N/A

- MI-R3 Please confirm the expected business hours – Is 24*7 support required

  • System management and maintenance of servers (Mon - Fri 8.00 - 18.00)

  • Corrective Support in case of malfunctions (H24 7/7)

- MI-R3 Is there a requirement for SP employees to interact with end customer, If Yes, will you be providing the necessary Voice / email infrastructure?

  Not needed.

- MI-R4 What will be the mode of application access (Citrix, VMware, RDP, Direct access etc.)?

  Direct access via browser.

- MI-R4 In order to define a MFA solution in term of technology and economics we would like to know:

  - Which factor should be used?

  - How many users?

  - Could be a SaaS solution compliant?

  - How and where a user will be created?

  We could consider evaluating the integration of MFA tools during the pilot phase.

- MI-R4 Does EPC need a dedicate Firewall or will it be possible to use a shared one (that's anyway compliant with RFP requirement)?

  The SP can also use a shared Firewall.

- MI-R4 Given that we have several options to respond to the MFA requirement, are you willing to include the evaluation of the available options during the pilot phase?

  Yes.

- RFP Section 1 and MI-R5 Could you confirm that EPC MISP Instance should be hosted on SP's infrastructure?

  Yes, indeed. Any intended subcontracting is to be clearly spelled out in the response to the RFP.

- MI-R5 Please provide any specific qualitative and quantitative security and compliance requirements for hosting of your platform

Security should be state of the art.

- MI-R5 Please provide the quantitative requirement that you need to host on Private or public cloud platform

  N/A

- MI-R5 Are there any other specific requirements provided by EPC for the SP for hosting MISP?

  N/A

- MI-R6 What would be the procedure for a service provider to become an MISP member?

  The onboarding procedure will be defined in the Terms of Use/ user manual for participants to the EPC MISP Instance. The EPC will approve the membership application, which will then be communicated to the SP for operational onboarding.

- MI-R7 What will be the skill set required for the MISP technical POC to be nominated by the SP?

  As a minimum, the technical POC will need to know all aspects at the application level (adding a user, adding an org, adding a new server, etc.).

- MI-R8 In case of platform upgrade of EPC MISP instance, after the notification between SP and EPC, is EPC the entity that should arrange the update date with the EPC community?

  The SP should monitor the releases of new versions of the platform. Thereafter, the EPC and the SP will jointly choose a date for the maintenance activities which will be communicated by the EPC to Participants with access to the platform.

- MI-R12 Which EPC figures are involved in the project? Is training of these resources required?

  N/A

- MI-R12 Is there any specific MISP related training material which the staff of the SP need to be trained in before hosting the instance?

  All MISP training material (including source code) is available at https://github.com/MISP/misp-training.

  https://www.circl.lu/doc/misp/.

- MI-R12 What would be the average size of the team on the SP side which would provide the support of this application?

  It is expected that maximum two people would be required. Once the project has started, we believe that one person will suffice to manage the profiling requests on the platform.

- MI-R12 Is there any other language other than English in scope?

  No, English will be the default language.

- RFP Section 3.3 and MI-R16 To share the economics, do you have a particular form you would like us to fill in or any format would be accepted?

  There is no predefined format.

- MI-R19 Please confirm if operation that is, manual disambiguation of Fraud hits is in scope for the RFP

  Yes, indeed.

- RFP Section 5.2: Our understanding is - SP needs to use the basic framework which has already been developed and available at https://github.com/MISP/MISP.

  - Whether this framework and its design is documented and will be made available to SP? Whether the framework is tested and test logs will be made available to SP?

  - Does this mean we will just implement and do the SIT, certify for readiness and operationalize?

  The framework has indeed been tried and tested; all necessary details are available through https://github.com/MISP/MISP.