

Explanation and Supplementation to the PMC Extension of the deadline to submit responses

Preliminary market consultation: „Supply, operation, support and further development of eFTI Gate CZ”

Evidence No.: PTK_2026_A416

Introductory Information

The Administrator of the Preliminary Market Consultation “Supply, Operation, Support, and Development of eFTI Gate CZ”, CENDIS, s.p. (hereinafter “**Administrator**”), conducted pursuant to Section 33 of Act No. 134/2016 Coll., on Public Procurement, as amended (hereinafter “**PMC**”) on behalf of the Ministry of Transport of the Czech Republic (hereinafter “**Contracting Authority**”), has received additional questions from participants of the PMC. The Administrator hereby provides the PMC participants with this explanation and supplementation as part of a transparent process, with the aim that the participants provide the most appropriate responses possible.

A. Timeline and process

A.1. Second round of PMC

Context: The PMC Invitation allows for the possibility of a second round, potentially in a format other than written.

Is the Contracting Authority planning a second round of PMC (e.g., a workshop, individual consultations, presentations), and if so, when is it tentatively scheduled?

Answer:

We are not currently planning a second round of PMC; we believe we will be able to obtain the necessary information during the first round.

A.2. Pilot operation and acceptance procedure

Context: Annex No. 1, Section 4.3 specifies a pilot operation and acceptance testing period of two months (06.05.2027 – 05.07.2027).

Could you please specify:

- (a) the anticipated scope of the pilot operation in terms of participating control authorities, geographic coverage, and modes of transport?
- (b) whether a pilot integration of a specific eFTI Platform is planned, and what type of integration it would be (test/production)?
- (c) the main acceptance criteria and how compliance with them will be measured?

Answer:

The scope and exact nature of the pilot operation cannot be precisely determined at this time. We anticipate that

- a) all Czech regulatory authorities affected by the eFTI Regulation will be actively involved in the pilot operation. Geographically, the entire Czech Republic and all modes of transport covered by the Regulation must be taken into account.

- b) Currently, no eFTI platform is available in the Czech Republic; therefore, it cannot be guaranteed that its integration will be possible before the launch of the pilot operation.
- c) Acceptance criteria and the method for measuring their fulfilment are not specified at this stage of the project.

A.3. Division of the public contract into lots

Context: The scope of supply includes three distinct components: eFTI Gate, the UAP user application, and the Helpdesk.

Is the Contracting Authority considering dividing the public contract into lots that could be awarded separately, or is a single integrated contract with a single supplier being planned?

Answer:

The goal is to issue a single public contract covering all components of the supply.

B. Supply options and infrastructure

B.1. Preferred variant of the Contracting Authority

Context: Annex No. 2 covers both SaaS and on-premise options.

Based on previous analyses, does the Contracting Authority have its own indicative preference regarding the supply option (SaaS, on-premises in the customer's cloud, or on-premises in its own infrastructure)? What factors are key for the Contracting Authority when deciding on the option? This is highly sensitive data—is the geographical factor important? For example, should data be stored only in the Czech Republic or within the EU?

Answer:

At this time, the Contracting Authority does not have a preference for any particular variant of tender. From a geographical data perspective, the most important factor is that the operator be listed in the National Cloud Computing Catalogue.

B.2. Customer's cloud

Context: The questionnaire (Annex No. 2) mentions the option of running the on-premises solution in the Customer's cloud.

Please specify:

- (a) What type of cloud platform is it (eGovernment cloud / proprietary private cloud / a specific provider's public cloud)?
- (b) What is the available capacity and what are the potential limitations for deploying the new information system?
- (c) What are the administrative and technical requirements for deploying the solution being provided?

Answer:

If the Customer's cloud is to be used, Microsoft Azure is available. There is no capacity limit (the cost of the infrastructure will be included in the price comparison). The technical requirements stipulate that the supplier will prepare Terraform scripts and all necessary pipelines.

B.3. Registration in the National Cloud Computing Catalogue

Context: Annex No. 1, Section 4.3, specifies the requirement for suppliers to register in the NK CC (approximately 3 months; registration must be completed by 09.07.2027).

Does the Contracting Authority require the supplier to register with NK CC even if the solution will be operated in the Customer's cloud, or does this obligation fall on the Customer in such a case?

Answer:

In accordance with the requirements of Act No. 365/2000 Coll., the entire supply chain must be registered. Therefore, the entity providing the service must be registered as of the date the service is provided.

C. Integration with CAAIS and other systems

C.1. CAAIS – Availability and integration requirements

Context: Integration with CAAIS is preferred as the primary method of user authentication and authorization for UAP.

Please clarify:

- (a) Is CAAIS currently fully operational and covering all required functions, or are some functions still missing or under development?
- (b) Is a CAAIS test environment available for development and integration testing?
- (c) What is the integration request process, and who will be the point of contact on the Customer's side (we assume DIA)?
- (d) What are the typical response times and SLAs for developer support from the CAAIS operator?

Answer:

- a) CAAIS currently supports all required functions.
- b) CAAIS has a testing environment for development and integration testing.
- c) Communication with DIA is handled by the Customer (Ministry of Transport).
- d) There is no defined SLA for these activities, but in general, the CAAIS team responds very promptly.

C.2. Alternative authentication mechanism

Context: Annex No. 1, Section 4.1, states that if integration with CAAIS is not completed on time, the delivery must include an alternative authentication mechanism in accordance with Implementing Regulation 2024/1942.

How does the Contracting Authority define the term "alternative mechanism"? What minimum level of equivalence to CAAIS does it expect (level of electronic identification assurance, MFA, federation, etc.)?

Answer:

The solution must meet all the requirements set forth in Implementing Regulation 2024/1942 in this regard, specifically the requirements set forth in Chapter II, Article 5, and Chapter II, Article 4, paragraph 3.

C.3. The existing IT environment of control authorities

Context: Annex No. 1, Section 4.2, lists integrations with the internal systems of audit authorities as a future development outside the current scope.

Does the current project plan include any integration with existing systems used by control authorities (Customs Administration - Celní správa České republiky, Directorate of Traffic Police Service - Ředitelství služby dopravní policie, Road Transport Inspection - Inspekce silniční dopravy, Civil Aviation Authority - Úřad pro civilní letectví, etc.) as part of the current supply, or will all such integrations actually be the subject of future development?

Answer:

The project as a whole does not plan to integrate with the existing systems of control authorities.

The project anticipates that control authorities will be provided with an integration interface that they can use to integrate their systems themselves. This interface is not planned to be part of the first phase of the project, but rather part of future development.

C.4. eFTI Platforms in the Czech Republic

Context: For the pilot integration and testing, it is important to know whether there are or will be operators of certified eFTI platforms in the Czech Republic.

Are there currently any operators of certified eFTI platforms in the Czech Republic, or is it expected that the first certification will take place concurrently with the implementation of eFTI Gate CZ? Does the Contracting Authority plan to conduct a pilot integration with a specific eFTI platform as part of the acceptance testing process?

Answer:

Currently, no eFTI Platform is available or certified in the Czech Republic. There is currently no clear timeline for its development. However, integration with the eFTI Platform is still part of the requested supply, based on the available technical specifications.

D. Security and PKI

D.1. PKI Infrastructure for eFTI Certificates

Context: Article 10 of Implementing Regulation 2024/1942 requires Member States to issue security certificates for eDelivery Access Points.

Please clarify the responsibilities regarding the PKI infrastructure:

- (a) Will the existing Czech Republic national certification authority be used?
- (b) Is the establishment of a dedicated certification authority for eFTI anticipated?
- (c) What are the technical security requirements for private keys (HSM, FIPS levels)?
- (d) Will PKI management be part of the supply, or will it be provided by a third party?

Answer:

a) It is necessary to use a certification authority that meets the requirements of the eIDAS Regulation 2.0.

b) No.

c) The requirements are specified in the eIDAS Regulation 2.0.

d) Services for qualified seals with time stamps provided by the Ministry of Transport may be used.

D.2. Classification under the Cybersecurity Act

Context: The implementation must comply with Act No. 264/2025. Coll.

Will eFTI Gate CZ be classified as a regulated service under Act No. 264/2025? If so, what specific security requirements arising from this classification apply to the provider and its supply chain?

Answer:

Yes, this is a regulated service. Security Level 3. The requirements for suppliers are set forth in Annex 5 of Decree No. 409/2025, and primarily within the scope of Sections 17–26 of that decree .

E. Operation, SLA and support

E.1. Definition of availability and SLA metrics

Context: Annex No. 1, Section 5.3 specifies an SLA requirement without providing specific values.

Please provide:

- (a) the method for calculating availability (with/without planned outages, penalty scheme)?
- (b) specific availability targets for eFTI Gate, UAP, and the Helpdesk?
- (c) RTO and RPO requirements for disaster recovery?
- (d) the proposed method for measuring and reporting SLA compliance?

Answer:

- a) including downtime
- b) 99.5% uptime for Gate and UAP during 24/7 operation; 98% uptime for the helpdesk during 10/5 hours
- c) RTO ≤ 4 hours, RPO ≤ 15 minutes
- d) defined automated reports from access logs made available to the Customer

E.2. Helpdesk operating hours

Context: Section 5.4 of Annex No. 1 specifies mandatory helpdesk hours of “10:00 a.m.–4:00 p.m. CET,” whereas Article 12(4) of Implementing Regulation 2024/1942 specifies synchronized availability of “8:00 a.m.–6:00 p.m. CET” across the EU.

Could you please clarify which hours apply to the L1 and L2 helpdesks for eFTI Gate CZ? We assume that the 10:00 a.m.–4:00 p.m. CET time slot represents the minimum coverage across the EU, while the national helpdesk must cover 8:00 a.m.–6:00 p.m. CET.

Answer:

Implementing Regulation 2024/1942 specifies a minimum coverage period of 10:00 a.m. to 4:00 p.m. CET, and the Contracting Authority requires the same coverage in accordance with this regulation.

E.3. On-call support outside working hours

Context: Article 12(4) of Implementing Regulation 2024/1942 requires on-call support on weekends and public holidays for urgent issues.

What is the expected scope of on-call support:

- (a) response time for urgent incidents?
- (b) types of incidents classified as “urgent”?
- (c) requirement to be available during which time window outside of regular working hours?

Answer:

We require 24/7 availability.

E.4. Change requests and scope of development

Context: Annex No. 2, the “Financial Details” sheet, provides an estimate of “approx. 200 MD/year” for change requests.

How did the Contracting Authority make this estimate, and what types of requirements are included in it (legislative updates, new functional requirements from regulatory authorities, technological updates to EU components)? Does the Contracting Authority expect legislative updates to be priced separately as a distinct item?

Answer:

The estimate of the scope of change requests, amounting to 200 MD per year, is based on an expert assessment of the minimum development requirements, excluding mandatory modifications related to legislative changes by the European Commission.

The participants should list legislative updates as a separate item.

Technological updates must be included under the "System Operation" item.

F. Contractual Framework and IP

F.1. Contract template

Context: Some questions in Annex No. 2 (G10, A10) ask about the supplier’s own contract template.

Does the Contracting Authority have its own standard contract template for this type of public contract? If so, will it be available in the PMC for pricing purposes, or only in the procurement documents? Key pricing factors include, in particular, the penalty scheme, guarantees, and the scope of the supplier’s liability.

Answer:

The contract template is not yet available.

F.2. Transfer of Source Code and Intellectual Property Rights

Context: For custom-developed components (e.g., user applications, integration with CA AIS, country-specific functionality).

What form of IP rights transfer does the Contracting Authority require:

- (a) a full transfer of copyright?
- (b) a broad license with the right to modify and transfer to another supplier?

- (c) escrow of source code?
- (d) a different approach for different types of components (custom development / open-source / proprietary)?

Answer:

The Contracting Authority requests the right to modify and use the supplied solution without restriction for its own purposes, without prejudice to the supplier's ability to continue using, providing, or licensing the solution to other clients. The contractual arrangement therefore does not aim at a complete transfer of copyright ownership to the Customer, but rather at granting a sufficiently broad license to use the work, including the right to modify and develop it.

F.3. Open-source components

Context: Since the standards (eDelivery, Domibus) are publicly available as open-source.

What is the Contracting Authority's position on the use of open-source components in the delivery:

- (a) Are components licensed under Apache 2.0, MIT, EUPL, or GPL acceptable?
- (b) What are the requirements for documentation regarding the origin of open-source components (e.g., SBOM)?

Answer:

- a) They are acceptable.
- b) A reference to the original documentation and the method of integration/configuration included in the supply is sufficient.

G. Clarification of the Scope of Performance

G.1. Backoffice application

Context: Annex No. 1, Section 4.2, refers to the "back-office application" as part of future development.

Is this application truly outside the scope of the current release, or is at least a basic administrative UI expected to be included in the standard release for essential operational functions (eFTI Platform registration, viewing statistics and audit logs, configuration management)?

Answer:

The back-office application is not included in the basic requested supply.

G.2. Cross-border testing activities

Context: Testing with eFTI Gates from other member states is key to verifying interoperability.

Does the Contracting Authority plan for eFTI Gate CZ to participate in cross-border testing activities with eFTI Gates from other Member States (e.g., as part of the eFTI4EU/eFTI4ALL pilots)? If so, what is the expected scope, and who will serve as the coordinator?

Answer:

During testing and pilot operations, it is also necessary to plan for integration with the eFTI gateways of other member states. The Ministry of Transport will coordinate these integrations.

Integration with the eFTI gateways of all member states must be taken into account. The specific practical possibilities for integration will not be known until the implementation phase.

G.3. Control authorities' cooperation

Context: The delivery involves up to 8 regulatory agencies with varying levels of IT capability.

How will coordination among control authorities be ensured during implementation:

- (a) Will there be a dedicated coordinating body or role on the part of the Contracting Authority?
- (b) How will any conflicting requirements from individual authorities be addressed?
- (c) Will approval from individual authorities be required as part of the acceptance procedure?

Answer:

The Contracting Authority has established an interagency working group comprising all relevant supervisory authorities, which will ensure information sharing and the necessary coordination. Specific requirements of individual control authorities that go beyond the scope of Implementing Regulation 2024/1942 are not included in the scope of the requested supply and will therefore be subject to further development as necessary.

G.4. Participation in EU working groups

Context: Article 13 of Implementing Regulation 2024/1942 establishes the Network of Operational Support as a subgroup of the DTLF.

Does the Contracting Authority or PMC Administrator plan to actively participate in the Network of Operational Support and related DTLF working groups prior to the start of implementation? Will the supplier be expected to provide technical support for this participation (e.g., preparation of materials, technical consultations)?

Answer:

A supplier may be involved, if necessary, but is not required. No preparation of materials is expected.

H. Operational and data aspects

H.1. Volume of Rol records and scaling

Context: To properly size the solution and establish realistic SLAs, it is essential to know the expected volume of data traffic.

What volume of data traffic does the Contracting Authority expect?

- (a) Estimated number of active eFTI datasets in the Rol under steady-state conditions?
- (b) Average and peak daily/monthly volume of newly created/updated records?
- (c) Estimated number of verification queries (search + UIL request) from Czech control authorities per day/month?
- (d) Expected number of follow-up reports?

Answer:

Information for (a) and (b) is not available.

Regarding the questions in (c) and (d), it can be assumed that there will be in the low hundreds of thousands of audits per year, with a gradual increase in the proportion of documents in eFTI format from 1% in the first year to 60% within five years.

H.2. Multicast search latency and timeout

Context: Article 3(3) of Implementing Regulation 2024/1942 sets a 60-second timeout for responding to requests for eFTI data, but does not explicitly address the behaviour of the search mechanism when querying up to 27 EU Gateways with varying latency and availability.

Please clarify the following:

- (a) What is the maximum total search response time the Contracting Authority expects from a road inspection UX perspective?
- (b) How should the system respond if a timeout is exceeded at one or more other Gates (partial results vs. complete failure)?
- (c) Should a mechanism be implemented to parallelize queries and degrade service when peer Gates are slow?

Answer:

- a) Maximum 3 seconds.
- b) According to Chapter I, Article 3, Paragraph 3, Subparagraph d) of the Regulation, the application must return a “no response” message sent by the eFTI gateway or platform if that gateway or platform confirmed receipt of the request but did not send a message containing the required eFTI data within 60 seconds of the acknowledgment of receipt. This should therefore also apply to the search mechanism.
- c) Can be implemented.

H.3. Standardization and normalization of identifiers across the EU

Context: The identifiers used to search eFTI data (particularly vehicle registration numbers) vary across EU member states in terms of format (delimiters, spaces, letter variations), alphabet (Latin vs. Cyrillic in Bulgaria), and structure. Standardization is key to ensuring reliable searches across the EU network.

Please clarify the following:

- (a) Is there a binding EU-level standard for identifier formats (e.g., specifications on how a license plate number should be written)?
- (b) Does the Contracting Authority expect the implementation of a normalization layer in eFTI Gate CZ (removal of separators, transliteration, conversion to lowercase, etc.)?
- (c) How should cross-alphabet searches be handled (e.g., a Bulgarian Cyrillic license plate during a check in the Czech Republic)?
- (d) Is there an EC technical guidance document available on this issue?

Answer:

Regarding the standardization of identifiers across the EU, we note that, according to currently available legislation and eFTI implementing acts, there is no known separate binding EU standard that uniformly defines the syntactic format of identifiers used for searching (e.g., vehicle registration plates), including rules for delimiters, case sensitivity, transliteration, or the representation of national variants. The implementing acts primarily define interoperable mechanisms for access, search, and the Registry of Identifiers (RoI), rather than detailed harmonization of national identifiers.

However, from the perspective of interoperability and practical usability, we recommend that eFTI Gate CZ include a normalization layer to enable robust search capabilities across EU member states. Typically, this involves removing spaces and separators, unifying character sizes, Unicode normalization, and supporting basic transliteration for supported alphabets. At the same time, we recommend always retaining the original identifier value for audit and legal purposes and creating a normalized (“canonical”) representation alongside it for search purposes.

When searching across different alphabets (e.g., Bulgarian Cyrillic), we recommend implementing deterministic normalization and transliteration rules that allow for comparison between the original and Latinized representations of the identifier. We do not anticipate the use of fuzzy or AI-based matching mechanisms, but rather a standard canonical comparison approach.

To date, there is no separate public technical guidance document from the European Commission specifically addressing the standardization of registration marks or the transliteration of identifiers within the eFTI framework.

However, it is expected that the European Commission may gradually issue additional recommendations or implementation guidance as part of the development of the eFTI interoperability framework.

H.4. Failure or delay in deactivating the RoI record.

Context: Article 11(4) of Implementing Regulation 2024/1942 provides for the deactivation of the UIL upon upload of the goods delivery date (eFTI188). In practice, deactivation may fail (technical error, unavailability) or be delayed, which may lead to a control based on a record that should be invalid.

Please clarify:

- (a) What consistency mechanism (eventual or strong consistency) does the Contracting Authority expect between the eFTI Platform and the RoI?
- (b) What is the liability of the eFTI Gate supplier if a check is performed on an invalid record where the error occurred on the eFTI Platform side?
- (c) Is monitoring and alerting required for failed or delayed deactivations?
- (d) Is a retry mechanism or a time limit for achieving consistency required?

Answer:

The Contracting Authority prefers a model of eventual consistency between the eFTI Platform and the Registry of Identifiers (RoI), whereby UIL deactivation must be propagated asynchronously via a reliable messaging mechanism with guaranteed delivery, a retry policy, and an audit trail.

Strong consistency is not required.

The solution must ensure:

- idempotent UIL deactivation,
- resilience against temporary component unavailability,
- auditability of state changes,
- a defined maximum propagation time for deactivation,
- and mechanisms for resolving transient inconsistencies.

The Registry of Identifiers is considered a discovery/index component, not an authoritative source of legal validity for transport data.

H.5. The Cabotage Logic and History

Context: Annex No. 2 contains only the general question G34 on cabotage. Cabotage checks under Regulation (EU) No 1072/2009 require access to transport history within a seven-day window, which goes beyond the scope of the standard UIL lifecycle.

Please clarify the following:

- (a) What is the expected scope of cabotage checks within the eFTI Gate CZ system?
- (b) Is it planned to store the history of deactivated UILs in the RoI for the period necessary for cabotage checks?
- (c) Is a UI in the UAP required that allows the inspector to view the vehicle's transport history?
- (d) Will integration with other data sources (e.g., vehicle registries) be part of the delivery or future development?

Answer:

- a) No additional eFTI functionality is expected with regard to cabotage. It is only required that records in the RoI not be deactivated before the time limit for cabotage transport under applicable legislation has expired, in the case of road transport (mode of transport).
- b) The deactivation of such specific records in the RoI should take place only after the time limit for cabotage transport under applicable legislation has expired. See Implementing Regulation 2024/1942, Chapter III, Article 11, Paragraph 4.
- c) The vehicle's transport history is not required.
- d) Integration with other data sources is not currently required.

H.6. SLA and Dependence on third parties

Context: The operation of eFTI Gate CZ depends on the availability of other eFTI Gates in the EU, on eFTI Platforms operated by the private sector, and on the European Commission's central services—that is, on third parties beyond the supplier's control.

Please clarify:

- (a) How will the SLA distinguish between the supplier's obligations regarding its own solution and those regarding end-to-end availability with third parties?
- (b) What are the expected exclusion clauses regarding outages of the EU Gate, the eFTI Platform, or EC services?
- (c) Is the supplier responsible for monitoring the availability of the EU Gate peer, or is this handled centrally by the EC?
- (d) What is the supplier's liability for incidents caused by third-party components (e.g., Domibus, eDelivery infrastructure)?

Answer:

- (a) The Contracting Authority anticipates separating SLA parameters for: components and services fully operated by the supplier within the eFTI Gate CZ, and services or infrastructure operated by third parties outside the supplier's direct control (e.g., EU Gate peers, eFTI Platforms, EC central services).

The supplier will be responsible for the availability, operability, monitoring, and support of the eFTI Gate CZ components it operates.

End-to-end availability of the entire cross-border transaction will be evaluated with regard to dependencies on external systems and will not automatically be considered a breach of the SLA by the supplier if the cause of the incident originated outside the environment managed by the supplier.

The Contracting Authority expects that the SLA will include a clear responsibility boundary between the national eFTI Gate CZ and the external components of the eFTI ecosystem.

(b) No central EC services are anticipated.

(c) The Contracting Authority expects the supplier to ensure monitoring of connectivity and operational availability of external dependencies relevant to the operation of eFTI Gate CZ, in particular:

- EU Gate peers,
- eDelivery endpoints,
- and integration interfaces used by the solution.

However, the supplier is not expected to be responsible for the operational management or availability management of EU Gate peers operated by other Member States or the European Commission.

If the EC provides centralized monitoring or service status, these are expected to be used as a supplementary source of information. Local monitoring of integration links, however, remains part of the operational responsibility of the eFTI Gate CZ supplier.

(d) The supplier shall not be liable for failures of third-party components or pan-European infrastructure that are not under its control (e.g., Domibus, eDelivery infrastructure, EC services, or external eFTI Platforms).

However, the supplier will be responsible for:

- the proper integration of these components into the eFTI Gate CZ solution,
- compatibility with the required versions and standards,
- the implementation of recommended resilience mechanisms,
- monitoring and alerting,
- retry and recovery mechanisms,
- secure behavior in the event of external service outages,
- and operational support during incident diagnosis.

The Contracting Authority expects the solution architecture to be designed to minimize the impact of transient outages of third-party components and to enable secure restoration of communication once the external service is restored.

H.7. UAP operation during connectivity outages

Context: Roadside inspections often take place in locations with limited or unreliable mobile connectivity (highways in remote areas, border crossings, underground parking garages). At the same time, the eFTI architecture requires online access to the Rol and eFTI Platforms.

Please clarify:

(a) What behaviour does the Contracting Authority expect from the UAP in the event of complete or partial network unavailability?

(b) Is support for offline buffering of queries, to be sent once connectivity is restored, expected?

(c) Are there requirements for a local cache for any data?

(d) How should the inspector be informed about the connectivity status and the extent of any limitations?

Answer:

The Implementing Regulation does not specify these requirements, and a proposal for a possible solution is therefore expected from the future supplier.

Article 4(2) of Regulation (EU) 2020/1056 states that economic operators must also be able to make regulatory information available in a human-readable format on the screen of an electronic device owned by the economic operator concerned.

H.8. Interpretation of the specifications and resolution of disputes with other Member States

Context: Experience with other EU digital infrastructures (EETS, eIDAS, ICS2) has shown that differing interpretations of the same legal text by individual Member States cause operational and integration problems. The Network of Operational Support (Article 13 of Implementing Regulation 2024/1942) is a formal forum, but its decision-making authority is not specified in detail in the regulation.

Please clarify:

- (a) What is the expected process for escalating technical or interpretive disputes with other Member States?
- (b) Is the Network of Operational Support, the EC's L3 helpdesk, or another entity considered the final arbiter?
- (c) Does the Contracting Authority plan for CZ Gate to actively contribute to the development of technical guidance documents, and is the supplier's participation expected in this regard?
- (d) What is the expected process for updating eFTI Gate CZ when new guidance documents are issued during the operational phase?

Answer:

(a) The Contracting Authority envisions a multi-level escalation process corresponding to the nature of the problem:

Technical/Operational Level – Issues will primarily be resolved among the operational teams of the affected eFTI Gates and the relevant support contacts.

Coordination/EU level – In the event of an unresolved issue, escalation is anticipated through structures established by the European Commission, particularly within the Network of Operational Support pursuant to Article 13 of Implementing Regulation 2024/1942.

Legislative/interpretative level - If the dispute requires a more binding interpretative opinion, the European Commission is expected to be involved as the coordinating body of the eFTI framework.

The Contracting Authority does not expect the supplier to independently decide on the legal interpretation of European legislation. However, the supplier must be able to provide technical documentation, analyses, and cooperation in resolving cross-border incidents and interoperability issues.

(b) Based on currently available legislation, the Network of Operational Support is not explicitly defined as a formal arbitration body with legally binding decision-making authority.

The Contracting Authority assumes that:

- The Network of Operational Support will be the primary coordination and operational forum for resolving interoperability and technical issues,

- technical guidance and recommended interpretation procedures may be further coordinated through the European Commission's support structures (e.g., L3 support/helpdesk),
- and in the case of fundamental interpretative issues, the decisive opinion will be provided by the European Commission within the eFTI governance framework.

Until such time as the EC's governance model is further clarified, the Contracting Authority anticipates a pragmatic interoperability approach based on common technical guidance and operational best practices.

(c) The Contracting Authority anticipates the active participation of the Czech Republic in the working and coordination structures related to the implementation of the eFTI framework, particularly in the areas of interoperability, operations, and technical harmonization.

At the same time, the Contracting Authority expects the supplier to provide expert technical cooperation, in particular:

- in analysing interoperability issues,
- in preparing technical opinions,
- in assessing the impacts of guidance documents,
- and in proposing implementation measures.

However, it is not expected that the supplier will act as an independent representative of the Czech Republic towards the European Commission or other Member States without authorization from the Contracting Authority.

(d) The Contracting Authority expects that the architecture and operational model of eFTI Gate CZ will be designed with regard to the ongoing development of the European eFTI framework and the expected issuance of new technical guidance, interoperability recommendations, or implementation specifications.

The supplier must ensure:

- ongoing assessment of the impacts of newly issued guidance documents,
- proposal of necessary changes to the solution,
- assessment of impacts on interoperability and operations,
- and implementation of changes within the standard change management process.

The Contracting Authority anticipates that:

- minor interoperability adjustments and configuration changes will be addressed within the scope of operational support,
- more extensive changes of a legislative or architectural nature may be addressed through a separate change request process.

The solution should include sufficient modularity and configurability to enable the implementation of future interoperability requirements without the need for a fundamental redesign of the entire eFTI Gate CZ.

Extension of the deadline to submit responses

Given the scope and technical complexity of the eFTI subject matter, and following the receipt of requests to extend the deadline for submitting responses, the Contracting Authority and the Administrator have decided to extend this deadline until Monday **25.05.2026 at 08:00**.

Conclusion

The PMC Administrator believes that these answers will enable participants to better respond to the structured questions in Annex No. 2 of the PMC Invitation and will provide the Contracting Authority with realistic and well-prepared documentation for the preparation of the procurement process.

CENDIS, s.p.
PMC Administrator, on behalf of Contracting Authority