Limited Liability Company “Tet”
Reg. No. 40003052786
Riga, Dzirnavu Street 105, LV-1011

Riga, 7 April 2026,

Description of the Procurement Subject
Procurement of a high-performance sovereign Key Management System (KMS) for secure data protection in a multi-tenant environment for the research project “Full-cycle data encryption key management platform solution for data protection in transit and at rest in data centres and cloud environments”

1. Purpose of the procurement

The purpose of the procurement is to acquire a high-performance sovereign Key Management System (hereinafter - KMS) that provides centralized cryptographic key management and secure servicing of multiple independent tenants (multi-tenant architecture).
The procurement is implemented within the Contracting Authority’s research project No. 1.7, “Full-cycle data encryption key management platform solution for data protection in transit and at rest in data centres and cloud environments”. The research project is implemented within the project of Limited Liability Company “IT Competence Center” entitled “Information and Communication Technology Competence Center for Digitization”, ID No. 2.2.1.3.i.0/1/24/A/CFLA/006.
The procurement is organized in accordance with Cabinet of Ministers Regulation No. 104 of 28 February 2017, “Regulations Regarding Procurement Procedure and Procedures for Application Thereof to Projects Financed by a Contracting Authority”, and taking into account Cabinet of Ministers Regulation No. 32 of 9 January 2024, “Regulations Regarding the Implementation of the Second Round of Investment 5.1.1.2.i "Support Instrument for Research and Internationalisation" under Reform 5.1.1.r "Innovation Management and Motivation of Private Research and Development (R&D) Investments" of Reform and Investment Direction 5.1 "Promotion of Productivity through Increase in the Amount of Investments for Research and Development (R&D)" of the Plan for Recovery and Resilience Facility of Latvia”.

2. Contracting Authority

Name:	Tet, Limited Liability Company
Registration number:	40003052786
Legal / actual address:	Riga, Dzirnavu iela 105, LV-1011
Contact person:	Zanda Strautiņa, phone: +371 26358611, e-mail: zanda.strautina@tet.lv

3. Description of the service

3.1. Scope of the procurement subject:
- 3.1.1. Software licences - rights to use the Tenderer’s offered KMS solution in accordance with the contract terms.
- 3.1.2. Maintenance and support services - if provided in the Tenderer’s offer or technical specification, including incident resolution, consultations, updates and technical support.

3.2. Service content:
- 3.2.1. The Contractor shall provide a solution that functions as a centralized platform for cryptographic operations and key management, capable of simultaneously serving multiple independent tenants (multi-tenant environment), ensuring their complete logical and cryptographic isolation.
- 3.2.2. The Contractor shall ensure operation of the system within local Tet’s Cloud infrastructure without dependence on external services and shall also ensure the possibility of integrating the solution with the Contracting Authority’s existing infrastructure, operating systems, databases and security systems.
- 3.2.3. The solution shall provide full lifecycle management functionality for cryptographic keys and digital certificates, including access control mechanisms, auditing and monitoring capabilities, as well as compliance with system security requirements, ensuring data protection both at rest and in transit.
- 3.2.4. As a result of the service provision, the Contracting Authority shall receive a functioning, scalable and secure KMS that meets technical, security and regulatory requirements.
- 3.2.5. The detailed Technical Specification of the service is set out in Annex No. 3 “Technical Specification”.
- 3.2.6. The place of service provision is the Republic of Latvia.

3.2.7. The term for service provision is up to 60 (sixty) months from the date of contract conclusion, including within the research project until 31 August 2027.

3.3. Procedure for service acceptance:

3.3.1. Service acceptance shall take place after delivery of the solution and commissioning in accordance with the Contract and the Technical Specification.

3.3.2. Detailed service acceptance procedure, including inspection procedure, defect rectification procedure and deadlines, shall be set out in the Contract.

3.3.3. The service shall be deemed accepted after mutual signing of the handover-acceptance act.

3.4. Selection criteria for Tenderers

3.4.1. The Tenderer entitled to submit an offer shall be registered in accordance with regulatory enactments and shall have the right to carry out commercial activity.

3.4.2. Tenderer shall have experience in the supply and implementation of information technology solutions related to data protection, cryptography or key management.

3.4.3. Tenderer shall have sufficient technical resources and competence to provide the Service in accordance with the Technical Specification.

3.4.4. Tenderer shall have access to qualified specialists with appropriate knowledge in the field of information technology and information security.

3.4.5. Contracting Authority may not conclude a contract with a Tenderer with whom the Contracting Authority is in a conflict of interest within the meaning of point 12 of Cabinet of Ministers Regulation No. 104 of 28 February 2017, "Regulations Regarding Procurement Procedure and Procedures for Application Thereof to Projects Financed by a Contracting Authority".

3.4.6. Tenderer entitled to submit an offer shall not be registered in any of the countries listed in Cabinet of Ministers Regulation No. 333 of 27 June 2023, "List of Low-Tax or Tax-Free Countries and Territories".

4. Deadline for submitting questions

4.1. Tenderer has the right to ask any question relating to this Procurement. Questions about the subject of procurement must be submitted in the correspondence module of the iepirkumi.lv procurement system or to the e-mail zanda.strautina@tet.lv. Questions regarding the procurement shall be accepted until 17 April 2026 at 12:00.

4.2. The Contracting Authority will provide answers to questions in accordance with the following procedure:

4.2.1. Within two working days after receipt of a question, the Contracting Authority prepares an answer and publishes it or send it to the Contractor together with the submitted question.

4.2.2. The identity of the question submitter shall not be disclosed.

5. Deadline and place for submitting the Tender

5.1. In accordance with the requirements stated in the notice published on the The Procurement Monitoring Bureau website (www.iub.gov.lv).

5.2. The tender shall be submitted in the iepirkumi.lv e-procurement system or sent to e-mail zanda.strautina@tet.lv by 24 April 2026 at 16:00 local time.

6. Requirements for Tender preparation

6.1. Tender shall be submitted for the entire scope of the procurement subject.

6.2. Tender shall be prepared in Latvian or English, in the computer file form, using the form attached in Annex No. 1, including all information necessary for evaluation.

6.3. Tender shall be signed by a person entitled to represent the Tenderer or by an authorized person. If Tender is signed by an authorized person, the tender shall include a power of attorney issued by the Tenderer.

6.4. Tender shall describe the compliance of the offered service with all Technical Specification requirements.

6.5. In Annex No. 1 "Tender Form", prices shall be stated in euros, separately indicating the tender price excluding VAT, VAT separately, and the total tender amount including VAT, including all costs related to service provision.

6.6. Tender shall be submitted in electronic document form, signed with a secure electronic signature, in the iepirkumi.lv e-procurement system or sent to e-mail zanda.strautina@tet.lv.

6.7. Received tenders shall be registered according to the time of receipt. Tenders received after the deadline shall not be evaluated.

6.8. After Tender submission deadline, the Tenderer may not unilaterally amend its tender.

6.9. The Tender validity period shall be not less than 60 (sixty) days from the date of submission of tenders. The Contracting Authority and the Tenderer may agree to extend the validity period of the Tender.

7. Documents to be submitted

7.1. Tender (completed Annex No. 1 "Tender" form).

7.2. Declaration (completed Annex No. 2 “Declaration” form).
7.3. Description of the Tenderer’s experience (completed Annex No. 4 form).
7.4. Information on the solution offered by the Tenderer, its compliance with the Technical Specification and its main functionalities.
7.5. Other documents at the Tenderer’s discretion, insofar as they do not conflict with the procurement documentation or the requirements of applicable regulatory enactments.

8. Evaluation of the Tender and decision-making

8.1. The Contracting Authority shall announce an open procurement procedure by publishing a notice of the procurement procedure of the funding recipient and the description of the procurement subject on the website of the Procurement Monitoring Bureau (www.iub.gov.lv). The notice of the procurement procedure of the funding recipient published on the IUB website shall specify the initial deadline for submission of tenders.
8.2. After opening the received tenders, the Contracting Authority shall evaluate them:
  8.2.1. Tenders that do not comply with the Tenderer selection criteria set out in the procurement regulations shall not be considered further.
  8.2.2. Tenders that comply with the Tenderer selection criteria shall be evaluated according to the principle of the economically most advantageous tender, considering the tender price and compliance with the Technical Specification.
  8.2.3. If necessary, the Contracting Authority shall initiate a negotiation procedure with selected Tenderers and ask Tenderers to submit final tenders.
8.3. The Contracting Authority shall select from the tenders the offer of the Tenderer that is economically the most advantageous for the Contracting Authority and complies with the requirements defined in the procurement regulations.
8.4. The Contracting Authority is entitled to terminate the procurement procedure at any time without determining a winner of the procurement, informing the Tenderers thereof.

Anex No. 3

Technical Specification

Purpose of the system:

The purpose of the Procurement is to acquire a high-performance sovereign Key Management System (hereinafter — KMS) that, as a central orchestration platform, can simultaneously and securely serve multiple independent tenants (for example, business units or client organizations) (multi-tenant architecture).

The solution shall offer self-service capabilities, allowing each tenant to independently and autonomously define its own cryptography policies.

The system shall guarantee data sovereignty, avoiding vendor lock-in and allowing the Root of Trust to be stored in local infrastructure (for example, on-premises HSM), while providing a standardized interface for encrypting public cloud and private infrastructure resources for the needs of each tenant.

High performance, scalability and data protection (at rest and in transit)

The system must be able to scale dynamically to serve a changing number of users, servers, applications, microservices and databases, ensuring consistently low response time (latency).

The system must guarantee continuous and comprehensive data protection both in the storage phase (data at rest) across different databases and repositories, and in the transmission phase (data in transit), automating the full lifecycle of keys and TLS certificates.

The system must ensure full lifecycle isolation for each tenant - requests, keys, configuration and user management - guaranteeing that the actions of one tenant do not affect the overall operation of the system or the quality of services received by other tenants.

The solution shall provide absolute logical and cryptographic isolation - the data, keys, configurations and policies of one tenant must under no circumstances be accessible to or affected by other customers.

The system shall support granular role-based access control (RBAC) within each tenant and shall generate individual, mutually separated audit logs.

Each tenant must be able to conduct an independent audit and meet its own regulatory requirements (for example, DORA, NIS2, GDPR), while allowing the platform's main administrators to integrate the overall system logs with centralized Security Information and Event Management (SIEM) solutions.

Cryptographic agility and post-quantum cryptography (PQC) readiness

The system architecture must incorporate the principles of cryptographic agility.

Given the development of quantum computing and the threats it poses to classical asymmetric encryption algorithms, the KMS solution must be proactively prepared for the implementation of Post-Quantum Cryptography (PQC).

This means the system must be capable, without architectural rebuild or service downtime, of dynamically updating, integrating and managing new standardized quantum-safe and hybrid algorithms (for example, NIST-approved ones).

In the context of a multi-tenant environment, the platform must provide flexibility allowing each tenant independently and gradually to migrate its encryption policies, keys and certificates to PQC standards.

General technical requirements of the system

Requirement ID	Requirement name and description
Cloud-1	All components necessary for system operation, configuration and maintenance - including the Control Plane, Management Plane, as well as the cryptographic operations data plane itself (Data/Crypto Plane) and audit modules - must be deployable and autonomously operable locally in Tet Cloud infrastructu
Cloud-2	The system must be able to fully function in this local environment (Tet Cloud) without any need to communicate with the developer's or any other third-party external (SaaS/PaaS) services. This applies to telemetry, license validation, update checks, key backup and any other administrative or management functions.
Cloud-3	The solution must technically support deployment on the sovereign cloud offered platform (VMWare Cloud Director 8+. The manufacturer must provide platform support).
Cloud-4	The system must include backup & restore functionality or otherwise provide support for backup and restoration at the VMWare hypervisor level.

Functional requirement: Management

Requirement ID	Requirement name and description
Admin-1	The system must provide a decentralized management model, offering each tenant a secure and isolated self-service portal (GUI). Tenant local administrators must be able to independently perform full lifecycle management of cryptographic assets — generate, import, rotate and revoke encryption keys. In addition, tenants must be able to define and adjust strict cryptographic policies themselves, such as approved algorithms, key validity periods, rotation schedules and specific role-based access (RBAC) rules within their resources. The tenant must be able to perform all actions necessary to use the solution without platform administrator involvement.
Admin-2	The solution must be fully automatable. All system functions and capabilities available in the graphical user interface (GUI) must be accessible and manageable through modern, secure and well-documented API endpoints. This includes both administrative operations (Management Plane), such as tenant creation and policy assignment, and operational operations (Data Plane), such as data encryption, decryption and signing.
Admin-3	The KMS platform must provide software development kits (SDKs) for multiple programming languages (for example, Java, Python, .NET).
Admin-4	The platform must include built-in tools for real-time telemetry and performance monitoring. The system must automatically collect detailed metrics on cryptographic operation intensity (for example, operations per second - TPS), key usage frequency, latency and error rates. In line with the isolation principle, each tenant must be able to see only the statistics of its own environment.

Functional requirements: Integration

Requirement ID	Requirement name and description
INTEGR-1	The system must provide full support for the KMIP (Key Management Interoperability Protocol) standard (versions 1.2 to 2.x/3.x).
INTEGR-2	The system must provide standard (out-of-the-box) compatibility with the most common virtualization hypervisors, at least VMware vSphere (supporting vCenter Server integration, VM and vSAN data encryption), and Microsoft Hyper-V (supporting Shielded VMs, i.e. protected virtual machine architecture). The KMS must be able to automatically, using KMIP, issue keys for encrypting virtual machine disks at rest.
INTEGR-3	The KMS platform must be able to serve as an external key manager and integrate with hardware from the most common disk array (SAN/NAS) manufacturers (for example, NetApp, Dell EMC, HPE, Pure Storage, etc.). The system must manage the authentication and encryption keys of hardware-level self-encrypting drives (SED - Self-Encrypting Drives) and storage controllers, ensuring media security in the event of physical theft or decommissioning.
INTEGR-4	The system must provide integration options with native cryptographic contexts of standard operating systems used. • Microsoft Windows: integration using the Windows CNG (Cryptography Next Generation) API and/or EKM (Extensible Key Management). • Linux (RHEL and Ubuntu families): support for standard PKCS#11 modules and OpenSSL interfaces, as well as the ability to orchestrate keys for operating system disk encryption (LUKS - Linux Unified Key Setup).
INTEGR-5	The system must provide integration options with standard middleware and database management systems (DBMS) to enable encryption at the application or database level. The system must support:

Requirement ID	Requirement name and description
	• Databases: integration through TDE (Transparent Data Encryption) technology with the most common database systems (for example, Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL, etc.) • Web / Application servers: integration with web servers (for example, NGINX, Apache HTTP Server) and Java application servers (Apache Tomcat, Red Hat JBoss/WildFly), to securely store and retrieve TLS session private keys outside the server file system.
INTEGR-6	The system must provide integration options with existing public key infrastructure (PKI). It is mandatory that it can integrate with Microsoft Windows Active Directory Certificate Services (MS AD CS), as well as other common CA systems. The KMS must securely generate asymmetric key pairs within its protected perimeter and orchestrate X.509 certificate request (CSR), issuance, renewal and revocation (CRL/OCSP) processes using standard protocols (e.g., SCEP, EST, CMP or REST API).

User authentication and roles

Requirement ID	Requirement name and description
IAM-1	The system must provide a fully separated, autonomous authorization and access control architecture for each tenant. Processing of access rights and authorization rules must be logically isolated, guaranteeing that one tenant's user rights, groups or access levels do not overlap with or affect other tenants' environments under any circumstances.
IAM-2	The solution must support the ability for both the platform's global administrators and each tenant individually to configure and connect their own independent external Identity Providers (IdP). For integration, the system must natively support at least SAML 2.0 and OpenID Connect (OIDC) protocols, allowing the organization's existing authentication solutions to be used.
IAM-3	The system must provide functionality that allows each tenant, within its isolated environment, to create, modify and administer customized access roles (Role-Based Access Control - RBAC), thereby ensuring strict adherence to the Segregation of Duties principle. For critical system, configuration or cryptographic operations (for example, key destruction), the platform must support the possibility of implementing the "four-eyes principle" (Quorum / Multi-party authorization), systemically requiring confirmation from at least two independent, duly authorized users.
IAM-4	The system must provide the ability for each tenant to create and maintain independent, built-in local user accounts. Tenants must have the right to define and manage password security policies for local accounts themselves, including password complexity requirements, validity periods, and change and rotation conditions. The system must provide multi-factor authentication (MFA) functionality for all local accounts, with the option to define it as a mandatory access requirement.
IAM-5	The system must automatically generate immutable audit records that are strictly separated for each tenant. Each tenant must be able to define a customized audit log retention policy in its own environment. In addition, the solution must provide a built-in capability to securely forward audit records to external centralized log storage solutions or SIEM (Security Information and Event Management) platforms, supporting standard protocols and formats (for example, Syslog, CEF format).

Cryptography standard requirements

Requirement ID	Requirement name and description
Crypto-1	The system must ensure strict logical and physical isolation of cryptographic keys between different platform tenants. Within the multi-tenant architecture,

Requirement ID	Requirement name and description
	the solution must support integration with Hardware Security Modules (HSM), allowing each tenant to be assigned a separate, independent HSM partition (slot).
Crypto-2	The system must offer flexible key storage and protection options depending on each tenant's security policy and performance requirements. It must provide the possibility to store keys securely at the software level (for example, in an encrypted local database), as well as offer the highest-security option - storing keys and processing operations directly bound to the HSM device (HSM-backed key storage).
Crypto-3	The system must provide full, automated orchestration of X.509 digital certificate lifecycles. The system must be able to centrally manage certificate request (CSR), generation, issuance, renewal (rotation) and revocation, using recognized standards (for example, SCEP, EST, ACME or REST API integrations).
Crypto-4	The platform's main security architecture must be based on a Hardware Root-of-Trust. All main system keys (Master Keys or Key Encryption Keys) used to encrypt and protect lower-level data keys (DEK) must be generated and continuously stored securely.
Crypto-5	The system must provide enforcement of a key residency policy (Key Residency Enforcement). The solution shall allow administrators to define rules that guarantee that the keys of certain tenants can be geographically or logically restricted (for example, they may reside only in a specific physical HSM device), systematically blocking any attempts to export, clone or synchronize them outside the permitted perimeter.
Crypto-6	The system must provide sustainability of the cryptographic algorithms used (Crypto Agility) in order to ensure readiness for threats to asymmetric cryptography posed by quantum computing. Technical support must be provided for the post-quantum cryptography (PQC) algorithms approved by the US National Institute of Standards and Technology (NIST) (for example, ML-KEM, ML-DSA). The system must provide the ability to use hybrid encryption (combining classical, e.g. RSA/ECC, and PQC algorithms simultaneously) to ensure a secure and standards-compliant transition process.

General security requirements

Requirement ID	Requirement name and description
DRO-1	The software development process shall be established in accordance with the guidelines of ISO/IEC 27034.
DRO-2	Data protection across different application layers shall be built using different protection mechanisms.
DRO-3	Information and data in the system must not be accessible by bypassing software security controls, for example at the operating system, file system or database level.
DRO-4	The system development and implementation shall not use components that the manufacturer positions as "Obsolete", software for which end-of-life is not planned within the next 2 (two) years, or software otherwise not recommended for use in production systems.
DRO-5	The Contractor shall, upon the Contracting Authority's request, provide a description of how the system compliance with security requirements will be ensured.
DRO-6	Access to subsystems must be designed so that authentication and authorization procedures cannot be bypassed and system information or files cannot be used without authorization. The system must serve only identified, authenticated and authorized users.

Requirement ID	Requirement name and description
DRO-7	The system must establish sufficient control mechanisms to ensure that system data, both during transmission and storage, are not disclosed to persons or programs that do not have the relevant authorization.
DRO-8	Access to the system data shall be ensured in accordance with the following principles: • The authorization principle shall be used, according to which everything that is not explicitly permitted is prohibited. • All actions must be checked for user authorization before execution. • Any unsuccessful authorization or authentication attempt must be automatically recorded in the audit logs. • The system shall automatically block the user account if several consecutive unsuccessful authentication attempts are made. • All actions performed by users and administrators in the system must be logged. • Any access to the system must be traceable to a specific user account or Internet Protocol (IP) address. • The system must include a notification mechanism that informs about session inactivity and session termination. • When authenticating in the system, a unique user session identifier must be created. • The system must include a control that prevents reuse of an already active session identifier to establish a new session. • Administrator access to the system must be retractable from one or more IP address ranges and Tet VPN access. • The Contractor shall ensure planned monitoring and analysis of system log content to detect incidents. • Registered user account shall be linked to a specific physical person.
DRO-9	It must be possible to create backup copies using commercially available backup tools without stopping the system.
DRO-10	The system's audit logs must include: • Information on user logins and logouts, user data selection, downloading, as well as creation, modification or deletion of a user account, recording the event time and IP address from which the action was performed. • Information on any access to the system, to ensure traceability of access to a specific user account. • System audit data - authentication data, network flow audit data, domain name system server logs, intrusion system logs, operating system authentication logs. The system's audit logs must be retained for at least 24 months after the record is made. • System audit logs must be created ensuring that the time indicated therein matches the actual coordinated universal time (UTC) of the event with 1 (one) second accuracy.
DRO-11	The Contractor shall ensure that software components used for the provision of the service are manufactured by a legal entity registered in a NATO, EU or EEA member state, or by a natural person who is a national of the Republic of Latvia, a citizen of a NATO, EU or EEA country.
DRO-12	The Contractor shall ensure that physical access to the equipment ensuring the operation of the system is permitted only to persons authorized by the institution's Contractor.
DRO-13	The Contractor is obliged to investigate, remedy and immediately inform the Contracting Authority's Contract contact person of any information technology

Requirement ID	Requirement name and description
	security incident or personal data protection breach that has direct or indirect consequences for personal data processing.

Maintenance requirements

Requirement ID	Requirement name and description
SUPPORT-1	The Tenderer must provide extended technical maintenance and support services from the manufacturer of the offered solution or an authorized partner of the manufacturer.
SUPPORT-2	Technical support services must be available: • 24 hours a day, 7 days a week, 365 days a year (24/7/365). • Incident reporting must be possible through multiple channels, including: - by telephone, - by e-mail, - in the support.
SUPPORT-3	The Tenderer must provide the following maximum response times after incident reporting: • For critical priority incidents - no later than within one hour. • For high-priority incidents - no later than within four hours. • For medium-priority incidents - no later than within eight hours.
SUPPORT-4	• Access to the manufacturer's technical support service. • Incident registration, tracking and escalation. • Problem diagnosis and remediation recommendations. • Remote technical support. • Access to software fixes, security patches, updates and the latest. supported versions. • Access to the knowledge base, technical documentation and the manufacturer's support portal. • Possible escalation of incidents to higher-level specialists of the manufacturer. • Software version updates. • Security patches and remediation of critical vulnerabilities. • Maintaining compatibility with supported platforms.