Sabiedrība ar ierobežotu atbildību "Tet"
Reģ. Nr. 40003052786
Rīga, Dzirnavu iela 105, LV-1011

Rīga, 2026. gada 7. aprīlī

Iepirkuma priekšmeta apraksts
Augstas veiktspējas suverēnas atslēgu pārvaldības sistēmas (Key Management System - KMS) iegāde drošai datu aizsardzībai multi-tenant vidē pētniecības projekta "Pilna cikla datu šifrēšanas atslēgu pārvaldības platformas risinājums datu aizsardzībai pārraidē un uzglabāšanā datu centros un mākoņvidē"

1. Iepirkuma mērķis

Iepirkuma mērķis ir iegādāties augstas veiktspējas suverēnu atslēgu pārvaldības sistēmu (Key Management System, turpmāk – KMS), kas nodrošina centralizētu kriptogrāfisko atslēgu pārvaldību un drošu vairāku neatkarīgu nomnieku apkalpošanu (multi-tenant arhitektūra).
Iepirkums tiek īstenots Pasūtītāja pētniecības projekta Nr. 1.7 "Pilna cikla datu šifrēšanas atslēgu pārvaldības platformas risinājums datu aizsardzībai pārraidē un uzglabāšanā datu centros un mākoņvidē" ietvaros. Pētniecības projekts tiek īstenots SIA "IT kompetences centrs" projektā "Informācijas un komunikācijas tehnoloģiju kompetences centrs digitalizācijai" ID Nr. 2.2.1.3.i.0/1/24/A/CFLA/006.
Iepirkums tiek organizēts saskaņā ar 28.02.2017. Ministru kabineta noteikumiem Nr. 104 „Noteikumi par iepirkuma procedūru un tās piemērošanas kārtību pasūtītāja finansētajiem projektiem", kā arī ievērojot 09.01.2024. Ministru kabineta noteikumus Nr. 32 "Latvijas Atveseļošanas un noturības mehānisma plāna 5.1. reformu un investīciju virziena "Produktivitātes paaugstināšana caur investīciju apjoma palielināšanu P&A" 5.1.1.r. reformas "Inovāciju pārvaldība un privāto P&A investīciju motivācija" 5.1.1.2.i. investīcijas "Atbalsta instruments pētniecībai un internacionalizācijai" otrās kārtas īstenošanas noteikumi".

2. Pasūtītājs

Nosaukums:	Sabiedrība ar ierobežotu atbildību "Tet"
Reģistrācijas numurs:	40003052786
Juridiskā / faktiskā adrese:	Rīga, Dzirnavu iela 105, LV-1011
Kontaktpersona:	Zanda Strautiņa, tālrunis: + 371 26358611, e-pasts: zanda.strautina@tet.lv

3. Pakalpojuma apraksts

3.1. Iepirkuma priekšmeta sastāvs:
3.2. Programmatūras licences - tiesības izmantot Pretendenta piedāvāto KMS risinājumu atbilstoši līguma noteikumiem;
3.3. Uzturēšanas un atbalsta pakalpojumi - ja tādi paredzēti Pretendenta piedāvājumā vai tehniskajā specifikācijā, tai skaitā incidentu novēršana, konsultācijas, atjauninājumi un tehniskais atbalsts;
3.4. Pakalpojuma saturs:
3.5. Izpildītājam jānodrošina risinājums, kas darbojas kā centralizēta kriptogrāfisko operāciju un atslēgu pārvaldības platforma, spēj vienlaicīgi apkalpot vairākus neatkarīgus nomniekus (multi-tenant vide), nodrošinot to pilnīgu loģisko un kriptogrāfisko izolāciju.
3.6. Izpildītājam jānodrošina sistēmas darbība lokālā Tet mākoņinfrastruktūrā bez atkarības no ārējiem pakalpojumiem, kā arī jānodrošina risinājuma integrācijas iespējas ar Pasūtītāja esošajām infrastruktūras, operētājsistēmu, datubāzu un drošības sistēmām.
3.7. Risinājumam jānodrošina kriptogrāfisko atslēgu un digitālo sertifikātu pilna dzīvescikla pārvaldības funkcionalitāte, tai skaitā piekļuves kontroles mehānismi, auditācijas un uzraudzības iespējas, kā arī sistēmas drošības prasību ievērošana, nodrošinot datu aizsardzību gan glabāšanā, gan pārraidē.
3.8. Pakalpojuma sniegšanas rezultātā Pasūtītājam jānodrošina funkcionējoša, mērogojama un droša KMS, kas atbilst tehniskajām, drošības un normatīvajām prasībām
3.9. Pakalpojuma detalizēta Tehniskā specifikācija noteikta pielikumā Nr. 3 "Tehniskā specifikācija".
3.10. Pakalpojuma sniegšanas vieta ir Latvijas Republika.
3.11. Pakalpojuma sniegšanas termiņš ir līdz 60 (sešdesmit) mēnešiem no līguma noslēgšanas dienas, tai skaitā pētniecības projekta ietvaros līdz 2027. gada 31. augustam.
3.12. Pakalpojuma pieņemšanas kārtība:

3.13. Pakalpojuma pieņemšana tiek veikta pēc risinājuma piegādes un nodošanas ekspluatācijā atbilstoši Līguma un tehniskās specifikācijas prasībām.
  3.13.1. Detalizēta Pakalpojuma pieņemšanas kārtība, tai skaitā pārbaudes procedūra, trūkumu novēršanas kārtība un termiņi, tiek noteikta Līgumā.
3.14. Pakalpojums tiek uzskatīts par pieņemtu pēc nodošanas-pieņemšanas akta abpusējas parakstīšanas.
3.15. Pretendentu atlases kritēriji
  3.15.1. Piedāvājumu tiesīgs iesniegt Pretendents, kas ir reģistrēts atbilstoši normatīvajiem aktiem un tam ir tiesības veikt komercdarbību.
  3.15.2. Pretendentam ir pieredze informācijas tehnoloģiju risinājumu piegādē un ieviešanā, kas saistīti ar datu aizsardzību, kriptogrāfiju vai atslēgu pārvaldību.
  3.15.3. Pretendentam ir pietiekami tehniskie resursi un kompetence Pakalpojuma sniegšanai atbilstoši tehniskajai specifikācijai.
  3.15.4. Pretendentam ir pieejami kvalificēti speciālisti ar atbilstošām zināšanām informācijas tehnoloģiju un informācijas drošības jomā.
  3.15.5. Pasūtītājs nedrīkst slēgt līgumu ar tādu Pretendentu, ar kuru Pasūtītājs atrodas interešu konfliktā Ministru kabineta 2017. gada 28. februāra noteikumu Nr. 104 "Noteikumi par iepirkuma procedūru un tās piemērošanas kārtību pasūtītāja finansētiem projektiem" 12. punkta izpratnē.
  3.15.6. Piedāvājumu tiesīgs iesniegt Pretendents, kas nav reģistrēts kādā no Ministru kabineta 2023. gada 27. jūnija noteikumos Nr. 333 "Zemu nodokļu vai beznodokļu valstu un teritoriju saraksts" minētajām valstīm.

4. Jautājumu iesniegšanas termiņš

4.1. Pretendentam ir tiesības uzdot jebkuru jautājumu, kas attiecas uz šo iepirkumu. Jautājumi par iepirkuma priekšmetu jānosūta iepirkumi.lv iepirkumu sistēmas sarakstes modulī. Jautājumi par iepirkumu tiek pieņemti līdz 2026. gada 14. aprīlim plkst. 12:00.
4.2. Pasūtītājs nodrošinās atbildes uz jautājumiem, ievērojot šādu kārtību:
  4.2.1. (divu) darba dienu laikā pēc jautājuma saņemšanas Pasūtītājs sagatavo atbildi un kopā ar uzdoto jautājumu publicē atbildes;
  4.2.2. jautājuma iesniedzējs netiek izpausts.

5. Piedāvājuma iesniegšanas termiņš un vieta

5.1. Saskaņā ar prasībām, kas norādītas Iepirkumu uzraudzības biroja mājas lapā (www.iub.gov.lv) publicētajā paziņojumā.
5.2. Piedāvājums iesniedzams iepirkumi.lv e-iepirkumu sistēmā līdz 2026. gada 22. aprīlim plkst. 16:00 pēc vietējā laika.

6. Prasības piedāvājuma noformēšanai

6.1. Piedāvājumu iesniedz par visu iepirkuma priekšmeta apjomu.
6.2. Piedāvājumu sagatavo latviešu valodā datorrakstā, izmantojot Pielikumā Nr. 1 pievienoto veidlapu, iekļaujot tajā visu izvērtēšanai nepieciešamo informāciju.
6.3. Piedāvājumu paraksta Pretendentu pārstāvēt tiesīga persona vai pilnvarota persona. Ja piedāvājumu paraksta pilnvarota persona, piedāvājumam pievieno Pretendenta izdotu pilnvaru.
6.4. Piedāvājumā apraksta piedāvātā pakalpojuma atbilstību visām Tehniskās specifikācijas prasībām.
6.5. Pielikumam Nr. 1 „Piedāvājuma veidlapa" norāda cenu eiro, atsevišķi norādot piedāvājuma cenu bez PVN, atsevišķi PVN un piedāvājuma kopējo summu ar PVN, ietverot visas ar Pakalpojuma sniegšanu saistītās izmaksas.
6.6. Piedāvājumu iesniedz elektroniska dokumenta formā parakstītu ar drošu elektronisko parakstu iepirkumi.lv e-iepirkumu sistēmā.
6.7. Saņemtie piedāvājumi tiks reģistrēti, atbilstoši to saņemšanas laikam. Piedāvājumi, kas saņemti pēc noteiktā termiņa, netiks vērtēti.
6.8. Pēc piedāvājuma iesniegšanas termiņa beigām Pretendents vienpusēji nevar savu piedāvājumu grozīt.
6.9. Piedāvājuma derīguma termiņš ir ne mazāks kā 60 (sešdesmit) dienas no piedāvājumu iesniegšanas brīža. Pasūtītājs ar Pretendentu var vienoties par piedāvājuma derīguma termiņa pagarināšanu.

7. Iesniedzamie dokumenti

7.1. Piedāvājums (aizpildīta pielikuma Nr. 1 „Piedāvājums" veidlapa).
7.2. Apliecinājums (aizpildīta pielikuma Nr. 2 "Apliecinājums" veidlapa).

7.3. Pretendenta pieredzes apraksts (aizpildīta pielikuma Nr. 4 veidlapa).
7.4. Informācija par Pretendenta piedāvāto risinājumu, tā atbilstību tehniskajai specifikācijai un galvenajām funkcionalitātēm.
7.5. Citi dokumenti pēc Pretendenta ieskatiem, ciktāl tie nav pretrunā ar iepirkuma dokumentāciju vai piemērojamo normatīvo aktu prasībām.

8. Piedāvājumu izvērtēšana un lēmuma pieņemšana

8.1. Pasūtītājs izsludina atklātu iepirkuma procedūru, publicējot paziņojumu par finansējuma saņēmēja iepirkuma procedūru un iepirkuma priekšmeta aprakstu Iepirkumu uzraudzības biroja mājas lapā (www.iub.gov.lv). IUB mājas lapā publicētajā paziņojumā par finansējuma saņēmēja iepirkuma procedūru noteikts sākotnējais piedāvājumu iesniegšanas termiņš.
8.2. Pēc saņemto piedāvājumu atvēršanas Pasūtītājs izvērtē tos:
  8.2.1. Piedāvājumi, kas neatbilst nolikumā noteiktām Pretendentu atlases kritērijiem, netiek tālāk izskatīti;
  8.2.2. Piedāvājumi, kuri atbilst Pretendenta atlases kritērijiem, tiek vērtēti pēc ekonomiski visizdevīgākā piedāvājuma principa, ņemot vērā piedāvājuma cenu un atbilstību tehniskajai specifikācijai.
  8.2.3. Nepieciešamības gadījumā Pasūtītājs uzsākt sarunu procedūru ar izvēlētiem Pretendentiem un lūdz Pretendentus sagatavot galīgos piedāvājumus.
8.3. Pasūtītājs no piedāvājumiem izvēlas tā Pretendenta piedāvājumu, kas Pasūtītājam ir ekonomiski visizdevīgākais un atbilst Nolikumā definētajām prasībām.
8.4. Pasūtītājs ir tiesīgs jebkurā brīdī izbeigt iepirkuma procedūru bez iepirkuma uzvarētāja noteikšanas, par to informējot pretendentus.

Tehniskā specifikācija

Sistēmas mērķis:

Iepirkuma mērķis ir iegādāties augstas veiktspējas, suverēnu atslēgu pārvaldības sistēmu (Key Management System, turpmāk - **KMS**), kas kā centrālā orķestrācijas platforma spēj vienlaikus un droši apkalpot daudzus neatkarīgus nomniekus (piemēram - struktūrvienības vai klientu organizācijas) (multi-tenant arhitektūra).

Risinājumam ir jāpiedāvā pašapkalpošanās (self-service) iespējas, ļaujot katram nomniekam patstāvīgi un autonomi definēt savas kriptogrāfijas politikas.

Sistēmai jāgarantē datu suverenitāte, novēršot piesaisti konkrētam mākoņpakalpojumu sniedzējam (vendor lock-in) un ļaujot uzticības sakni (Root of Trust) glabāt lokālā infrastruktūrā (piemēram, on-premise HSM), vienlaikus nodrošinot standartizētu saskarni dažādu publisko mākoņu un privāto infrastruktūras resursu šifrēšanai katra nomnieka vajadzībām.

Augsta Veiktspēja, Mērogojamība un Datu Aizsardzība (At-Rest un In-Transit),

Sistēmai ir jābūt spējai dinamiski mērogoties, lai apkalpotu mainīgu lietotāju - serveru, lietojumu, mikroservisu, datubāžu skaitu, nodrošinot nemainīgi zemu atbildes laiku (latency).

Sistēmai ir jāgarantē nepārtraukta un visaptveroša datu aizsardzība gan to glabāšanas fāzē (data at-rest) dažādās datubāzēs un krātuvēs, gan datu pārraides fāzē (data in-transit), automatizējot atslēgu un TLS sertifikātu pilnu dzīvesciklu.

Sistēmai ir jānodrošina katra nomnieka pilna cikla izolācija - pieprasījumu, atslēgu, konfigurācijas, lietotāja pārvaldības, garantējot, ka viena nomnieka darbības neietekmē sistēmas kopējo darbību un citu nomnieku saņemto pakalpojumu kvalitāti.

Risinājumam jānodrošina absolūta loģiskā un kriptogrāfiskā izolācija - viena nomnieka dati, atslēgas, konfigurācijas un politikas nekādos apstākļos nedrīkst būt pieejamas vai ietekmējamas no citu klientu puses.

Sistēmai jāatbalsta granulāra, lomu bāzēta piekļuves kontrole (RBAC) katra nomnieka ietvaros un jāģenerē individuāli, un savstarpēji nodalīti auditācijas žurnāli.

Jābūt iespējai katram nomniekam veikt neatkarīgu auditu un izpildīt savas normatīvās prasības (piemēram, DORA, NIS2, GDPR), vienlaikus ļaujot platformas galvenajiem administratoriem integrēt kopējos sistēmas žurnālus ar centralizētiem drošības incidentu uzraudzības (SIEM) risinājumiem.

Kriptogrāfiskās elastības (Crypto Agility) un pēckvantu kriptogrāfijas (PQC) gatavība
Sistēmas arhitektūrā ir jābūt iestrādātiem kriptogrāfiskās elastības (crypto agility) principiem. Ņemot vērā kvantu skaitļošanas attīstību un tās radītos draudus klasiskajiem asimetriskajiem šifrēšanas algoritmiem, KMS risinājumam ir jābūt proaktīvi sagatavotam pēckvantu kriptogrāfijas (Post-Quantum Cryptography - PQC) ieviešanai. Tas nozīmē sistēmas spēju bez arhitektūras pārbūves vai pakalpojumu dīkstāves dinamiski atjaunināt, integrēt un pārvaldīt jaunos, standartizētos (piemēram, NIST apstiprinātos) kvantu drošos un hibrīdos algoritmus. Daudznomnieku vides (multi-tenant) kontekstā platformai jānodrošina elastība, kas ļauj katram nomniekam neatkarīgi un pakāpeniski migrēt savas šifrēšanas politikas, atslēgas un sertifikātus uz PQC standartiem.

Sistēmas vispārējās tehniskās prasības

Prasības ID	Prasības nosaukums un apraksts
Cloud-1	Visiem sistēmas darbībai, konfigurēšanai un uzturēšanai nepieciešamajiem komponentiem — tostarp vadības plaknei (*Control Plane*), pārvaldības plaknei (*Management Plane*), kā arī pašai kriptogrāfisko operāciju datu plaknei (*Data/Crypto Plane*) un auditācijas moduļiem — ir jābūt izvietojamiem un autonomi darbināmiem lokāli Tet mākoņinfrastruktūrā.
Cloud-2	Sistēmai jāspēj pilnvērtīgi funkcionēt šajā lokālajā vidē (Tet mākonī) bez jebkādas nepieciešamības sazināties ar izstrādātāja vai citu trešo pušu ārējiem (SaaS/PaaS) servisiem. Tas attiecas uz telemetriju, licencēšanas validāciju, atjauninājumu pārbaudi, atslēgu rezerves kopēšanu un jebkādām citām administrēšanas vai vadības funkcijām.
Cloud-3	Risinājumam ir tehniski jāatbalsta izvietošana uz suverēna mākoņa piedāvāto platformu (VMWare Cloud Director 8+. Ražotājam ir jānodrošina platformas atbalsts).
Cloud-4	Sistēmā ir jābūt iekļautai rezerves kopiju (backup & restore) veidošanas funkcionalitātei vai arī jānodrošina atbalsts rezerves kopiju veidošana un atjaunošanai VMWare hypervisor. līmenī.

Funkcionālās prasība: Pārvaldība

Prasības ID	Prasības nosaukums un apraksts
Admin-1	Sistēmai jānodrošina decentralizēts pārvaldības modelis, piedāvājot katram nomniekam (tenant) drošu un izolētu pašapkalpošanās portālu (GUI). Nomnieka lokālajiem administratoriem jāspēj patstāvīgi veikt pilnu kriptogrāfisko aktīvu dzīvescikla pārvaldību — ģenerēt, importēt, rotēt un atsaukt šifrēšanas atslēgas. Papildus jānodrošina iespēja nomniekiem pašiem definēt un pielāgot stingras kriptogrāfijas politikas, piemēram, apstiprinātos algoritmus, atslēgu derīguma termiņus, rotācijas grafikus un specifiskus lomu bāzētas piekļuves (RBAC) noteikumus savu resursu ietvaros. Nomniekam jāvar visas risinājuma lietošanai nepieciešamās darbības veikt bez platformas administratora iesaistes.
Admin-2	Risinājumam jābūt pilnībā automatizējamam. Visām sistēmas funkcijām un iespējām, kas ir pieejamas grafiskajā lietotāja saskarnē (GUI), jābūt sasniedzamām un pārvaldāmām caur moderniem, drošiem un labi dokumentētiem API galapunktiem. Tas ietver gan administratīvās darbības (*Management Plane*), piemēram, nomnieku izveidi un politiku piešķiršanu, gan operacionālās darbības (*Data Plane*), piemēram, datu šifrēšanu, atšifrēšanu un parakstīšanu.
Admin-3	KMS platformai jānodrošina izstrādātāju rīku komplekti (SDK) vairākām programmēšanas valodām (piemēram, Java, Python, .NET).
Admin-4	Platformai ir jāietver iebūvēti instrumenti reāllaika telemetrijas un veiktspējas uzraudzībai. Sistēmai automātiski jāapkopo detalizēta metrika par kriptogrāfisko operāciju intensitāti (piemēram, operācijas sekundē - TPS), atslēgu izmantošanas biežumu, latentumu un kļūdu rādītājiem. Ievērojot izolācijas principu, katram nomniekam jābūt redzamai tikai savas vides statistikai.

Funkcionālās prasības: Integrācija

Prasības ID	Prasības nosaukums un apraksts
INTEGR-1	Sistēmai jānodrošina pilnvērtīgs atbalsts KMIP (Key Management Interoperability Protocol) standartam (versijas 1.2 līdz 2.x/3.x).
INTEGR-2	Sistēmai jānodrošina standarta (out-of-the-box) savietojamība ar izplatītākajiem virtualizācijas hipervizoriem, vismaz VMware vSphere

Prasības ID	Prasības nosaukums un apraksts
	(atbalstot vCenter Server integrāciju, VM un vSAN datu šifrēšanu), un Microsoft Hyper-V (atbalstot *Shielded VMs* jeb aizsargāto virtuālo mašīnu arhitektūru) atbalstu. KMS ir jāspēj automātiski, izmantojot KMIP, izsniegt atslēgas virtuālo mašīnu disku šifrēšanai miera stāvoklī (at-rest).
INTEGR-3	KMS platformai jāspēj kalpot kā ārējam atslēgu pārvaldniekam (External Key Manager) un jāintegrējas ar izplatītāko disku masīvu (SAN/NAS) ražotāju aparatūru (piemēram, NetApp, Dell EMC, HPE, Pure Storage u.c.). Sistēmai jāpārvalda aparatūras līmeņa paššifrējošo disku (SED - Self-Encrypting Drives) un krātuvju kontrolleru autentifikācijas un šifrēšanas atslēgas, nodrošinot datu nesēju drošību to fiziskas zādzības vai norakstīšanas gadījumā.
INTEGR-4	Sistēmai ir jānodrošina integrācijas iespējas ar standarta izmantoto operētājsistēmu natīvajiem kriptogrāfijas kontekstiem. • Microsoft Windows: Integrācija izmantojot Windows CNG (Cryptography Next Generation) API un/vai EKM (Extensible Key Management). • Linux (RHEL un Ubuntu saimes): Atbalsts standarta PKCS#11 moduļiem un OpenSSL interfeisiem, kā arī spēja orķestrēt atslēgas operētājsistēmas disku šifrēšanai (LUKS - Linux Unified Key Setup).
INTEGR-5	Sistēmai ir jānodrošina integrācijas iespējas ar standarta starpprogrammatūru un datubāžu vadības sistēmām (DBMS), lai nodrošinātu šifrēšanu lietotņu vai datu bāzes līmenī. Sistēmai jāatbalsta: • Datubāzes: Integrācija caur TDE (Transparent Data Encryption) tehnoloģiju ar izplatītākajām datubāžu sistēmām (piemēram - Microsoft SQL Server, Oracle Database, MySQL, PostgreSQL u.c.) • Web / Aplikāciju serveri: Integrācija ar tīmekļa serveriem (piemēram, NGINX, Apache HTTP Server) un Java aplikāciju serveriem (Apache Tomcat, Red Hat JBoss/WildFly), lai droši glabātu un izgūtu TLS sesiju privātās atslēgas ārpus servera failu sistēmas.
INTEGR-6	Sistēmai jānodrošina integrācijas iespējas ar esošo publiskās atslēgas infrastruktūru (PKI). Obligāta ir spēja integrēties ar Microsoft Windows Active Directory Certificate Services (MS AD CS), kā arī citām izplatītām CA sistēmām. KMS ir droši jāģenerē asimetrisko atslēgu pāri savā aizsargātajā perimetrā un jāorķestrē X.509 sertifikātu pieprasīšanas (CSR), izsniegšanas, atjaunošanas un atsaukšanas (CRL/OCSP) procesi, izmantojot standarta protokolus (piem., SCEP, EST, CMP vai REST API

Lietotāju autentifikācija un lomas

Prasības ID	Prasības nosaukums un apraksts
IAM-1	Sistēmai jānodrošina pilnībā atdalīta, autonoma autorizācijas un piekļuves kontroles arhitektūra katram nomniekam (tenant). Piekļuves tiesību un autorizācijas noteikumu apstrādei jābūt loģiski izolētai, garantējot, ka viena nomnieka lietotāju tiesības, grupas vai piekļuves līmeņi nekādos apstākļos nepārklājas ar citu nomnieku vidēm vai nevar tās ietekmēt.
IAM-2	Risinājumam jāatbalsta iespēja gan platformas globālajiem administratoriem, gan katram nomniekam individuāli konfigurēt un pieslēgt savus neatkarīgos ārējos identitātes pakalpojumu sniedzējus (Identity Providers - IdP). Integrācijas nodrošināšanai sistēmai standartā jāatbalsta vismaz SAML 2.0 un OpenID Connect (OIDC) protokoli, ļaujot izmantot organizāciju esošos autentifikācijas risinājumus.

Prasības ID	Prasības nosaukums un apraksts
IAM-3	Sistēmai jānodrošina funkcionalitāte, kas ļauj katram nomniekam savas izolētās vides ietvaros veidot, modificēt un administrēt pielāgotas piekļuves lomas (Role-Based Access Control - RBAC), tādējādi garantējot stingru pienākumu sadales (Segregation of Duties) principu ievērošanu. Kritisku sistēmas, konfigurācijas vai kriptogrāfisko operāciju (piemēram, atslēgu iznīcināšana) veikšanai platformai jāatbalsta "četru acu principa" (Quorum / Multi-party authorization) realizācijas iespēja, sistēmiski pieprasot vismaz divu neatkarīgu, attiecīgi pilnvarotu lietotāju apstiprinājumu.
IAM-4	Sistēmai jānodrošina iespēja katram nomniekam izveidot un uzturēt neatkarīgus, sistēmā iebūvētus lokālos lietotāju kontus. Nomniekiem jābūt tiesībām pašiem definēt un pārvaldīt lokālo kontu paroļu drošības politikas, tostarp paroļu sarežģītības prasības, derīguma termiņus, kā arī maiņas un rotācijas nosacījumus. Visiem lokālajiem kontiem sistēmai obligāti jānodrošina daudzfaktoru autentifikācijas (MFA) funkcionalitāte ar iespēju to definēt kā obligātu prasību piekļuvei.
IAM-5	Sistēmai automātiski jāģenerē nemaināmi auditācijas pieraksti, kas ir stingri atdalīti katram nomniekam. Katram nomniekam jāspēj definēt pielāgotu auditācijas žurnālu glabāšanas politiku (retention period) savā vidē. Papildus risinājumam jānodrošina iebūvēta iespēja pārsūtīt auditācijas pierakstus drošā veidā uz ārējiem, centralizētiem žurnālu glabāšanas risinājumiem vai SIEM (Security Information and Event Management) platformām, atbalstot standarta protokolus un formātus (piemēram, Syslog, CEF formāts).

Kriptogrāfijas standarta prasības

Prasības ID	Prasības nosaukums un apraksts
Crypto-1	Sistēmai jānodrošina stingra kriptogrāfisko atslēgu loģiskā un fiziskā izolācija starp dažādiem platformas nomniekiem (tenants). Daudznomnieku (multi-tenant) arhitektūras ietvaros risinājumam jāatbalsta integrācija ar Aparatūras drošības moduļiem (HSM), ļaujot katram nomniekam piesaistīt atsevišķu, neatkarīgu HSM partīciju (slotu).
Crypto-2	Sistēmai jāpiedāvā elastīgas atslēgu glabāšanas un aizsardzības iespējas atkarībā no katra nomnieka drošības politikas un veiktspējas prasībām. Jānodrošina iespēja atslēgas droši glabāt programmatūras līmenī (piemēram, šifrētā lokālā datubāzē), kā arī piedāvāt augstākās drošības opciju – atslēgu glabāšanu un operāciju apstrādi tieši sasaistīt ar HSM iekārtu (HSM-backed key storage).
Crypto-3	Sistēmai jānodrošina pilnvērtīga, automatizēta X.509 digitālo sertifikātu dzīvescikla orķestrācija. Sistēmai jāspēj centralizēti pārvaldīt sertifikātu pieprasīšanu (CSR), ģenerēšanu, izsniegšanu, atjaunošanu (rotāciju) un atsaukšanu (revocation), izmantojot atzītus standartus (piemēram, SCEP, EST, ACME vai REST API integrācijas).
Crypto-4	Platformas galvenajai drošības arhitektūrai ir jābūt balstītai uz uzticības sakni (Hardware Root-of-Trust). Visām sistēmas galvenajām atslēgām (Master Keys jeb Key Encryption Keys), kas tiek izmantotas zemāka līmeņa datu atslēgu (DEK) šifrēšanai un aizsardzībai, jābūt ģenerētām un nepārtraukti glabātām drošā veidā.
Crypto-5	Sistēmai jānodrošina tehnoloģiska atslēgu rezidences politiku uzspiešana (Key Residency Enforcement). Risinājumam jāļauj administratoriem definēt noteikumus, kas garantē, ka noteiktu nomnieku atslēgas var tikt ģeogrāfiski vai

Prasības ID	Prasības nosaukums un apraksts
	loģiski ierobežotas (piemēram, tās drīkst atrasties konkrētā fiziskā HSM iekārtā), sistēmiski bloķējot jebkādus mēģinājumus tās eksportēt, klonēt vai sinhronizēt ārpus atļautā perimetra.
Crypto-6	Sistēmai ir jāparedz izmantoto kriptogrāfijas algoritmu ilgtspēja (Crypto Agility), lai nodrošinātu gatavību kvantu skaitļošanas radītajiem draudiem asimetriskajai kriptogrāfijai. Ir jāparedz tehnisks atbalsts ASV Nacionālā standartu un tehnoloģiju institūta (NIST) apstiprinātajiem pēckvantu kriptogrāfijas (PQC) algoritmiem (piemēram, ML-KEM, ML-DSA). Sistēmai jānodrošina iespēja izmantot hibrīdo šifrēšanu (vienlaikus apvienojot klasiskos, piem., RSA/ECC, un PQC algoritmus), lai nodrošinātu drošu un standartiem atbilstošu pārejas procesu.

Vispārējās drošības prasības

Prasības ID	Prasības nosaukums un apraksts
DRO-1	Programmatūras izstrādes process tiek veidots atbilstoši ISO/IEC 27034 standarta vadlīnijām.
DRO-2	Datu aizsardzība dažādos pielietojuma slāņos jāveido, izmantojot dažādus aizsardzības mehānismus.
DRO-3	Informācijai un datiem sistēmā nedrīkst piekļūt, apejot programmatūras drošības kontroles, piemēram, operētājsistēmas, failu sistēmas vai datu bāzes līmenī.
DRO-4	Sistēmas izstrādē un ieviešanā nedrīkst izmantot komponentes, kuras ražotājs pozicionē kā “Obsolete”, programmatūra, kurai nav plānots “end-of-life” tuvāko 2 (divu) gadu laikā vai kādā citā veidā nerekomendē izmantošanai ražošanas sistēmās.
DRO-5	Izpildītājam pēc Pasūtītāja pieprasījuma jāsniedz apraksts, kādā veidā tiks nodrošinātas Sistēmas atbilstības drošības prasībām.
DRO-6	Apakšsistēmu piekļuvei jābūt izveidotai tā, lai nevarētu apiet autentifikācijas un autorizācijas procedūras, un nesankcionēti lietot Sistēmas informāciju vai datnes. Sistēmai jāapkalpo tikai identificētus, autentificētus un autorizētus lietotājus.
DRO-7	Sistēmai jāizveido pietiekami kontroles mehānismi, lai nodrošinātu, ka Sistēmas dati gan to pārraides, gan glabāšanas laikā netiek atklāti personām vai programmām, kurām nav attiecīgās autorizācijas.
DRO-8	Piekļuve Sistēmas datiem nodrošināma, ievērojot sekojošus principus: • Jāizmanto autorizācijas princips, saskaņā ar kuru viss, kas nav tiešā veidā atļauts, ir aizliegts; • Visām darbībām pirms to izpildes jāpārbauda lietotāja autorizācija darbības izpildei; • Jebkurš nesekmīgs autorizācijas vai autentifikācijas mēģinājums automātiski jāreģistrē auditācijas pierakstos; • Sistēmai jāveic lietotāja konta automātiska bloķēšana, ja tiek izdarīti pēc kārtas vairāki pēc kārtas izdarīti nesekmīgi autentifikācijas mēģinājumi; • Sistēmā visām lietotāju un administratoru veiktajām darbībām jābūt fiksētām žurnālfailos; • Jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;

Prasības ID	Prasības nosaukums un apraksts
	• Sistēmai ir jāietver paziņojumu sniegšanas mehānisms, kas informē par tā darba sesijas neaktivitāti un sesijas pārtraukšanu; • Jānodrošina, ka, autentificējoties Sistēmā, tiek izveidots unikāls lietotāja sesijas identifikators; • Sistēmā ir jābūt ietvertai kontrolei, kas liedz atkārtoti izmantot jau aktīvu izveidotu sesijas identifikatoru jaunas sesijas izveides nodrošināšanai; • Administratoru pieeju Sistēmai jāspēj ierobežot no viena vai vairākiem IP adrešu apgabaliem un Tet VPN piekļuves; • Izpildītājs nodrošina sistēmas pierakstu satura plānveida uzraudzību un analīzi, lai konstatētu incidentus; • Katrs reģistrēta lietotāja konts ir saistīts ar konkrētu fizisko personu.
DRO-9	Jānodrošina iespēja veikt rezerves datu kopiju veidošanu, izmantojot tirgū pieejamos rezerves kopēšanas rīkus bez Sistēmas apturēšanas.
DRO-10	Sistēmas auditācijas pierakstos jāietver: • Informācija par lietotāja pieslēgšanos un atslēgšanos, lietotāja veikto datu atlasi, lejupielādi, kā arī lietotāja konta izveidi, grozīšanu vai dzēšanu, fiksējot notikuma laiku un IP adresi, no kuras veikta darbība; • Informācija par jebkuru piekļuvi sistēmai, lai nodrošinātu piekļuves izsekošanu līdz konkrētam sistēmas lietotāja kontam; • Sistēmas auditācijas datus – autentifikācijas datus, tīkla plūsmas auditācijas datus, domēna vārdu sistēmas servera pierakstus, ielaušanās sistēmas pierakstus, operētājsistēmas autentifikācijas pierakstus. Sistēmas auditācijas pierakstiem jānodrošina uzglabāšana vismaz 24 mēnešus pēc ieraksta izdarīšanas; • Sistēmas auditācijas pieraksti jāveido nodrošinot, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar 1 (vienas) sekundes precizitāti.
DRO-11	Izpildītājs nodrošina, ka pakalpojuma nodrošināšanai izmanto programmatūras komponentes, kuru ražotājs ir juridiska persona, kas reģistrēta NATO, ES vai EEZ dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas valsts piederīgais, NATO, ES vai EEZ valstu pilsonis.
DRO-12	Izpildītājs nodrošina, ka fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes Izpildītāja pilnvarotām personām.
DRO-13	Izpildītājam ir pienākums izmeklēt, novērst un nekavējoties informēt Pasūtītāja Līguma kontaktpersonu par jebkuru informācijas tehnoloģijas drošības incidenta gadījumu vai personas datu aizsardzības pārkāpumu, kam ir tiešas vai netiešas sekas uz personas datu apstrādi.

1. Uzturēšanas prasības

Prasības ID	Prasības nosaukums un apraksts
SUPPORT-1	Pretendentam jānodrošina piedāvātā risinājuma ražotāja vai ražotāja autorizēta partnera paplašinātas tehniskās uzturēšanas un atbalsta pakalpojums
SUPPORT-2	Tehniskā atbalsta pakalpojumam jābūt pieejamam: • 24 stundas diennaktī, 7 dienas nedēļā, 365 dienas gadā (24/7/365); • incidentu pieteikšana jānodrošina pa vairākiem kanāliem, tai skaitā: • pa tālruni, • e-pastā • atbalsta portālā

Prasības ID	Prasības nosaukums un apraksts
SUPPORT-3	Pretendentam jānodrošina šādi maksimālie reakcijas laiki pēc incidenta pieteikšanas: • Kristiskas prioritātes incidentiem - ne vēlāk kā vienas stundas laikā. • Augstas prioritātes incidentiem - ne vēlāk kā četru stundu laikā. • Vidējas prioritātes incidentiem - ne vēlāk kā astoņu stundu laikā
SUPPORT-4	• piekļuvei ražotāja tehniskā atbalsta dienestam; • incidentu reģistrēšanai, uzskaitei un eskalācijai; • problēmu diagnostikai un novēršanas rekomendācijām; • attālinātam tehniskajam atbalstam; • piekļuvei programmatūras labojumiem, drošības ielāpiem, atjauninājumiem un jaunākajām uzturētajām versijām; • piekļuvei zināšanu bāzei, tehniskajai dokumentācijai un ražotāja atbalsta portālam; • iespējamai incidentu eskalācijai uz ražotāja augstāka līmeņa speciālistiem. • Programmatūras versiju atjauninājumiem. • Drošības ielāpiem un kritisko ievainojamību novēršanai. • Savietojamības uzturēšana ar atbalstītajām platformām