Questions RFP-2026-007 - Certificate life cycle management solution

1. How many environments are required? (Prod, DR, Dev, Test)

Production, qualification, test

2. How many Active Directory Forests does UPU have, and how many of them are needed for certificate management?

out of the scope

3. Is Auto-enrollment to network devices a requirement (SCEP Protocol)?

No, ACME is the requirement

4. Do you need CA that can issue PQC Certificates?

No

5. Do you need deployment to be done on-site or remotely?

On-site or remotely -- both options are accepted

6. Can you please elaborate on this requirement? "Support for up to 40 SSL certificates (wildcard and standard) and potential future expansion"

That's the current volume of SSL certificates being used

7. Can you please elaborate on this requirement? "Centralized policy enforcement for: approved CAs, key sizes and algorithms, certificate validity periods" - Do you need to view a compliancy report/dashboard, use predefined external CA Cert profile, or need Entrust to help with CP/CPS?

Ability to centrally define key sizes, algorithms and validity periods per defined profiles

8. the total number of SSL/TLS certificates across all CAs, or
9. only public SSL/TLS certificates, with private/internal certificates excluded from this count?

Public SSL/TLS certificates.

10. How many certificates do you have from DigiCert and Sectigo?

~40 in total

11. Would you consider moving to Sectigo to consolidate your CLM and certificates with a single vendor?

No considerations for the time being

12. Can UPU provide an estimated number or range of private/internal certificates currently in use or expected during the contract term?

Up to 10.

13. Does UPU anticipate material growth in certificate volumes over the four-year contract period (e.g. due to automation, cloud expansion, or shorter certificate lifetimes)?

Consider 10% increase.

14. Please confirm current and projected volumes for the following certificate categories:

Public trusted certificates: ~40
Private TLS certificates: ~10
User certificates (if applicable): N/A
Device certificates (if applicable): N/A

15. Should bidders assume that other certificate types (e.g. internal service certificates, client authentication certificates) are:

supported but not required at this stage? X

16. Does UPU expect ACME to be used primarily for public certificates (e.g. Sectigo, digicert), or also for internal/private CA issuance?

At this stage we are targeting public certificates only.

17. Can UPU confirm whether hosting within the EU (outside Switzerland) with appropriate data protection controls would be acceptable?

Affirmative.

18. Do you need any ITSM, SIEM integration?

If you could support Splunk or any syslog collector, that'd be sufficient.

19. Does UPU have a preference between on-premises, cloud-based (SaaS), or hybrid deployment models, or will all compliant options be evaluated equally?

All three options will be evaluated equally.

20. Please confirm the current private CA in use (e.g., Microsoft AD CS, EJBCA), including hosting model and scope of usage.

Microsoft AD CS (on-premise) used for internal web server certificates.

21. Please confirm the current public CA provider(s) and existing certificate procurement/management model.

Digicert and Sectigo

22. Is there an objective to consolidate public certificates under a single CA, or should the solution assume a multi-CA operating model?

There are no objectives nor restrictions to consolidate, however, at this stage we'd request to support a multi-CA operating model.

23. Please confirm which integrations and platforms are explicitly in scope (e.g., web servers, load balancers, cloud platforms, security devices).

Primarily on-premise F5 load balancers, on-premise web servers (IIS, Apache) and Azure Web Application Gateways.

24. Is end-to-end automation required, including automatic installation and renewal on target systems (web servers, load balancers, devices)?

Yes

25. If end-to-end automation is required, please confirm the primary platforms and technologies involved and main usecases (e.g., IIS, Apache, NGINX, F5, Citrix, Kubernetes).

Primarily on-premise F5 load balancers and on-premise web servers (IIS, Apache)

26. Can UPU provide guidance on expected support? We offer standard, enhanced and premier support.

Standard support would be sufficient, however, please make sure to include some days for the initial implementation phase as per 4.1.3 Technical requirements.

27. Does UPU anticipate regular on-site presence in Berne? (Our SCM is a cloud-based SaaS solution that can be implemented in just a few online sessions.)

Not required, therefore, online/remote sessions would be sufficient.

28. Can UPU clarify how 'quality of partnerships with security suppliers' will be evaluated?

This is applicable to vendors reselling products through the partnership channels, hence the quality of the partnership will be assessed (Gold/Platinum/etc).

29. Do you have specific constraints regarding the UPU data residency in case of a cloud solution not hosted in Switzerland, for instance in case of hosting in the EU ?

It's okay. Please specify exact location where UPU data will be stored.

30. Could you please provide the exhaustive list of load balancers, network devices, and applications that must be covered by the certificate discovery and inventory?

We can't provide detailed inventory at this stage, but the total amount of devices is up to 50.

31. Could you please provide more details on the expected integrations with AWS and Azure Key Vault (AKV) in order to enable us to deliver the most detailed and relevantresponse?

We expect integrations with the AWS/Azure Web Application Gateways where the publicly exposed SSL certificates are automatically renewed.

32. What IT Service Management (ITSM) solution is used internally, and with which the CLM must integrate?

EasyVista

33. How many internal certificates are currently managed by your Microsoft ADCS private PKI?

Up to 10.

34. What are the associated use cases and integrations? We understand that this specific point is outside the initial scope of the consultation; however, our CLM is designed to act as a federation layer for workflows and capabilities across both private and public certificates.

Automatic renewal of the SSL certificate used in the IIS.

35. Which technology or provider currently supports your public DNS infrastructure

Authoritative DNS servers are hosted and managed by UPU.

36. What types of public certificates do you issue (e.g., DV, OV, EV)?

OV

37. What integration is expected with Delinea?

For example, storing of the export password during the PFX generation.

38. What integration is expected between the CLM and your Thales Luna network

HSMs? Is it a Data at Rest scenario mentioned in section 4.1.3?

Storing of the private key during the Certificate Signing Request generation.

39. Is the list of vendors mentioned in section 4.1.3 exhaustive for both discovery and public certificate automation/deployment?

Affirmative

40. How many distinct top domains are currently registered with your public CAs (DigiCert and Sectigo) to enable domain control validation (DCV) and certificate enrollment?

Up to 20.

41. How many non-SSL/TLS certificates should be actively managed by the solution (i.e., certificates deployed on endpoints such as VPN-devices, mobile devices and workstations)?

This is out of the scope at this stage.

42. Is 40 SSL certificates an accurate reflection of the total known certificate estate, or does it represent only the certificates currently visible and managed, with a potentially much larger undiscovered population sitting across servers, load balancers, and applications that a discovery exercise would surface?
    Specifically, what is the anticipated volume for Public versus Private certificates today and for the next 4 years?

40 is an accurate reflection of public certificates.

The volume of private certificates is ~10.

We expect ~10% of increase of certificate volumes per year.

43. Is the HSM already deployed and operational, and is it accessible from the network location where the CLM platform will be hosted, or does the HSM connectivity need to be designed and established as part of this engagement?

Already setup and operational.

44. Is the expectation that certificates provisioned through the CLM platform will have their private laws automatically vaulted into Delinea as part of the issuance workflow?

We plan to use Delinea to store PFX export passwords (if required).

45. Stakeholder wise, are F5 instances managed centrally, or are they administered independently per country or region? If managed separately, how many stakeholders approximately would be in scope?

All F5 instances are managed centrally with ~10 IT operations admins.

46. Regarding Microsoft CA as the internal PKI, is there a single enterprise CA hierarchy serving the entire organisation, or do individual countries or regions operate their own subordinate or standalone CAs that would each need to be individually onboarded into the CLM platform?

Single enterprise CA

47. Are certificates on Exchange and ADFS currently renewed manually and on an ad hoc basis, and have there been any recent expiry-related incidents on either platform that are driving urgency here?

Exchange and ADFS certificates are renewed manually and, on an ad, -hoc basis.

The driving urgency here is the lifetime reduce of certificates, which will make the manual process very time consuming.

48. Is the organization currently using Let's Encrypt or any ACME-based issuance anywhere in the estate, or is ACME support a forward-looking requirement to enable future automation, and if the latter, are there firewall or network policies that would currently block outbound ACME challenge traffic?

We are not using Let's Encrypt or any ACME-based issuance at the moment, however, this is a forward-looking requirement. Firewall or network policies will be adjusted accordingly.

49. Are you considering the requirement for ACME challenge types (HTTP-01 and DNS-01) as mandatory?

Yes

50. Is there a known, maintained mapping of which team or individual owns each certificate, or is establishing that ownership registry expected to be part of the implementation work?

The mapping is known

51. Who currently controls DNS for the organisation's domains, is it centralised or delegated per country?

It's is centralized, hosted and maintained by UPU

52. Is there an API-accessible DNS platform that would allow automated DNS record creation during certificate issuance?

Not at the moment but to be configured

53. Is there an existing ITSM platform in use for alert integration

Yes, EasyVista

54. Is the ITSM platform consistent across all 50 countries or are there regional variations in ticketing systems that the CLM alerting would need to accommodate?

ITSM platform is consistent

55. Is the expectation that certificate requests always follow an automated straight-through process, or are there specific certificate types, CAs, or environments where a human approval step is mandatory before issuance?

The scope of this RFP is HQ only, therefore, full automation is required

56. Are workloads running in these platforms using cloud-native certificate services today such as AWS Certificate Manager or Azure Key Vault certificates, and if so, is the intent to replace those with CLM-managed certificates or to bring them under visibility only?

The AWS and Azure workloads currently use certificates that are renewed manually, hence the intent is to replace them with CLM-managed certificates

57. What does the organization consider the minimum viable outcome for the initial implementation phase — is it full automation across all 40 certificates, or is establishing inventory, monitoring, and alerting considered sufficient for an initial go-live with automation to follow in a subsequent phase?

Automation across the vast majority of certificates would be considered as the minimum viable outcome

58. Do you see the primary value of this engagement as reducing operational risk through automation, or is audit readiness and compliance reporting the more immediate driver?

The primary value is reducing operational risk through automation

59. For a SaaS offering, would hosting the service and data within the Frankfurt or Amsterdam regions meet your primary data residency and compliance requirements?

Yes

60. Would the integration of Kubernetes support be a point of interest or a strategic priority for your team’s deployment roadmap?

Not at this stage

61. Could you please specify, what is the total number of certificates issued by your CAs and intended to be managed?

User/device certificates are out of the scope of this RFP and there is no use case that could be associated for the time being. You can include 350 user certificates (based on total number of staff members) in your offer, but please note that it won’t assessed nor considered during the evaluation.

62. What types of certificates are required? (TLS or S/MIME only? Code Signing? Others?)

SSL/TLS server certificates only

63. Which types of systems require certificate lifecycle management? (e.g., IIS Servers, Linux Web Servers, F5, Azure, etc.)

All mentioned systems would require certificate lifecycle management

64. Do you expect the solution to be QuantumSafe (PQC ready)? Do you expect the solution to be used for migration from legacy to Quantum Safe certificates ?

Not at the moment

65. What Operating Systems should we collect information from ?

Windows 2016-2025, Linux Debian 12/13

66. What type and brand of Load Balancer should we collect information from?

F5 BIG-IP, F5 Distributed Cloud (XC), Azure Application Gateway

67. What type and brand of Network devices should we collect information from?

N/A

68. What type of applications should we collect information from? If possible precise what proportion would be accessible via API.

IIS, Apache Tomcat, Microsoft Exchange, Microsoft ADFS

69. Confirm this concerns only the same ecosystem as for Certificate Discovery ?

Confirmed

70. RBAC : what types of role / segregation do you expect ?

IT operations (all actions), Finance/admin (read-only for inventory), Audit (read-only)

71. Approval workflow : do you expect approval workflow even for automated certificate lifecycle ? Initial request only ? Other ? Do you expect multiple approval steps for a workflow ?

Considering our low volume no approval workflows are expected.

72. What ITSM do you use? Do you confirm you expect automatic ticket creation in case of alert ?

EasyVista. Confirmed.

73. Regarding compliance report, can you confirm against what referential should the compliance report be generated ? (internal, ISO, PCI, others…)

Internal (primarily for inventory and audit)

74. Integration with Delinea: can you precise to what purpose ? Secure storage of what information ?

Storing of PFX export/import passwords.

75. Integration with HSM : can you precise if you intend to store all private keys in HSM (CA certificates, leaf certificates) or only a subset ? If a subset, can you precise?

Storing of private keys during CSR generation.

76. What is the number of certificates (volumes) you would like to manage?

40 public TLS/SSL certificates, and ~10 private TLS/SSL certificates

77. Do you want a payment upfront or yearly payment?

We prefer annual payments for the budget allocation

78. Please confirm that the supplier will not be required to be physically on-premises if successful in the RFP. This is not something we can offer.

Remote presence is fine.

79. Under 3.8, it notes that the UPU General Terms and Conditions for Provision of Services is attached for reference - we have not received this. Please can you send it to us?

https://www.upu.int/en/universal-postal-union/procurement#reference-documents

80. Under CA Support, what does "bring your own CA" mean? What is technically necessary to comply to this?

It's a generic model where we can use our own Certificate Authority (CA) if necessary. For example, on-premise Microsoft Active Directory Certificate Services.

81. How many automation / certificate management seats will be required per year? A seat is consumed per each unique endpoint / IP address a certificate is on and will require automation. Our pricing and quote depend heavily on this quantitative figure. Example: A seat is consumed for each active endpoint being managed. Each endpoint consists of a unique combination of an FQDN + IP address. Example: a load balancer with 1 FQDN but 10 different IP addresses = 10 seats.

We heavily use wildcard certificates, how are seats calculated in such case?

82. When a Certificate Authority (CA) issues certificates, the CA's signing keys are protected by an HSM such as Entrust & Thales Network HSM. The issued end-entity certificates themselves are delivered to the requesting client or published to configured destinations (e.g., web servers, load balancers, key vaults) and managed through the CLM platform. The HSM integration is therefore typically handled at the CA/PKI layer rather than the CLM layer.

Based on the above, kindly describe the approach you would like to take for this."Our plan was to store certificate keys on HSM during the CSR generation.

83. Secrets managers/PAM solutions like Delinea Secret Server can integrate with certificate management platforms as an identity provider for user authentication via protocols such as OpenID Connect (OIDC) or LDAP.

To ensure we align with your requirements, could you please describe the outcome you are looking to achieve from this integration?" Our plan was to store PFX export/import password on Delinea Secret Server

84. Certificate lifecycle management (CLM) platforms can operate in two modes: managing certificates issued by existing external CAs (such as DigiCert, Sectigo, or Microsoft AD CS) through CA connectors, or providing a built-in private CA to issue certificates directly. A 'Bring Your Own CA' capability typically refers to connecting the CLM platform with your organization's existing CA infrastructure rather than deploying a new one.
Could you please clarify which of the above best aligns with your objective?

The first assumption, managing certificates issued by existing external CAs (such as DigiCert, Sectigo, or Microsoft AD CS), is accurate.

85. Post-quantum cryptography (PQC) is an emerging area of cryptographic security designed to protect against the threat of quantum computers being able to break traditional encryption algorithms such as RSA and ECC, which underpin today's certificate infrastructure. This is often referred to as the 'harvest now, decrypt later' threat, where adversaries collect encrypted data today with the intent of decrypting it once quantum computing matures. The Entrust

Cryptographic Security Platform Certificate Authority already supports PQC algorithms such as ML-DSA, along with dashboard visibility into post-quantum readiness across your certificate inventory.

Would you like to explore PQC readiness as part of the scope of this engagement or in a future phase?"
Could be in a future phase.

86. Certificate lifecycle management platforms are designed to manage all certificates across an organization's environment — including publicly trusted SSL/TLS certificates (wildcard and standard), private-trust certificates used internally, and certificates discovered across servers, load balancers, and cloud platforms. Organizations often have more certificates in active use than initially accounted for, particularly across multiple domains, subdomains, and cloud-hosted services.
    Could you please describe the scope of certificates you intend to manage - including the total number of public SSL/TLS certificates currently in use across all domains, any internal or private-trust certificates, and any anticipated growth?"

Our volume is relatively small, so 40 is the total number of known, publicly exposed, certificates. The number of internal certificates is ~10. We anticipate 10% growth in a volume, per year.

87. Based on the current assumption, are the 40 certificates the maximum number of certificates to be actively managed and automated?

Correct. Our current volume is ~40 public and ~10 private SSL certificates.

88. What is your definition of a security provider?

An entity, system, or software component responsible for supplying cryptographic services, trust infrastructure, and identity verification used in issuing and validating digital certificates.

89. Question regarding the tender: p. 11, section 4.1.2 'Support for bring-your-own-CA' – which CA is this specifically referring to?

It's a generic model where we can use our own Certificate Authority (CA) if necessary. For example, on-premise Microsoft Active Directory Certificate Services.

90. Where can the "UPU General Terms and Conditions" be found?

https://www.upu.int/en/universal-postal-union/procurement#reference-documents

91. Is our assumption correct that this refers to services as "installation, configuration, trainings etc." rather than licenses or maintenance?

This refers to any recurring fees that need to be paid (such as subscription or license fees). If your services require upfront and/or one-time payment, please indicate so.

92. Are additional certificates expected to be managed via the solution, or is the initial volume limited to 40 SSL/TLS certificates?

The initial volume is limited to 40 public SSL/TLS certificates and ~10 private SSL/TLS certificates.

93. What is the expected number of certificates to be managed by the Certificate Lifecycle Management solution – CLM? (In some scenarios, there can exist certificates issued by the same Certificate authority, but out of CLM management – for example certificates for WiFi managed directly by the WiFi management)

Up to 40 public server SSL certificates and ~10 private server certificates.

94. We assume there is already a Certificate authority in place. Will the current CA be continued or a new CA and PKI is planned to be setup and licensed?

We're using two public CAs and one private CA. We'd prefer to continue using current arrangements.

95. Is this tender intended to establish a framework agreement that could potentially be leveraged by other UPU member countries or affiliated entities during the contract term?

No, the coverage of this tender is primary for UPU headquarters and doesn't have any intentions to cover other UPU member countries or affiliated entities.

96. Is the intention to procure certificate management licenses solely for the currently stated scope, or do you plan to use these licenses to manage certificates on behalf of your 192 member countries, with UPU acting as a central managing entity or Managed Service Provider (MSP)?

Solely for the currently stated scope.

97. Alternatively, do you envisage engaging an external MSP partner that would procure the licenses and manage the certificate environment on your behalf?

Considering our current volume we don't expect engagement of an external MSP.

98. It would also be helpful to understand which IT Service Management (ITSM) solution is currently in use within your organization.

EasyVista

99. Finally, you mentioned the possibility of future expansion. Could you please provide additional insight into how this expansion might materialize (for example, increased certificate volumes, additional certificate types, or an expanded organizational or geographic scope)?

We expect ~10% of increase of certificate volumes per year.

100. Can the UPU provide additional information on the expected scope of the environment, including the approximate number and types of systems, applications, cloud environments, and network components to be covered by the CLM solution, beyond the indication of approximately 40 SSL certificates?

The full inventory could be shared once the suitable candidates are shortlisted. At this this stage we can only share the number of certificates and brands involved.

101. Can the UPU provide an indication of the number of users who will require access to the CLM solution (e.g. IT operations or administrative users), including any expected role differentiation?

We're relatively small, so up to 10 users are expected. 5-7 IT operations and 2-3 admin (finance).

102. Can the UPU provide an indication of the number and types of private certificates currently in use (e.g. server, machine, application certificates), in addition to the approximately 40 SSL certificates mentioned?

All certificates are server certificates. The volume is ~40 public SSL certificates and up to 10 private certificates.

103. Are all listed integrations, such as F5 BIG-IP, F5 Distributed Cloud (XC), Azure, AWS, and Apache Tomcat, mandatory requirements, or can partial coverage be proposed if clearly documented?

All listed integrations are mandatory. If partial coverage is proposed, please indicate on mitigation measures to cover missed assets.

104. Are these systems the primary target platforms for certificate deployment, or are additional systems expected to be included?

They are primary target platforms.

105. Can the UPU confirm whether the listed certificate authorities represent the current standard, and whether alternative providers may be proposed?

The alternative providers can be proposed, however, it's outside of the scope if this RFP. The UPU, at this stage, is not seeking for alternative providers.

106. Does the UPU have a preferred deployment model (on-premises, SaaS, or hybrid), particularly with regard to data residency and cryptographic key management?
If a cloud-based solution is proposed, are there specific requirements regarding hosting location, particularly with respect to Switzerland-based data hosting?

We are open to all three models. In case of cloud-based solution, we'd prefer the solution hosted in Switzerland, otherwise, please specify where the UPU data will be hosted.

107. Which compliance standards are considered mandatory versus optional, such as ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2, or PCI DSS?

ISO 27001, ISO 27017, ISO 27018 and ISO 27701.

108. Can the UPU provide further guidance on the expected scope and duration of the initial implementation phase, including configuration, integration, testing, and go-live support?

Please propose the implementation plan considering our volume and the scope.

109. Are there specific expectations regarding support hours, incident response times, maintenance windows, and service continuity that bidders should consider when defining SLAs?

No specific expectations.

110. Does the UPU foresee extending the CLM solution beyond SSL/TLS certificates during the contract period, for example to client certificates, device identities, or code signing?

Not at this stage.

111. Could the UPU provide additional clarification on the intended operational scope of the functional requirements in section 4.1.2, in particular with regard to :Certificate discovery and inventory: scope of certificates, certificate types, and monitoring expectations

For example: discovery of server certificates based on the server inventory or domain list.

112. Lifecycle automation: expected use cases for issuance, renewal, rotation, revocation, and replacement

For example: automation of the renewal of the SSL certificate installed on F5 Big-IP appliance.

113. CA support: use of public CAs, private/internal PKI, ACME-based CAs, and bring-your-own-CA scenarios

For example: automation of the issuance and renewal of SSL certificates from listed public (DgiCert) and private (Microsoft CA) authorities.

114. ACME protocol support: intended use cases and supported challenge types

For example: automation of the renewal of the SSL certificates with Let's Encrypt supporting HTTP-01 and DNS-01.

115. Monitoring and alerts: definition of certificate health and alert thresholds

For example: alerting when the certificate is going to expire in XX days or alerting in case of a failed renewal.

116. Integrations and APIs: intended use of Delinea Secret Server and Thales Luna HSM, and whether these are used for storage, orchestration, or integration with downstream systems

For example: Delinea: storing of PFX export password, Thales Luna HSM: storing of the private key during CSR generation.

117. Could the UPU provide further detail on how compliance with the functional requirements will be assessed within the technical scoring, and whether individual requirements will be scored separately or by category?

Answered in 4.4

118. For a SaaS based offering would a hosting of the service and data in Frankfurt and/or Amsterdam be accepted?

Yes.

119. Is support for ACME challenge types: HTTP-01, DNS-01 a must criteria?

Please clarify what other challenges are supported by your solution, since those two are the most common challenge types nowadays.

120. Please can you confirm the number of certificates that should be managed? How many of them are public and how many private certificates?

Up to 40 public certificates and up to 10 private certificates.

121. Will support for Kubernetes also be of interest?

Not at this stage.

122. Could you please clarify the intended purpose and use cases for the integration with Thales Luna HSM within the scope of the CLM solution?

Storing of private keys during the certificates issuance.

123. Could you please clarify the intended deployment model for the CLM solution (e.g. virtual machine, physical appliance)?

Both models will be considered and evaluated equally.

124. If a SaaS solution is proposed, but not deployed in Switzerland, would it be a problem if it is under European space?

Please indicate where the UPU data will be stored.

125. For the renewal part. Is it expected Autoenrollment, is there any application or API that needs connector development?

Autoenrollment is expected. Please clarify what connector deployment is used for? Required vendor integration is provided in Page 12.

126. CA Support: If a SaaS solution is in place, for integration needs, can we deploy VPN for CA internal access?

OK.

127. Is there any validation process for DifiCert or Sectigo prior to issue any certificate today like email, phone call needed?

We currently use DNS validation.

128. What actions are expected from the CLM against HSM?

Storing of private keys during the certificates issuance.

129. We understand that this RFP covers TLS certificates for servers, applications and APIs.

Yes.

130. Does this also include pre-production and development environments, or just production?

All three environments should be covered.

131. Are there any requirements regarding key management using HSMs, or is it limited to certificate inventory and updates?

We would like to store private keys during the certificates issuance.

132. In case a SaaS solution is considered, has UPU any preferred Hyperscalers to be the one considered for the installation?

Please clarify the requirement for the hyperscales in case a SaaS solution is provided? What is the connection?

133. What is the estimation of that future expansion (4 years)? Should we consider a 25% increase per year?

10% increase could be considered.

134. How many references must be considered?

Up to 3.

135. Should all the installation be done remotely if possible?

Can be done remotely.

136. Will UPU provide a template to write the technical specification?

No. You can use Sections 4.1.2 and 4.1.3 to compare your solution against our requirements.

137. Is there a limit of pages on the technical specification?

N/A

138. Is there any time consideration for the project to be implemented?

Please refer to section 4.5.

139. May you please clarify the following: In the event that Bidders propose a cloud-based solution, this should be hosted in Switzerland. If the proposed solution is not hosted in Switzerland, Bidders shall indicate where the UPU data managed by the solution will be stored. It reads that cloud-based must be in Switzerland, but in the following sentence it reads it is not mandatory. May you please so kind to clarify.

In case of a cloud-based solution we prefer to have it hosted in Switzerland. If it's not possible, we'd ask you to indicate where the UPU data will be stored.

140. Could you please elaborate on the expected use cases for integrating Delinea Secret Server and Thales HSM with a centralized key and certificate management platform?

For example, for Delinea Secret Server integration: storing PFX export password. For Thales HSM: storing keys on HSM.

141. What are the primary objectives behind this integration (e.g., centralized certificate lifecycle management, key protection via HSM, compliance, automation, etc.)?

The primary objective is the key protection via HSM.

142. Which processes are you aiming to automate across these systems (e.g., certificate issuance, renewal, revocation, secret rotation, key storage, etc.)?

Key storage.

143. Would you be open to leveraging a middleware layer to orchestrate API interactions between Delinea, Thales HSM, and Key Manager Plus?

Yes.

144. If so, do you have any constraints or preferences regarding the middleware (e.g., on-premise vs. cloud deployment, specific technologies, security requirements, etc.)?

On-premise would be preferable. No other constraints.