Questions : RFP-2025-021 - UPU security certification system

1. Do you already have a CI/CD system in place, or do you expect the vendor to build a deployment pipeline?

The UPU does not have a pre-existing CI/CD pipeline for this project. The Vendor is expected to build and maintain a deployment pipeline appropriate to the solution's architecture and requirements.

2. Does the UPU expect the import of historical worksheets, processed certifications, and existing certificates into the new system? If so, in what format will the data be provided and how many records are estimated?

Yes, the UPU expects historical worksheets, processed certifications, and existing certificates to be imported into the new system. These will primarily be in Microsoft Excel and PDF formats. While the RFP does not specify the volume, bidders should plan for scalability and structured ingestion of these records. Currently, the list of certified countries may be found here: https://www.upu.int/UPU/media/upu/files/postalSolutions/programmesAndServices/postalSupplyChain/Security/Certified%20critical%20facilities/S58-S59-Certification-Review-Tracker-05-05-2025.pdf

3. Do you already have existing APIs (e.g., national operator databases) that the system will need to integrate with?

The solution must be capable of integrating with external systems, and interoperability via standardized APIs is expected.

4. Which specific optional plug-ins (e.g., risk assessment, AI detection) is the UPU considering over the next 12–24 months? Accordingly, should the APIs be public or internal-only (for integration with UPU systems)?

The UPU anticipates potential integration of plug-ins for risk assessment, compliance reporting, and AI-driven threat detection within 12–24 months. APIs should be modular and secure, and may be public or internal depending on the function. External integrations must follow strict security protocols.

5. Do you have requirements regarding the data-exchange format: REST / GraphQL / SOAP?

The RFP specifies the need for interoperability using standardized APIs but does not mandate a specific format. The system should ideally support REST and be extendable to others like GraphQL or SOAP if necessary.

6. Has the UPU already decided whether the platform will be hosted in the cloud or on-premises?

If not on-prem, does the client prefer a specific cloud provider (AWS, Azure, GCP)? If cloud, which provider and region? This may significantly affect costs. Should the cost of hosting services be included in the financial proposal, or is it covered by a separate UPU budget? Hosting Environment and Cost Responsibility:

The final decision on hosting (on-premises vs. cloud) has not yet been made. The RFP indicates that the UPU will manage infrastructure—either via its own servers or through a UPU-managed cloud environment. Therefore:

Bidders should not include hosting costs in their financial proposal.

Vendors are not expected to procure or manage hosting services.

No specific cloud provider or region has been designated at this stage.

The vendor should deliver the platform in a manner that supports deployment in both environments and adheres to ISO 27001-compliant security principle

7. Does the client foresee the need for auto-scaling, or will resources be allocated statically?

The RFP indicates the need for scalable infrastructure to handle increasing certification volumes and expanding datasets. Auto-scaling capabilities are recommended.

8. Should backups be managed by the vendor, or will they be handled by the UPU infrastructure? How long must (a) audit logs and (b) evidence attachments be retained? Are there policies for deletion/anonymization and, if so, which standard do they follow?

Backup responsibilities are not specified, but Vendors should propose solutions. Audit logs must capture administrative and superuser actions and should be retained according to standard security practices (e.g., at least 2 years). Evidence attachments must also be securely stored, with retention and deletion policies aligned with applicable data protection norms.

9. Are there specific requirements regarding encryption of data at rest and in transit (e.g., AES-256, TLS 1.3)?

The platform must implement robust data protection measures. While not naming specific standards, AES-256 for data at rest and TLS 1.3 for data in transit are considered industry best practices and are recommended.

10. Are there requirements for regular penetration tests or external audits that should be coordinated by the vendor and included in the costs?

Yes, regular security audits and penetration testing are expected, especially for administrator and superuser access control systems.

11. Is Active Directory intended only for authentication (SSO), or also for authorization and role-based access control (RBAC)?

The UPU's Active Directory is to be used for user authentication. Role-based access control (RBAC) may also be mapped via AD group membership.

12. Can users outside of AD (e.g., guests or external reviewers) log in through other methods?

Yes, users outside of AD, such as external reviewers, should be able to authenticate through alternative secure methods, possibly via federation protocols.

13. Should only domain-based authentication (LDAP) be supported, or should the federation protocols (e.g., SAML, OIDC, Azure AD) be taken into consideration?

Yes, support for federation protocols like SAML, OIDC, and Azure AD should be considered to accommodate non-domain users and cross-organization access.

14. Do we need to implement Single Sign-On (SSO)? Which other systems must it interoperate with?

Single Sign-On (SSO) is required. It should interoperate with UPU's internal systems, particularly Active Directory, and allow secure access for designated users globally.

15. Will you expose the LDAP endpoint internally, or should we set up a VPN tunnel / cloud connection?

The system should not rely on direct exposure of LDAP endpoints. A secure connection method such as VPN or cloud interconnect is preferable.

16. Should role assignment (e.g., reviewer, admin, superuser) be based on AD group membership (memberOf)?

Where possible, roles should be assignable via AD group membership (e.g., using 'memberOf' attributes) to streamline administration.

17. Can role assignment within the system be overridden locally, independent of AD?

Yes, the platform should allow authorized superusers to override or assign roles locally in special cases, independent of AD groups.

18. Does the UPU have an internal help desk, or does it expect first-line support from the vendor? What is the required SLA response time?

The UPU will oversee platform management but expects first-line user support to be provided by the Vendor. SLAs for incident response should be clearly defined in the proposal (e.g., critical within 2 hours, normal within 24 hours).

19. How many people and in which roles need to be trained? Are e-learning materials required?

Training is required for various user roles (e.g., superusers, admins, reviewers, security focal points). E-learning materials are expected to be SCORM-compliant

20. We would like to inquire whether the Contracting Authority plans to organize a second Q&A round or a pre-bid conference to further clarify specific aspects of the tender.

A second Q&A round or pre-bid conference is not planned

21. We understand that the scope focuses on software delivery and that hosting will be managed by UPU (either on UPU's servers or in the cloud). Kindly confirm that bidders are not expected to include hosting or cloud infrastructure in their financial proposal, and that the system is to be delivered as software only.

Confirmed.

22. As the bidder is responsible for designing the user interfaces and content, we understand that the responsibility for preparing translations into the six required languages (English, Arabic, French, Spanish, Portuguese, Russian) lies with the bidder. However, we kindly ask whether UPU will provide support or validation for official terminology, particularly for Russian and Portuguese.

The UPU will provide validation for official terminology.

23. Can you confirm whether the digitization of the tools in Annex 1 (e.g. question bank, scoring sheets, heat maps) must replicate the structure exactly as-is, or whether the bidder may redesign the user experience as long as all logic and requirements are maintained?

Bidders may redesign the user interface and experience to enhance usability and efficiency, provided that all underlying logic, functionalities, scoring rules, and compliance mechanisms (as defined in Annex 3 of the RFP) are fully maintained and traceable

24. Is it expected that the platform will automatically calculate section ratings (FI, LI, PI, NI) and overall goal-level characterizations based on the scoring logic defined in Annex 3? Or will reviewers continue to apply these manually?

The system is expected to automate the calculation of section ratings (FI, LI, PI, NI) and overall goal-level outcomes based on the logic defined in Annex 3.

25. Will sample or anonymized data from previous certifications (e.g., completed self-assessments, audit reports) be made available to support testing and quality assurance during the development phase?

Full data will be made available to support testing and quality assurance with the expectation the information will treated in a confidential manner.

26. Could you provide an approximate estimate of the number of designated operators, reviewers, and administrators expected to use the platform concurrently?

This will assist with planning for performance and scalability.

The system must be capable of supporting concurrent use by at least:

- 100 Designated Operator (DO) users (security focal points)
- 20–30 Reviewers
- 5–10 Administrators
- Up to 5 Superusers (UPU only)

The platform should be scalable to accommodate increased future adoption. The UPU has 192 member countries and approximately 207 DO's.

27. Should the platform integrate with any existing UPU systems, such as Active Directory for user authentication? If yes, please specify the expected integration points or protocols.

The system must integrate with the UPU's Active Directory for user authentication. Role-based access control should be managed accordingly. No other system integrations are mandatory at this stage, but the architecture should support interoperability with potential third-party tools via standard APIs (e.g., REST)

28. Is the scoring/grading logic from Annex 1–3 final, or do you expect flexibility/updates later?

The scoring logic is initially based on Annex 3 and reflects the current certification methodology. However, the system must be built to allow flexibility for future updates, improvements, or the addition of new standards and scoring models.

29. Should the system support manual overrides by reviewers or UPU?

Yes

30. Can you confirm the steps and roles in the workflow? (e.g. DO → Reviewer → Admin → Certificate) The general workflow is:

1. DO Security Focal Point submits the self-assessment.

2. Reviewer validates evidence and assigns scores.

3. Administrator manages records and oversees completeness.

4. Superuser provides final validation and issues the certificate.

This linear flow must be enforced by the platform, with branching for recertifications or escalations as necessary.

31. What format should the certification output be (PDF, digital badge, API feed)?

Certification outputs must be available in PDF format. Support for additional formats (e.g., digital badges, structured API outputs) is encouraged and should be proposed as optional features.

32. Will the system be hosted on UPU-managed infrastructure, or do you expect a vendor-managed cloud environment?

The system may be hosted on UPU infrastructure or in the cloud. Infrastructure is managed by the UPU's Postal Technology Centre. If the Vendor proposes a cloud solution, hosting costs must be included in the financial proposal.

33. Will translations be provided by UPU, or should the system support translation management (e.g. i18n module)?

The system must support localization in Arabic, French, Spanish, Portuguese, Russian, and English. Translations of key materials will be provided by the UPU, but the platform should include an internationalization (i18n) framework for managing multilingual content.

34. Should questionnaires be language-dependent, or user-preference based?

Questionnaires and interfaces should adapt based on user language preference. The system must allow users to select their preferred language upon login and store that preference for future sessions.

35. What granularity is required for audit logging (login/logout, submission, reviewer comments, role changes)? Audit logs must record:

- Login/logout and failed attempts

- Form submissions and evidence uploads

- Reviewer comments and scoring actions

- Role assignments/changes

- Administrative and configuration actions by superusers

Granular and timestamped logging is mandatory for system integrity.

36. Should audit logs be exportable or only viewed via UI?

Audit logs should be viewable via the UI and exportable (e.g., CSV, JSON) by authorized users, to support compliance reviews and investigations.

37. Are there any planned integration with external regulators or third-party systems (ICAO, IATA)?

No immediate integrations are defined. However, the system must be API-ready to support future interoperability with ICAO, IATA, or WCO systems as part of expanding security certification recognition.

38. How many concurrent users do you expect during peak certification windows?

While exact concurrency figures are not specified, the system must support simultaneous access by at least 100 users globally, with elasticity to accommodate regional certification drives.

39. Should all internal rules (scoring, workflows) be editable via admin panel, or hard coded from spec?

Where feasible, scoring weights and workflow configurations should be editable by superusers through an admin panel. However, critical security logic may be embedded to protect integrity.

40. Are there any regulations preventing data from being stored outside specific jurisdictions (e.g. Switzerland, EU)?

No

41. Is Multi-Factor Authentication (MFA) required for any user roles, particularly superusers or reviewers?

Yes. MFA is mandatory for superusers and administrators, and recommended for reviewers. The system must support MFA implementation as part of its access control measures.

42. Will there be a warranty/bug-fixing period post-handover outside the six-month technical support window?

The six-month post-deployment technical support includes bug fixing. Any warranty or support extension beyond this period must be clearly proposed in the financial and service offer.

43. What will be the project governance structure on the UPU side (sponsor, steering committee, technical and functional contacts)?

The project will be overseen by a UPU-appointed Project Sponsor supported by a Steering Committee comprising key UPU stakeholders. Technical and functional leads from the UPU's Postal Technology Centre (PTC) and Security Programme will provide guidance throughout.

44. Who will validate deliverables at each milestone? Is there an existing validation or acceptance framework?

Deliverables will be validated through a defined acceptance framework. Each milestone will be subject to formal review and approval by designated UPU personnel.

45. Will any external stakeholders (partners, consultants, institutions) be involved in project validation or oversight?

External consultants may be invited to provide expert input, but final validation authority rests with the UPU.

46. What will be the main working language during exchanges with stakeholders?

English will be the main language for communication and documentation.

47. Could you please confirm if our company, incorporated in Senegal, is eligible to submit a proposal for this call for tenders?

Companies incorporated in UPU member countries, including Senegal, are eligible to submit a proposal.

48. What is UPU's current reference architecture (servers, databases, middleware, security)?

The UPU's infrastructure includes virtualized environments hosted on-premises and in the cloud, using PostgreSQL, MS SQL Server, and Active Directory.

49. Does the project need to comply with any existing IT standards or urbanization schemes?

Yes, solutions should respect the UPU's internal cybersecurity and urbanization standards.

50. Should the source code be open and transferable to UPU?

Yes, the code must be open and fully transferable to the UPU upon delivery.

51. Are there any preferences or constraints regarding programming languages, frameworks, or tools?

The UPU has no strict preferences but favors mainstream, well-documented frameworks.

52. What internal security standards should be respected (in addition to ISO 27001 – e.g., OWASP, CIS, NIST)?

Solutions should comply with ISO 27001 and incorporate OWASP, CIS benchmarks, and NIST practices where applicable.

53. Should the solution be auditable by third parties (e.g., internal audit, security certification)?

Yes, the system should be auditable by internal and external parties.

54. Does UPU already use monitoring, backup, or logging solutions that the new system must integrate with?

The solution must integrate with existing UPU tools where applicable.

55. Are there specific continuity requirements (expected RPO/RTO, high availability)?

Target RPO ≤ 24h and RTO ≤ 48h; high availability is preferred.

56. Should the system support offline or partially disconnected use cases?

No offline operation is required.

57. Should the APIs/interfaces follow specific interoperability standards (REST, SOAP, GraphQL, etc.)?

RESTful APIs are preferred; GraphQL or SOAP may be accepted if justified.

58. Is the 3 to 6-month implementation period fixed or flexible depending on the technical proposal?

The 3–6 month range is indicative. Proposals with justified adjustments will be considered.

59. Is the expected start date (end of May 2025) negotiable depending on contract signature?

Negotiable, depending on contracting timelines.

60. What are the key project milestones (e.g., MVP, integration testing, training, go-live)?

Expected milestones include kick-off, MVP delivery, integration testing, user training, UAT, and go-live.

61. What will be the availability of UPU stakeholders (to avoid overlap with holidays or international events)?

Avoids overlap with UPU Congress (September 2025) and summer holidays; stakeholder availability will be confirmed during planning.

62. Will UPU provide a test environment, or should the contractor set it up?

Bidders may propose to set up test environments as part of their proposal.

63. Is there a high-priority scope to be delivered first (critical feature, region, user type)?

The digital workbook module and user management tools will be considered a priority for early delivery.

64. How many user profiles need to be trained by role (administrators, reviewers, superusers, etc.)?

Training should cover four main roles – security focal points, reviewers, administrators, superusers – totaling approximately 100–120 users globally.

65. Does UPU have a documentation platform where deliverables should be uploaded?

Yes, the UPU provides documentation and training repositories (e.g., TRAINPOST (SCORM), internal Confluence-based systems).

66. What is the technical level of the end users and administrators to be trained?

Varied; assume moderate digital literacy for focal points and higher for admin roles.

67. Does UPU expect a structured knowledge transfer plan (training, coaching, documentation)?

Yes, a structured transfer plan (with documentation, coaching, handover sessions) is required.

68. Should the training be multilingual? If so, which languages are required?

Yes, training and user interfaces should support EN, FR, ES, AR, PT, and RU.

69. Will the training sessions be conducted onsite in Bern, online, or hybrid?

A hybrid model is preferred – core training in Bern or online, followed by recorded/self-paced materials.

70. Are the user roles (security focal point, reviewer, admin, superuser) fixed or likely to evolve?The four core roles are fixed, but future adaptations may be required.
71. What level of customization is expected for access rights, views, and workflows?

Fine-grained role customization, views, and workflows should be supported.

72. What are the most common use cases to be covered in the first version?

Certification tracking, document upload, reviewer scoring, notifications, and dashboard reporting.

73. Should the system include advanced statistics or dynamic dashboards on certifications?

Yes, dynamic dashboards with filter and export options are expected.

74. Is modularity required to support multiple certification standards from version 1 (beyond S58/S59)?

Yes, support for future certification modules is essential.

75. Should the document management features include advanced functions (versioning, legal archiving, OCR)?

Versioning, secure storage, and export are required; OCR and legal archiving are preferred but not mandatory.

76. Do existing business procedures or forms (e.g., commitment form, Excel annexes) need to be kept as-is?

The Excel-based workbook and forms will be preserved as reference during early implementation phases.

77. What sensitive data will be handled? Are there requirements for pseudonymization, anonymization, or end-to-end encryption?

PII and security data will be processed; the system must use pseudonymization, encryption at rest/in transit, and logging.

78. Does UPU have a list of future certifications or regulatory changes to anticipate in the design?

The system should allow onboarding of additional certification frameworks (e.g., S60) as needed.

79. Will the platform need to integrate with other internal tools (e.g., reporting systems, member database, CRM)?

Yes, with PTC systems, user database (Active Directory), and reporting interfaces (Power BI preferred).

80. Are there dependencies with other IT projects or internal processes (e.g., AD migration, ERP overhaul)?

AD integration is required; future ERP or legacy system integration should be modular.

81. Are payment conditions tied to results or deliverables?

Yes, payments are tied to milestone achievement and deliverable validation.

82. Are travel and accommodation expenses in Bern allowed (or should they be avoided)?

Travel to Bern is discouraged unless explicitly requested by UPU. Any such costs require prior written approval.

83. What are the expected billing modalities (per milestone, time & materials, other)?

Fixed price preferred, aligned to deliverables/milestones; no time & materials model unless justified.

84. Are there clauses regarding usage rights, intellectual property, or solution reuse?

UPU retains all IP rights; reuse of solution elements outside the UPU requires prior written authorization.

85. Are late penalties foreseen? From what delay threshold ?

Yes, delays beyond agreed timelines may incur penalties as defined in the contract.

86. Should the 6-month post-delivery support be extendable through an addendum?

Yes, the 6-month support period may be extended via addendum.

87. Does UPU expect an agile approach with iterative deliveries, or a more traditional model with fixed specifications?

Agile preferred, with iterative delivery and continuous feedback loops. A hybrid model is acceptable.

88. Is there a preferred project management tool (e.g., Jira, MS Project, Trello)?

Jira is preferred for task tracking; however, other tools may be considered.

89. Would UPU like a dedicated online project dashboard (shared timeline, decision logs, progress tracking)?

Yes, an online shared dashboard for tracking milestones and decisions is recommended.

90. Are there formal KPIs expected (e.g., on deadlines, quality, satisfaction)?

Yes – timelines, quality indicators, stakeholder satisfaction, and issue resolution metrics.

91. What are the key checkpoints for UPU (spec validation, milestones, UAT, go-live)?

Key checkpoints include spec validation, MVP, UAT, and go-live.

92. Would UPU like a final report or documented project retrospective?

A final report and project retrospective must be delivered at project completion.

93. In case of major issue or deviation, what escalation or arbitration process should be followed?

The escalation process will be defined during kick-off and governed by the Steering Committee.

94. Fixed-Price Proposals and Budget Expenditure Logging

You are correct in your assumption. For fixed-price proposals, detailed expenditure tracking is not required for invoicing or reimbursement purposes.

95. Audit Trails and System Activity Logs

The “audit trails and system activity logs” referenced under the RFP relate not to development task tracking (e.g., Jira), but to the operational behavior of the delivered system. Specifically, once the platform is deployed (even during UAT or staging), the system must be capable of logging user actions—particularly for superusers and administrators. These logs should include:

- Logins, session durations, and access attempts

- Data modification or submission (e.g., assessment forms, certification records)

- Configuration or user rights changes

- Any security-related events (e.g., failed authentication attempts, role escalations)

These logs are essential for accountability, certification process verification, and compliance monitoring.

96. Integration of Reports into the Platform

During the development phase, we do not expect dynamic integration of development status reports into the platform dashboards. The language in the RFP refers to the final operational platform’s capability to generate internal system reports (e.g., certification status dashboards, audit histories).

For project management purposes during the development lifecycle, release notes, testing reports, and milestone updates can continue to be shared externally with UPU project leads via standard formats (PDF, Excel, Jira exports, etc.). There is no requirement to embed development reports into the pre-live platform.

97. What specific aspects of budget expenditure are expected to be logged and reported?

Scope of “Budget Expenditure” Logging and Reporting: This refers specifically to logging activities and costs incurred within the scope of services related to the automation of the S58/S59 certification process. It includes internal system costs such as hours logged by consultants, development costs, licensing costs (if any), infrastructure usage (e.g., hosting services), and other relevant implementation or support expenses billed to the project. It does not include broader UPU financial oversight or certification financing mechanisms by designated operators, as referenced in Section VII of the Certification Process document.

98. What is the intended structure or process for this reporting?

Reporting Structure: Vendors will be expected to provide structured reporting via audit trails and system activity logs that track service progress, user activity, and budget expenditure breakdowns. This will be tied into the platform’s administrative and superuser dashboards. The format of these reports will be defined by the UPU and should include monthly summaries as part of the routine project reporting deliverables.