PACAM 2027

PAN-AMERICAN CONGRESS OF AEROSPACE MEDICINE

TECHNICAL AND OPERATIONAL SPECIFICATION No. 001/2026

CERTIFICATE ISSUANCE AND VALIDATION SYSTEM

Functional requirements, security, governance and public validation

Field	Details
Responsible entity	PACAM PARAGUAY E.A.S.
RUC	80173825-3
Internal code	CERT-SYS-001/2026
Event	PACAM 2027 — Pan-American Congress of Aerospace Medicine
Related documents	Academic Project; Attendance and Certification Regulation; Attendance Control SOP; Official Certificate Template
Current scientific-academic workload	18 hours and 50 minutes
Minimum attendance for general certificate	75% — operational minimum of 14h10 under the current schedule
Version	1.0
Issued	October 7, 2026

Specification document for procurement, development, acceptance testing and system operation.

www.pacam2027.com

1. PURPOSE AND SCOPE

This Specification defines the minimum requirements for the digital system responsible for generating, registering, making available, reissuing, cancelling and publicly validating PACAM 2027 certificates. The system must integrate with the established academic process and use the attendance database consolidated and approved by the Academic Secretariat and Academic Committee as its authoritative source.

The system must support both individual issuance and batch issuance, preserve traceability for every action, reduce the possibility of document fraud and provide universities, employers, professional councils and other receiving entities with a simple authenticity-check mechanism.

CENTRAL PRINCIPLE

The QR Code and public validation code must allow certificate authenticity to be confirmed without exposing CPF, identity-document number, email, telephone number, date of birth or other unnecessary personal data.

2. SOURCE DOCUMENTS AND DATA

- PACAM 2027 Academic-Scientific Project, defining the event, program, academic workload and responsible parties.
- Act establishing and appointing the Academic Committee and Technical Officers.
- Attendance, Academic Workload and Certification Regulation, establishing eligibility and issuance criteria.
- Attendance Control SOP, defining capture, correction, auditing and closure of records.
- PACAM 2027 Official Certificate Template, containing dynamic fields and institutional presentation.
- Final participant database containing identification, actually certified workload, attendance, modality and eligibility status.

No certificate may be issued directly from preliminary registration data or attendance records that have not yet been consolidated.

3. OVERVIEW OF THE SOLUTION

Component	Function
Administration Module	Manages registrations, profiles, parameters, templates, batches and permissions.
Academic Import Module	Receives the final attendance database and performs consistency checks.
Certification Engine	Calculates eligibility, populates the template, generates the PDF and records version and hash.
Certificate Repository	Maintains the official file, metadata, versions and status.
Public Validation Portal	Allows validation through QR Code or validation data without requiring authentication from the person checking it.
Reissue/Cancellation Module	Controls corrections, replacements, cancellations and justifications.
Audit Trail	Records administrative actions, changes, approvals and relevant technical events.
Security Services	Provides authentication, authorization, MFA, backups, encryption, monitoring and abuse protection.

Logical flow: Finalized attendance database → eligibility validation → batch approval → certificate generation → signature/sealing → publication of validation page → delivery to participant → audit and any subsequent reissue/cancellation.

4. UNIQUE CERTIFICATE CODE STANDARD

4.1 Visible public code

Each certificate must receive a permanent, random public identifier independent of the participant's registration number and the database's internal key.

Recommended format: PACAM27-C-XXXX-XXXX-XXXX-XXXX
Example: PACAM27-C-7K4M-Q9T6-H2VX-R8NP

The 16 variable characters must be generated by a cryptographically secure source and use an alphabet without visually ambiguous characters, for example: 23456789ABCDEFGHJKMNPQRSTUVWXYZ. The code must not contain CPF, participant initials, date of birth, registration number or any derivable personal data.

- The PACAM27 prefix identifies the event and year.
- The letter C identifies the Certificate class and reserves room for future document classes.
- The random portion must be unique in the database and protected by a uniqueness constraint.
- The code remains associated with the same credential in a corrective reissue; document revision is controlled separately.

4.2 Internal identifier

The database must use its own internal identifier, preferably a UUID, which need not be displayed publicly. The internal ID must not be reused as a validation token.

4.3 Secret validation token

In addition to the public code, each active certificate must have a high-entropy random token of at least 128 bits, used exclusively in the QR Code URL. The token must not be sequential or predictable.

Conceptual example: https://cert.pacam2027.com/v/

5. QR CODE STRUCTURE

The QR Code printed on the certificate must contain only an HTTPS validation URL. It must not contain JSON with personal data, CPF, email, telephone number, date of birth or detailed attendance data.

Element	Minimum specification
Content	HTTPS validation URL with a random token.
Recommended destination	https://cert.pacam2027.com/v/
Minimum size in PDF	25 mm × 25 mm, preserving a clear margin around it.
Quiet zone	At least 4 modules on all sides.
Error correction	Level M or Q.
Contrast	Light background and dark modules, with no overlaid images that impair readability.
Redirection	Permitted only within a PACAM-controlled domain and using HTTPS.
Tracking	Access may generate a technical validation log, without unnecessary profiling of the person checking it.

6. PUBLIC VALIDATION PAGE

6.1 Access

The page must work without requiring the person checking it to log in. Validation may take place directly through the QR Code or through a manual form requiring the certificate code and, if adopted, a short verification key.

The portal must not offer open searches by name, CPF, email or participant lists. Validation pages must be configured not to be indexed by search engines.

6.2 Public fields when the certificate is ACTIVE

Field	Public display
Status	ACTIVE / ACTIVE
Participant name	Full name exactly as shown on the certificate.
Event	Pan-American Congress of Aerospace Medicine — PACAM 2027.
Dates	April 23–25, 2027.
Location	Foz do Iguaçu, Paraná, Brazil.
Certified workload	Individual workload actually certified.
Attendance	Consolidated percentage or equivalent, when included in the certificate.
Certificate code	Full public identifier.
Revision	Current revision number, e.g. Rev. 01.
Issue date	Date of first issuance.
Reissue date	When a later revision exists.
Issuing entity	PACAM PARAGUAY E.A.S. — RUC 80173825-3.
Validation	Explicit message confirming authenticity and integrity of the current version.

6.3 Data that must not be publicly displayed

- CPF, identity card, passport or other personal document.
- Home address, email, telephone number or date of birth.
- Attendance logs by time, device or access door.
- Internal justifications, attached documents and detailed appeal reasons.
- Administrative user who made changes, IP addresses, internal hashes or security data.

7. CERTIFICATE STATUSES

Status	Visibility	Meaning
DRAFT	Internal	Data prepared but not approved; cannot be publicly validated.
PENDING	Internal	Awaiting approval, signature, consolidation or processing.
ACTIVE	Public	Valid and current certificate; public page confirms authenticity.
SUPERSEDED	Public	Previous version replaced by reissue. Must indicate that a current revision exists without exposing internal data.
CANCELLED	Public	Certificate is no longer valid. The page must clearly state that it must not be accepted.
TECHNICAL ERROR	Internal	Transitional state for a generation, storage, signature or publication failure.

Validity rule: only certificates with ACTIVE status may be presented by the system as valid. An old PDF does not regain validity if the public page indicates SUPERSEDED or CANCELLED.

8. ISSUANCE RULES

1. Accept only the final attendance database after definitive closure.
2. Validate the participant's name, internal identifier, individual workload, attendance and certificate type.
3. Apply the eligibility criteria in the Certification Regulation.
4. Automatically block issuance when minimum requirements are not met, unless a formally authorized and recorded decision applies.
5. Generate unique public codes and validation tokens.
6. Populate the dynamic fields of the Official Certificate Template.
7. Generate the final document as a PDF; the Word file remains a template and must not be distributed as an official certificate.
8. Calculate and store the SHA-256 hash of the final issued PDF.
9. Apply an electronic signature or the defined institutional mechanism to the final version, when available.
10. Record date, time, user/approver, template version, revision and status.
11. Publish the validation page and only then make the certificate available to the participant.

9. DYNAMIC TEMPLATE FIELDS

Field	Source / use
<>	Validated full name.
<>	Workload in Portuguese, e.g. 16h40 or 18h50.
<>	Workload in the English version.
<>	Consolidated attendance percentage/indicator.
<>	Unique public code.
<>	Short/canonical URL for the public page.
<>	Initial issue date or field according to the layout.
<>	Name of authorized representative according to current documentation.
<>	Credential revision, e.g. 01, 02.
<>	Image generated from the validation URL.

10. REISSUANCE AND REVISION CONTROL

Reissuance must not erase history. Every new version must be recorded as a credential revision or, in the cases defined below, as a new credential linked to the previous one.

Situation	Treatment
Verified spelling error in name	Keep certificate code; generate a new revision; previous version becomes SUPERSEDED.
Workload correction after an approved appeal	Keep code; create a new revision; record decision and recalculation; previous version becomes SUPERSEDED.
Signature update or visual element change without academic change	Keep code; create a new revision when the PDF is regenerated and published.
Corrupted file or download failure without content change	May be regenerated; record technical event and preserve content and code.
Certificate issued to the wrong person	CANCEL the incorrect certificate and issue a new code to the correct recipient.
Confirmed fraud, falsified attendance or loss of eligibility	CANCEL; do not automatically reissue; require a formal decision by the competent body.
Substantial change to event, modality or credential type	Issue a new code and retain an audit link to the previous credential.

The public page for a superseded version must state that the document is not current. Where technically appropriate, it may provide a secure link to validation of the current version, without allowing enumeration of other certificates.

11. CANCELLATION

Cancellation requires an authorized role, a mandatory justification and a record of the approving authority. The file must not be deleted from the institutional repository; it must be retained for auditing with restricted access.

- The public page must prominently display CANCELLED status.
- The system must not publicly disclose the detailed reason for cancellation. It may use a neutral message: "This certificate is not currently valid. Contact the PACAM Academic Secretariat for clarification."
- The cancelled document's QR Code must continue to resolve to the validation page, which will display the correct status.
- Cancellation must create an audit event with date, time, user, internal reason, approver and documentary reference where applicable.
- If cancellation was made in error, reactivation may occur only through a formal procedure with dual authorization and a complete record of the reversal.

12. ROLES AND ACCESS CONTROL

Role	Minimum scope
System Administrator	Technical configuration, users and integrations; must not change academic workload without academic authorization.
Academic Secretariat	Search participants, request issuance, correct permitted data and track reissues.
Attendance Supervisor	Provide/validate the consolidated database and access necessary attendance data.
Academic Approver	Approve batches, exceptions and corrections affecting workload or eligibility.
Institutional Representative/Signer	Approve or sign documents where applicable, according to current authority.
Auditor/Read-only	Read-only access to reports and audit trail.
Participant	Access only their own documents if an authenticated portal exists; public validation remains separate.

Segregation of duties: whenever possible, the same person should not be solely responsible for changing workload, approving an exception and publishing the certificate. Significant academic changes require dual validation.

13. INFORMATION SECURITY

Control	Requirement
Transport	HTTPS mandatory across the portal, APIs and public pages.
Administrative authentication	Individual credentials; MFA mandatory for privileged roles.
Passwords	Stored using a resistant password-hashing algorithm and current parameters; never in plain text.
Authorization	Role-based access control and least-privilege principle.
Database	Encryption at rest where supported by the infrastructure and protected backups.
Validation tokens	Cryptographically secure generation; non-sequential and never reused.
Logs	Logical immutability or controls against alteration; retention according to institutional policy.
Backups	Automated routine, periodic restoration tests and segregated copy.
Abuse protection	Rate limiting, progressive blocking and additional mechanisms after anomalous attempts.
Secrets	Keys, passwords, service tokens and digital certificates kept outside source code with controlled rotation.
Environments	Separate development/acceptance and production; real data must not be used in testing unless necessary and adequately protected.
Monitoring	Alerts for issuance failures, mass status changes, privileged-access attempts and abnormal validation patterns.

14. DATA PROTECTION AND PRIVACY

The system must apply data minimization, access control and separation between information needed for issuance and information actually disclosed during public validation. The public page must reveal only the elements necessary to verify the credential.

- Do not include sensitive personal data or identification documents in the QR Code.
- Do not allow public searches by CPF or enumeration of participants.
- Display an appropriate privacy notice on the portal and identify an institutional contact channel.
- Define a retention policy for certificates, issuance records, logs and supporting documents, respecting applicable obligations and defense/audit needs.
- Log administrative access to personal data and registration changes.
- Allow correction of registration data through a controlled workflow while preserving history.

15. FILE INTEGRITY AND SIGNATURE

The official certificate delivered to the participant must be a PDF generated by the system. The Word file is only the source template. For each published PDF, the system must store at least its SHA-256 hash and the reference to the template version used for generation.

If a cryptographic digital signature is adopted, the system must keep certificates/keys under institutional control and record the time and identity of the signing process. A digital signature does not eliminate the need for public validation through QR Code and unique code.

Expected result: authenticity must be verifiable through two complementary layers: (1) file integrity/signature, when available; and (2) confirmation of status and essential data on the official PACAM portal.

16. AUDIT TRAIL

Event	Minimum record
Issuance	Who requested, who approved, date/time, batch, participant, template version, ID and hash.
Reissuance	Previous/new revision, categorized reason, requester, approvers and dates.
Cancellation	Certificate, internal reason, approver, date/time and documentary reference.
Reactivation	Justification, dual authorization and complete history.
Registration change	Field changed, previous/new value where permitted, user and date/time.
Attendance import	File/batch, hash or database identifier, responsible party and validation result.
Privileged access	Login, relevant failures, user creation/deactivation and permission changes.
Public validation	Date/time, certificate queried and result; collect only technical data necessary for security and statistics.

17. MINIMUM DATA MODEL

Logical field	Purpose
certificate_id_internal	UUID/internal key.
certificate_public_id	PACAM27-C-...
validation_token_hash	Token hash or equivalent; avoid storing the secret in clear text when architecture permits.
participant_id	Internal participant reference.
participant_name	Certified name.
event_code	PACAM2027.
certificate_type	Participant, speaker, moderator, instructor, scientific paper, committee, etc.
certified_minutes	Certified workload in minutes.
attendance_percent	Consolidated percentage, where applicable.
status	draft, pending, active, superseded, cancelled, technical_error.
revision	Sequential integer per credential.
first_issued_at	Date/time of first issuance.
reissued_at	Date/time of current revision, if any.
pdf_storage_ref	Secure reference to the official file.
pdf_sha256	SHA-256 hash of the PDF.
template_version	Version of the template used.
issuer_entity	PACAM PARAGUAY E.A.S.
issuer_ruc	80173825-3.
approval_ref	Reference to approval batch/action.
created_by / approved_by	Responsible users.
created_at / updated_at	Audit timestamps.

18. FUNCTIONAL REQUIREMENTS

ID	Requirement
RF-01	Import eligible participant database with schema and inconsistency validation.
RF-02	Generate certificates individually and in batches.
RF-03	Automatically generate unique public codes and tokens.
RF-04	Generate QR Code and insert it into the template.
RF-05	Generate bilingual PDF according to the official template.
RF-06	Publish public validation page immediately after activation.
RF-07	Allow validation through QR Code and manual form.
RF-08	Allow reissuance with revision control and preservation of history.
RF-09	Allow cancellation with justification and authorization.
RF-10	Clearly display ACTIVE, SUPERSEDED or CANCELLED status.
RF-11	Generate reports on batches, pending items, failures, reissues and cancellations.
RF-12	Export certificate list with ID, name, type, workload, status and dates, respecting permissions.
RF-13	Store PDF hash and template version.
RF-14	Record an audit trail of administrative actions.
RF-15	Block issuance when attendance/workload does not meet the Regulation.
RF-16	Support different certificate types without changing public-validation logic.

19. NON-FUNCTIONAL REQUIREMENTS

ID	Requirement
RNF-01	Responsive portal usable on mobile, since the QR Code is the primary validation method.
RNF-02	Public validation response time suitable for academic and institutional use.
RNF-03	Availability and backups sufficient to maintain validation after the congress ends.
RNF-04	Architecture supports batch issuance without duplicate IDs or documents.
RNF-05	Compatibility with accented characters and international names in UTF-8.
RNF-06	Logs use standardized time and a time-zone reference for auditing.
RNF-07	Basic accessibility of public page: contrast, keyboard navigation and alternative text where relevant.
RNF-08	Ability to maintain future template and event versions without overwriting PACAM 2027 history.
RNF-09	Administrative exports respect the minimum necessary dataset.
RNF-10	System can be accepted in a separate environment before production.

20. API AND INTEGRATION GUIDELINES

If the system uses APIs, they must be authenticated and versioned. The public portal may consume a restricted read-only API, but must never expose endpoints returning participant lists or administrative data.

Example route	Purpose
POST /admin/certificates/batch	Create batch from approved database; restricted.
POST /admin/certificates/{id}/issue	Issue/activate certificate; restricted.
POST /admin/certificates/{id}/reissue	Create a new revision; restricted.
POST /admin/certificates/{id}/cancel	Cancel; restricted and audited.
GET /public/v/{token}	Return minimum credential-validation data.
POST /public/verify	Validate manual code; apply abuse protection.

The routes above are illustrative and may be adapted by the supplier, provided security, auditing and data-minimization controls are preserved.

21. PUBLIC PAGE MESSAGES

Status	Portuguese message	English message
ACTIVE	Certificado válido. Os dados abaixo correspondem ao registro oficial vigente do PACAM 2027.	Valid certificate. The information below matches the current official PACAM 2027 record.
SUPERSEDED	Esta versão foi substituída e não é a versão vigente do certificado.	This version has been superseded and is not the current valid version of the certificate.
CANCELLED	Este certificado não possui validade vigente. Contate a Secretaria Acadêmica do PACAM para esclarecimentos.	This certificate is not currently valid. Contact the PACAM Academic Secretariat for further information.
NOT FOUND	Não foi possível localizar um certificado com os dados informados. Verifique o código e tente novamente.	No certificate could be found with the information provided. Check the code and try again.

22. ACCEPTANCE TESTING

Test	Acceptance criterion
TA-01	Issue a test certificate with 18h50 and verify all fields/QR Code.
TA-02	Issue a certificate with partial workload and confirm the individual value is not replaced by the maximum workload.
TA-03	Validate QR Code on Android and iOS and in at least two browsers.
TA-04	Attempt validation with an invalid code and confirm no data leakage.
TA-05	Reissue after name correction and confirm SUPERSEDED status on the previous version.
TA-06	Cancel a certificate and confirm CANCELLED status appears immediately on the portal.
TA-07	Test batch concurrency to confirm no duplicate IDs.
TA-08	Confirm CPF/email/document data do not appear in the QR Code or public page.
TA-09	Verify stored PDF hash and file integrity.
TA-10	Test permissions: unauthorized role cannot cancel, change workload or issue.
TA-11	Test backup and restoration of a sample of certificates and metadata.
TA-12	Verify audit trail for issuance, reissuance and cancellation.
TA-13	Test names with accents, hyphens, apostrophes and international characters.
TA-14	Confirm public page is not indexable by search engines.
TA-15	Perform final test with the Official Certificate Template before production issuance.

23. PRODUCTION WORKFLOW

Step	Action
1	Close the attendance appeal period and consolidate the final database.
2	Academic Secretariat imports or makes available the approved batch.
3	System performs eligibility and consistency checks.
4	Resolve pending issues before issuance.
5	Academic Approver authorizes the batch.
6	System generates IDs, tokens, QR Codes, PDFs and hashes.
7	Apply institutional signature/sealing, if configured.
8	Certificates become ACTIVE and public pages are published.
9	Participants receive access to/download of the official PDF.
10	Archive issuance report in the academic dossier.
11	Subsequent reissues and cancellations follow a specific audited workflow.

24. GOVERNANCE RESPONSIBILITIES

Responsible party	Assignment
PACAM PARAGUAY E.A.S.	Institutional owner of the system and issuance policy.
Academic Committee	Approval of academic rules, exceptions and eligibility criteria.
Academic Secretariat	Registration data quality, operational processing and correction requests.
Technology Team / Supplier	Security, availability, implementation, logs, backups and technical support.
Authorized Issuance Officer	Formal approval of batches and documents according to defined governance.
Institutional Audit	Periodic review of logs, certificate samples and access controls.

25. CHANGE CONTROL

Any change affecting code format, public data, status criteria, reissue/cancellation rules, certificate fields or security architecture must result in a new version of this Specification. Technical changes that do not affect requirements may be recorded in the implementation history.

Version	Date	Change	Responsible party
1.0	07/10/2026	Initial issuance of the certificate issuance and validation system specification.	PACAM PARAGUAY E.A.S.

26. APPROVAL

The system may enter production only after functional acceptance testing, security testing proportionate to the risk, validation of the Official Certificate Template and institutional approval of this Specification.

PACAM PARAGUAY E.A.S.	Chair of the Academic Committee
Authorized representative Name: _____ Signature: _____ Date: ____/____/_____	Prof. Dr. Guilherme Weiss Freccia CREF 010199-G/SC Signature: _____ Date: ____/____/_____
Academic Secretariat	Technical System Approval
Géssica Pereira Signature: _____ Date: ____/____/_____	Name/Role: _____ Signature: _____ Date: ____/____/_____
Medical Technical Officer — Brazil	Medical Technical Officer — Paraguay
Dr. Neidson Ricart Ribeiro CRM-RJ 714470 Signature: _____ Date: ____/____/_____	Dr. Pablo H. Diniz Medical Registration PY 42.970 Signature: _____ Date: ____/____/_____

Acceptance / production-version notes: _____
_____

APPENDIX I — EXAMPLE OF PUBLIC VALIDATION RECORD

Field	Example
Status	ACTIVE
Participant	FULL NAME OF PARTICIPANT
Event	PACAM 2027 — Pan-American Congress of Aerospace Medicine
Dates	23–25/04/2027
Location	Foz do Iguaçu, Paraná, Brazil
Certified workload	18h50
Attendance	100%
Code	PACAM27-C-7K4M-Q9T6-H2VX-R8NP
Revision	01
Issued on	30/04/2027
Issuer	PACAM PARAGUAY E.A.S. — RUC 80173825-3

VALID CERTIFICATE

The page must display the institutional visual identity, but its primary function is to provide an unequivocal answer about the certificate's current validity and the essential credential data.