Generator Product Validation Request

Form PV-1: conformance and security review of a manifest-generating product before claim-signing issuance under the TLCA CP/CPS

FOR CA USE ONLY

Case No. TLCA-PV- _____ Received _____ Validation Specialist _____

PART A APPLICANT AND LINKED ORGANIZATION VALIDATION

Product validation builds on a current organization validation. If the organization does not hold an active TLCA OV, submit Form OV-1 first or alongside this request.

Organization legal name
As validated, or as submitted on Form OV-1

OV case number
TLCA-OV reference, if already assigned

Engineering contact
Name of the person able to answer technical questions

Engineering contact email

PART B PRODUCT IDENTIFICATION

Product name

Version / build under review
Validation covers this major version only

Product category (tick one):

- ☐ Desktop or mobile application
- ☐ Cloud service or API
- ☐ Camera or other capture hardware
- ☐ SDK or embeddable library
- ☐ Other (state in Part F enclosures)

Operating platforms
e.g. Windows, macOS, iOS, Android, Linux, embedded

Product documentation URL

PART C C2PA CONFORMANCE STATUS

Conforming Products List (CPL) status (tick one):

- ☐ Listed on the CPL
- ☐ Conformance application pending
- ☐ Not yet submitted

CPL entry or application ID
If listed or pending

C2PA specification version implemented

Assurance level sought
Per the C2PA requirements and the TLCA CP/CPS

PART D SIGNING AND KEY ARCHITECTURE

Where does manifest signing occur? (tick all that apply)

- ☐ On the end-user device
- ☐ Server side, operated by the applicant
- ☐ Hybrid or delegated signing service

How is the private key protected? (tick all that apply)

- ☐ Hardware security module (HSM)
- ☐ Secure enclave / TPM / secure element
- ☐ Software keystore with access controls
- ☐ TLCA managed key service

Signing authorization controls
How unauthorized or anomalous signing is prevented and det

PART E MANIFEST INTEGRITY

The product implements the following (tick all that apply):

- ☐ Hard bindings (content hashes) per the C2PA spec
- ☐ Soft binding or watermark for re-identification
- ☐ Trusted timestamps (RFC 3161)
- ☐ Revocation data embedded at signing time

Display integrity measures
How content shown to users is kept consistent with the signe

PART F ENCLOSURES

Enclose the following with your submission (tick all enclosed):

- ☐ Signing path architecture overview
- ☐ Key management summary
- ☐ CPL listing or application evidence
- ☐ Sample asset signed by this product
- ☐ Recent security assessment summary
- ☐ Other (describe):

PART G DECLARATION AND SIGNATURE

On behalf of the applicant organization, I confirm that the product is accurately described in this form and its enclosures, that its deployed signing path matches the architecture disclosed here, and that provenance data it produces will be truthful. I acknowledge that: (1) TLCA may test the product and request further evidence; (2) any claim-signing certificate is issued only for the product and version validated; (3) material changes to the signing path, key protection, or content binding must be reported to TLCA before release; and (4) misstatements are grounds for refusal of this request and for revocation under the Subscriber Agreement.

Name | Signature | Date

HOW YOUR REQUEST IS PROCESSED

1. Documentation review - a TLCA specialist checks the disclosed architecture and enclosures against the C2PA requirements.
2. Conformance check - CPL status and the product's binding, timestamping, and revocation handling are verified.
3. Technical session - a walkthrough or supervised test of the signing path may be scheduled with your engineering contact.
4. Decision - you receive the outcome by email, normally within ten (10) business days of a complete submission.

Validation covers the product and major version identified in Part B. Re-submit this form before releasing changes that affect signing, key protection, or content binding.