Verifiable Credential Readiness Checklist

A one-page gate to run before shipping credentials from a learning product. Engineering guidance, not legal advice — confirm specifics with qualified counsel.

A. Standards conformance

- [ ] Target Open Badges 3.0 on the W3C Verifiable Credentials Data Model 2.0
- [ ] Require conformance in the contract; verify against 1EdTech certification, not the sales deck
- [ ] Avoid proprietary-only formats — credentials must read in any conformant wallet/verifier

B. Issuance trigger

- [ ] Wire issuance to a real completion signal (LMS record, xAPI statement, or cmi5 result)
- [ ] Define the achievement criteria and metadata that make the credential meaningful
- [ ] For cross-LMS assessment, capture the result via LTI Advantage grade services

C. Signing & key management

- [ ] Sign each credential with the issuer's private key; publish the public key at a stable address
- [ ] Protect the private key (HSM / managed KMS); plan key rotation

D. Delivery & revocation

- [ ] Deliver to the learner's wallet via Badge Connect API (OAuth 2.0, learner-initiated)
- [ ] Ship a revocation status list (W3C Bitstring Status List) — set expiry where it applies

E. Privacy

- [ ] Support selective disclosure so a learner shares only what is needed
- [ ] Minimize personal data in the credential; keep the learner in control of sharing