Certificate of Completion

All required signers have completed this document electronically.

Document Title: SAMPLE - Fictional agency proposal
Document ID: sample-agency-proposal
Completed At: September 30, 2026 at 10:15:01 AM UTC
Content fingerprint: eb7a45da42c83c1f7ed5c2e79039a4d98a436511ac2d484fa390349fc406b471

Signing Details

Name	Email	Role	Signed At	IP Address	Method
Avery Sample	avery@example.test	signer	2026-09-30 10:15 UTC	192.0.2.20	type

Disclosure Versions Per Signer

Email	ERCD Version	Intent Text Version
avery@example.test	v2	v1

This Certificate of Completion ("Certificate") evidences the electronic execution of the document identified above by each signer listed in the Signing Details table. Plutosign produces this Certificate as a contemporaneous business record of the signing transaction.

The electronic signatures captured by Plutosign on this document are valid and enforceable under the U.S. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §7001 (validity of electronic signatures) and §7006 (definitions), and the Uniform Electronic Transactions Act as enacted in each U.S. state, including §7 (legal recognition), §9 (attribution), and §12 (retention). Under 15 U.S.C. §7001(a)(1), a signature, contract, or record may not be denied legal effect or enforceability solely because it is in electronic form.

For each signer Plutosign recorded: identity by possession of a unique signing link delivered to the signer's email address of record; IP address as observed by Plutosign's servers at signing; browser and operating system information at signing; the timestamp of each interaction (view, sign, decline, delegate) in Coordinated Universal Time; the version of the Electronic Records Consent Disclosure each signer accepted before signing; and the verbatim version of the affirmation text each signer was shown immediately above the Sign button at their signing event. These items appear in the tables above and form an append-only, hash-chained audit log; the hash chain makes deletion or re-ordering of recorded events forensically detectable.

Document integrity. The content fingerprint identifies application document content or signing configuration at sending; it is not a hash of the completed PDF bytes. A separate stored SHA-256 hash, when available, identifies the signed PDF including its embedded certificate. That byte hash is provided on the separately downloaded Certificate of Completion and can be checked against SHA-256 recomputed over the complete signed PDF. It does not hash the separately generated certificate. Plutosign treats any mismatch as a high-severity incident, and a mismatch does not, of itself, invalidate the record.

Limitations. Plutosign captures electronic signatures meeting U.S. ESIGN/UETA standards. Plutosign does NOT, in this Certificate, represent that the signatures meet the European Union eIDAS Advanced or Qualified Electronic Signature standards, the PAdES long-term-validation profile, or industry-specific frameworks such as HIPAA, FINRA, or FDA Title 21 CFR Part 11. The signed PDF does not contain an embedded PKCS#7 / CMS cryptographic signature.

This Certificate is generated automatically and is not a legal opinion as to the enforceability of the underlying transaction. Specific

FICTIONAL SAMPLE - NOT A CUSTOMER AGREEMENT

Certificate statements (continued)

questions about enforceability of a signed document should be directed to qualified counsel in the relevant jurisdiction.

Certificate template version: v1

FICTIONAL SAMPLE - NOT A CUSTOMER AGREEMENT

Signed PDF integrity

Stored signed PDF SHA-256:

990970b7a55be4ccb3eb19dbe4da42b2cb16dda74a6406b209daf536d37457f7

Recompute SHA-256 over the complete downloaded signed PDF, including its embedded certificate, and compare it with this stored hash.

This hash identifies the signed PDF, not this separately generated Certificate of Completion. It is the stored reference; generating this certificate does not re-verify the current file bytes.

The content fingerprint, when shown, identifies application document content or signing configuration at sending. It is separate from the signed PDF byte hash.

FICTIONAL SAMPLE - NOT A CUSTOMER AGREEMENT

Captured Signatures

Avery Sample
avery@example.test



FICTIONAL SAMPLE - NOT A CUSTOMER AGREEMENT

Document History

Timestamp (UTC)	Event	Actor	IP Address
2026-09-30 10:00:00 UTC	Created	Robin Sample	192.0.2.10
2026-09-30 10:05:00 UTC	Sent for signature	Robin Sample	192.0.2.10
2026-09-30 10:10:00 UTC	Viewed	Avery Sample	192.0.2.20
2026-09-30 10:12:00 UTC	Consent accepted	Avery Sample	192.0.2.20
2026-09-30 10:15:00 UTC	Signed	Avery Sample	192.0.2.20
2026-09-30 10:15:01 UTC	Completed	Robin Sample	192.0.2.10

FICTIONAL SAMPLE - NOT A CUSTOMER AGREEMENT