

Testing checklist: e-signature service

Source: <https://howtotestaproduct.com/how-to-test/e-signature/>

Generated: 2026-10-07. Licence: CC BY 4.0.

☐ 1. release smoke tests

Done when: On every build, a two-signer test envelope completes, the test consumer signer sees the electronic records disclosure before the document opens, its certificate lists each signer's email, authentication method, IP address and timestamp, and the signed PDF shows a valid signature.

Risks: regulatory-penalty, data-corruption. Tool class: browser automation. Usually run by: QA engineer.

☐ 2. regression suite

Done when: The certificate, consent and tamper cases rerun on every release, and a missing certificate field or a passed tamper case blocks the release.

Risks: regulatory-penalty, data-corruption. Tool class: test management. Usually run by: QA engineer.

☐ 3. compliance checks

Done when: Legal signs off the consent text, certificate fields and retention period against ESIGN and, for life-science customers, the 21 CFR Part 11 audit trail rules, and access to completed documents is limited to the named signers and the sender.

Risks: regulatory-penalty, data-breach. Tool class: test management. Usually run by: product manager.

☐ 4. end-to-end functional tests

Done when: A first-time consumer signer sees the electronic records disclosure and gives consent before the document opens, and withdrawing consent switches that signer to paper.

Risks: regulatory-penalty. Tool class: browser automation. Usually run by: QA engineer.

☐ 5. accessibility testing

Done when: A screen-reader user and a keyboard-only user find every signature and initial field, review all entries and confirm before the final sign action.

Risks: accessibility-liability. Tool class: accessibility checker. Usually run by: accessibility specialist.

☐ 6. unit tests

Done when: In the test report, every unchanged sample document passes signature validation and every sample with a changed byte or page fails it.

Risks: data-corruption. Tool class: unit framework. Usually run by: developer.

☐ 7. security scanning

Done when: The scan of the signing pages, document storage and API has no open high findings.

Risks: data-breach. Tool class: DAST scanner. Usually run by: security specialist.

☐ 8. penetration testing

Done when: A tester with a forwarded or edited signing link cannot open another signer's document, an access code or SMS check cannot be skipped by replaying the link.

Risks: data-breach. Tool class: proxy. Usually run by: security specialist.

☐ 9. data integrity and migration testing

Done when: Editing a completed document makes signature validation fail, and editing a document mid-flow restarts signing for everyone who already signed.

Risks: data-corruption. Tool class: data validation. Usually run by: QA engineer.