Initiator State Machine (Policy-Aware)

idle → sendingMessageA : initiate

sendingMessageA → waitingMessageB : send ok

waitingMessageB
deadline enforced

invalidSig / parse

MessageB valid

timeout

established
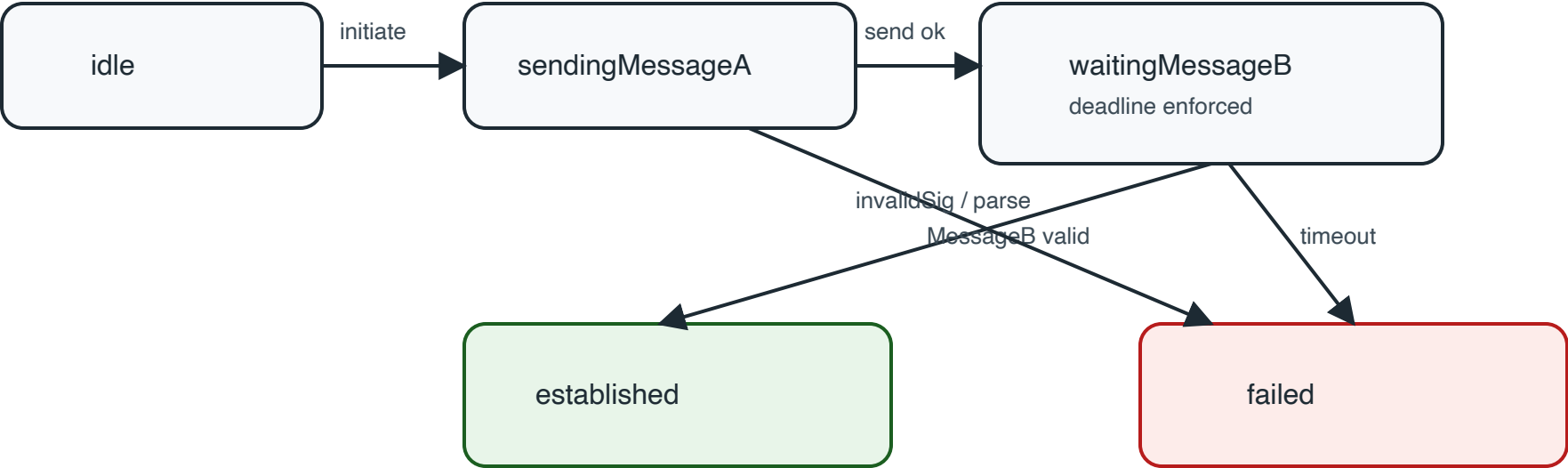
failed

Policy Gates on Failure Edges

strictPQC: suiteNotSupported / pqcUnavailable ⇒ fail (no classic fallback)

default: allowed fallback only for explicit whitelist errors

All failure edges emit SecurityEvent.handshakeFailed