

T402 Threat Model & Mitigations

Threats

Mitigations

Replay Attack

Nonce + Deadline + Domain

Signature Forgery

ECDSA/Ed25519 + On-chain

Man-in-the-Middle

HTTPS + Signed Parameters

Double Spending

Blockchain Finality

Insufficient Payment

Amount in Signed Data

Wrong Recipient

payTo in Signed Data

Expired Authorization

On-chain Deadline Check

Fund Redirection

Facilitator Cannot Alter payTo

All mitigations are protocol-level, requiring no trust in Facilitator