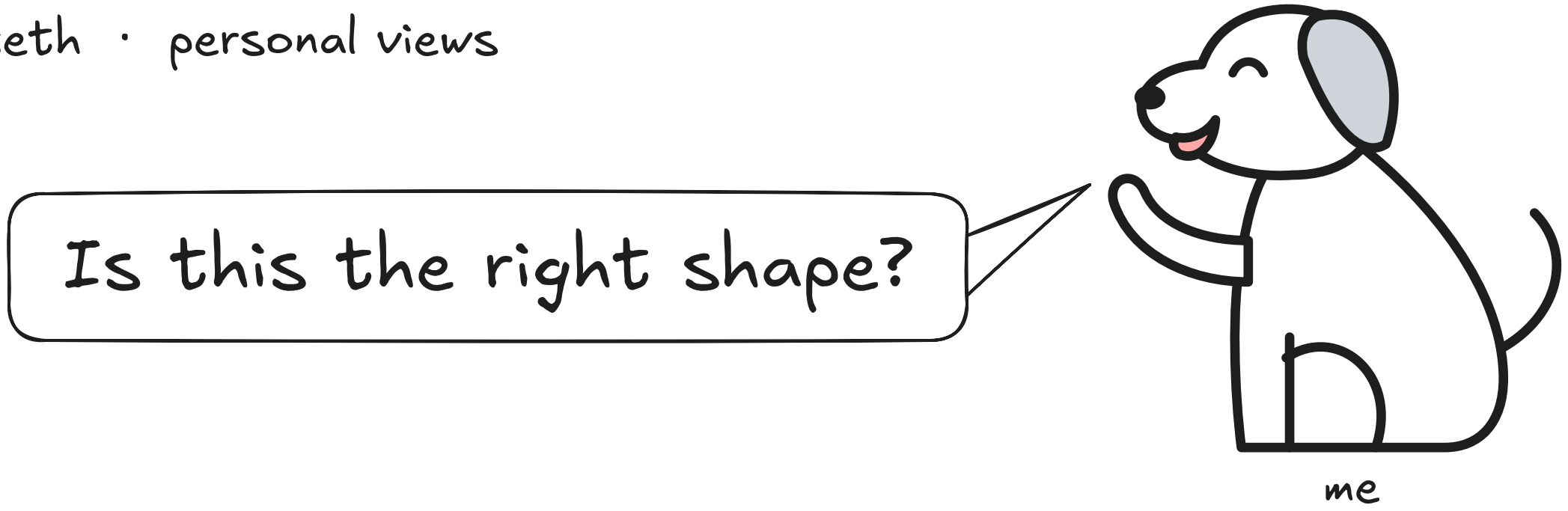
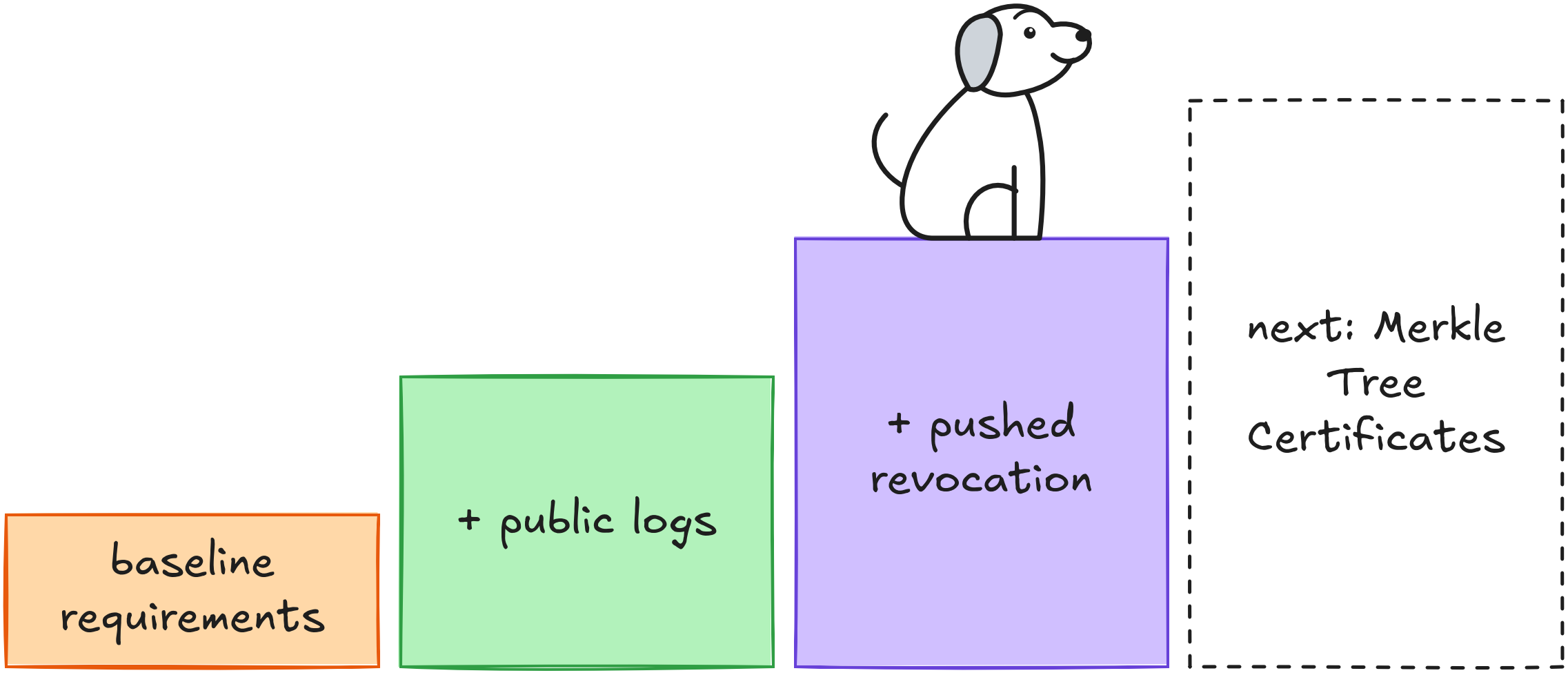
MTC architecture

draft-sanketh-plants-mtc-architecture-00

sanketh · personal views

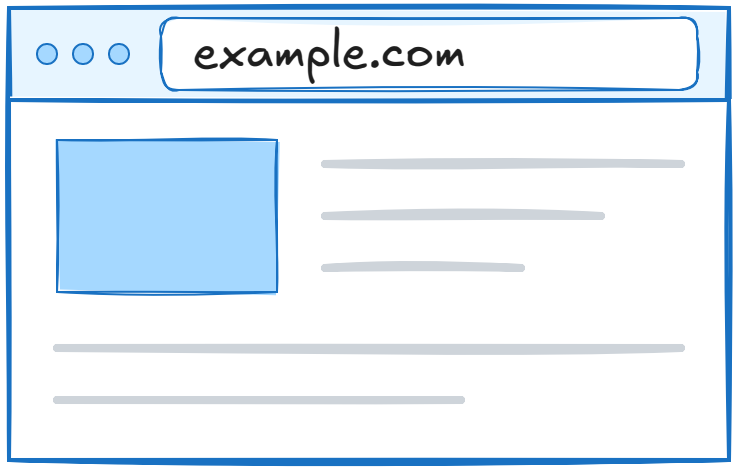


We've come a long way

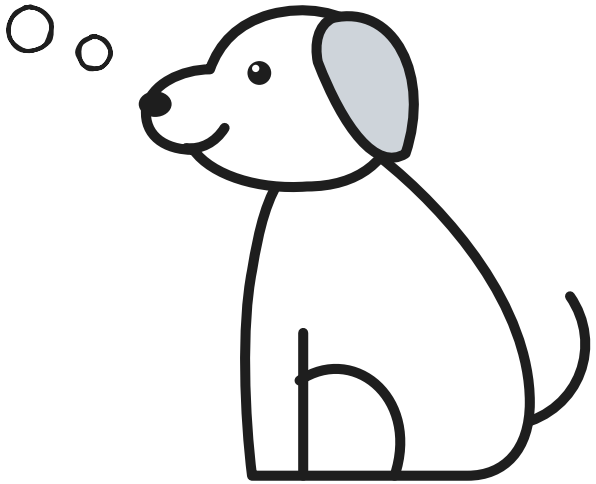


We expect more

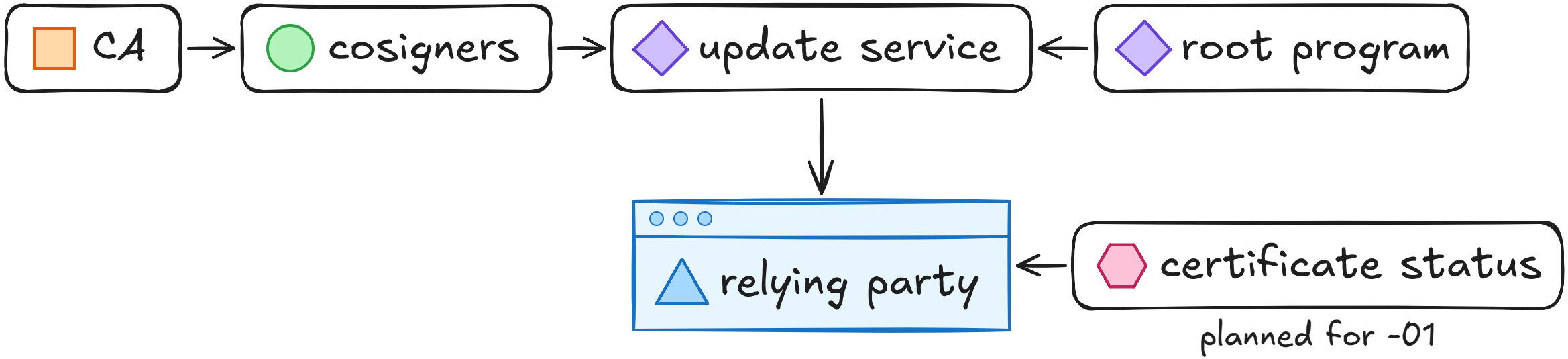
a website
just opens



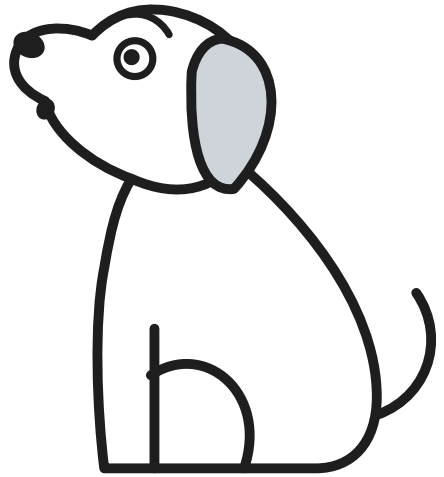
- [ ] it was issued after validation
- [ ] it is in a public log
- [ ] the public log is the same for everyone
- [ ] it has not been revoked



We rely on many parties



gets	relies on
☐ it was issued after validation	■
☐ it is in a public log	● ◆
☐ the public log is the same for everyone	● ◆
☐ it has not been revoked	◆ ⬢



We should write it down

☐ it is in a public log ○ ◇

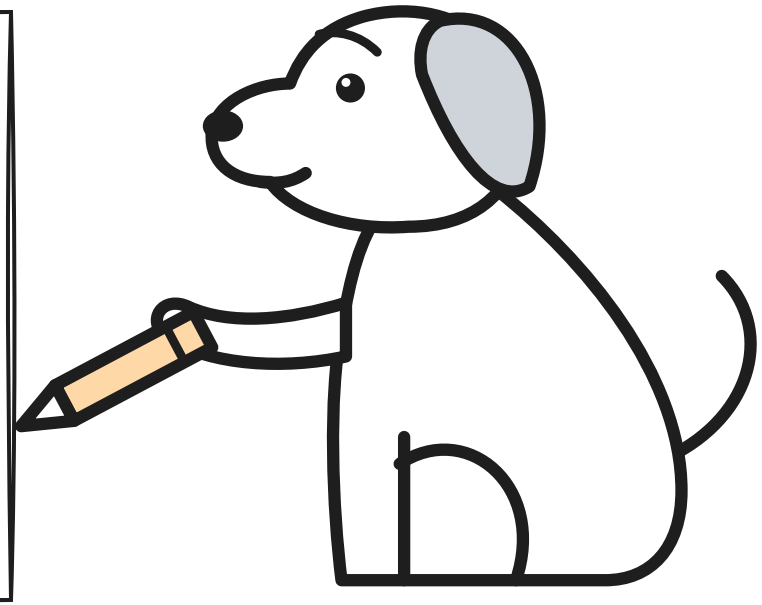
↓

if ◇ policy requires a mirror

and ○ that mirror is faithful

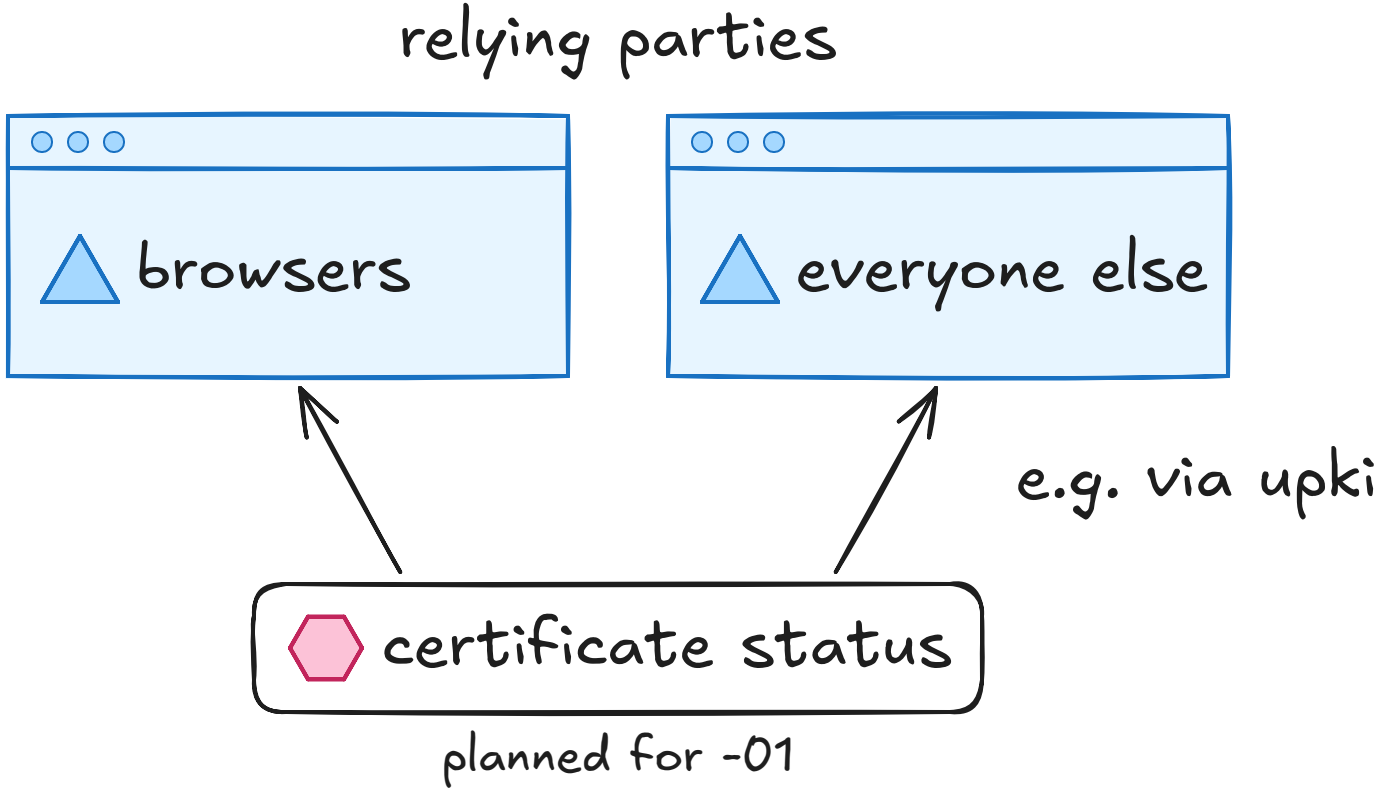
---

then ☑ a mirror stored the entry before acceptance



× 5 guarantees

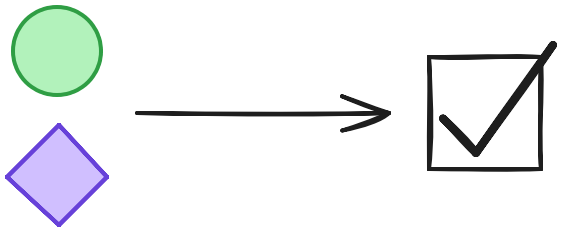
We want this for everyone





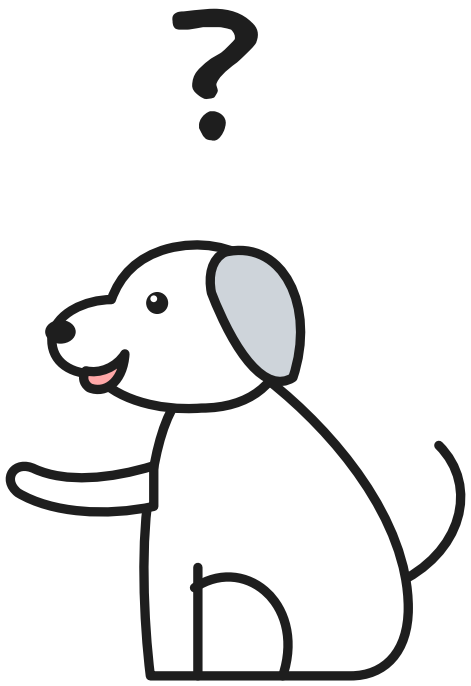
Which shape do we want?

my proposal

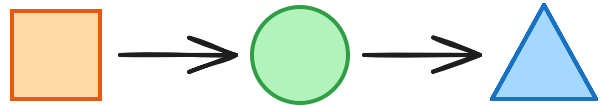


guarantees, and what they depend on

long · low-level · pedantic



the alternative



components and flows

much shorter

reviewers and co-authors welcome · PLANTS list

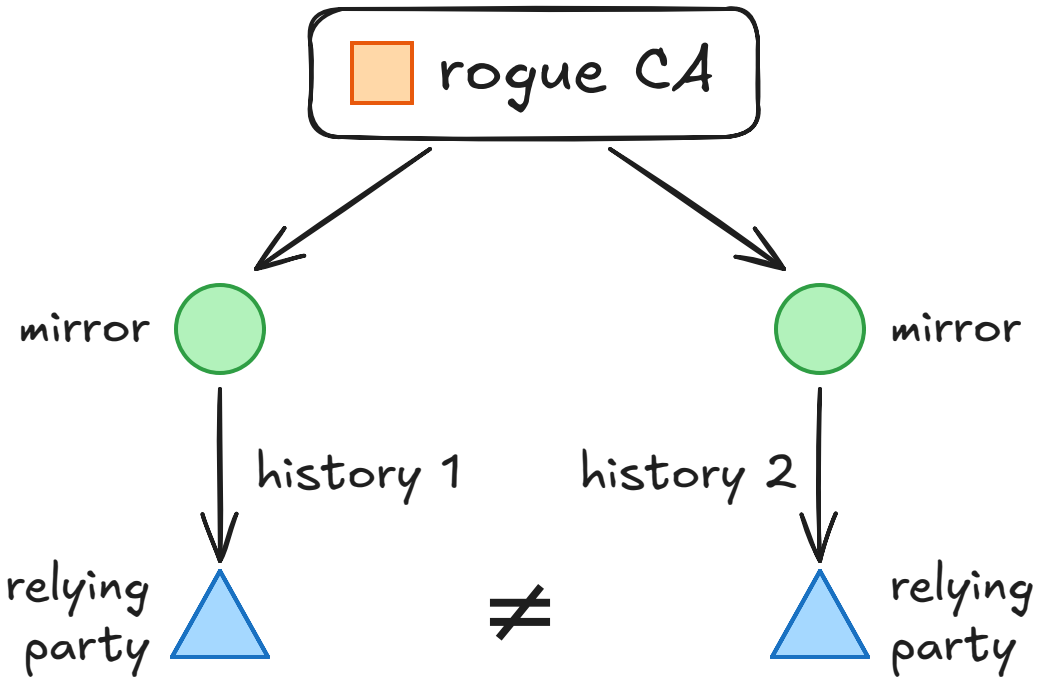
read first: Table 1 and Section 2

Backup: Table 1 of the draft

Guarantee	What the relying party learns	Rests on	Against a rogue CA
G1 Certification	the CA key certified exactly this entry	the CA cosigner key, if the policy requires it	holds unless the key is extracted
G2 Recording	a mirror stored the entry before acceptance	a supporting mirror faithful to the log	holds
G3 Consistency	relying parties agree on the entry at each index	a faithful supporting cosigner shared by every pair of acceptances (the intersection condition)	holds
G4 Revoked ranges	an installed range rejects on both paths, and stays installed	the update key, numbered complete updates with a version floor, and the installation check	holds for the positions named
G5 Validated configuration	each trusted subtree was validated under the policy in effect	local validation, or an honest update service; the installation check and retention rule	holds

Backup: detect or prevent?

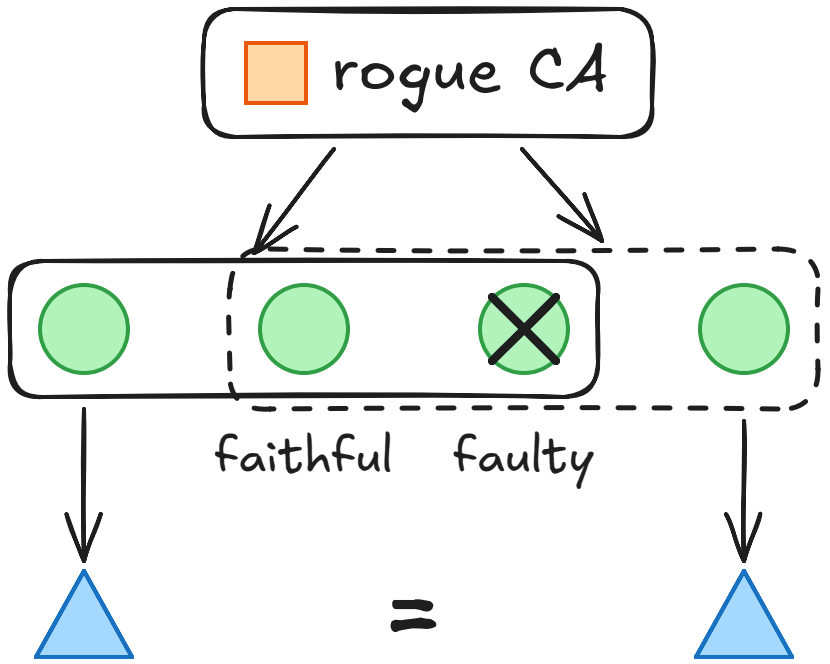
CA + any one mirror



a split view can be detected, not prevented

detection depends on monitoring

CA + 3 of 4 mirrors



a split view is prevented, at a cost in bytes

the draft's intersection condition: $2k > n + f$
here: at most one faulty mirror ($f = 1$)

Sources

slide		
1	my draft	draft-sanketh-plants-mtc-architecture-00
2	baseline requirements	CA/Browser Forum, TLS Baseline Requirements (2026)
2	public logs	RFC 6962 and RFC 9162, Certificate Transparency
2	CRLite	Larisch et al., CRLite, IEEE S&P 2017
2	eMudhra incident	Mozilla Bugzilla, bug 2083449 (October 2026)
2	Merkle Tree Certificates	draft-ietf-plants-merkle-tree-certs-08
4	"additional state"	the same draft, Section 12.2.1
4	cosigners and mirrors	C2SP tlog-cosignature, tlog-witness, tlog-mirror
4	certificate status	Salz and Gray, Merkle Tree Revocation (this session)
5	Tamarin	tamarin-prover.com
6	upki	github.com/rustls/upki
6	landmark distribution	draft-gray-plants-mtc-ldp
backup	root program policy	Chrome Quantum-resistant Root Program Policy, v0.4.0

everything else: the reference list in Section 10 of my draft