IETF Web PKI

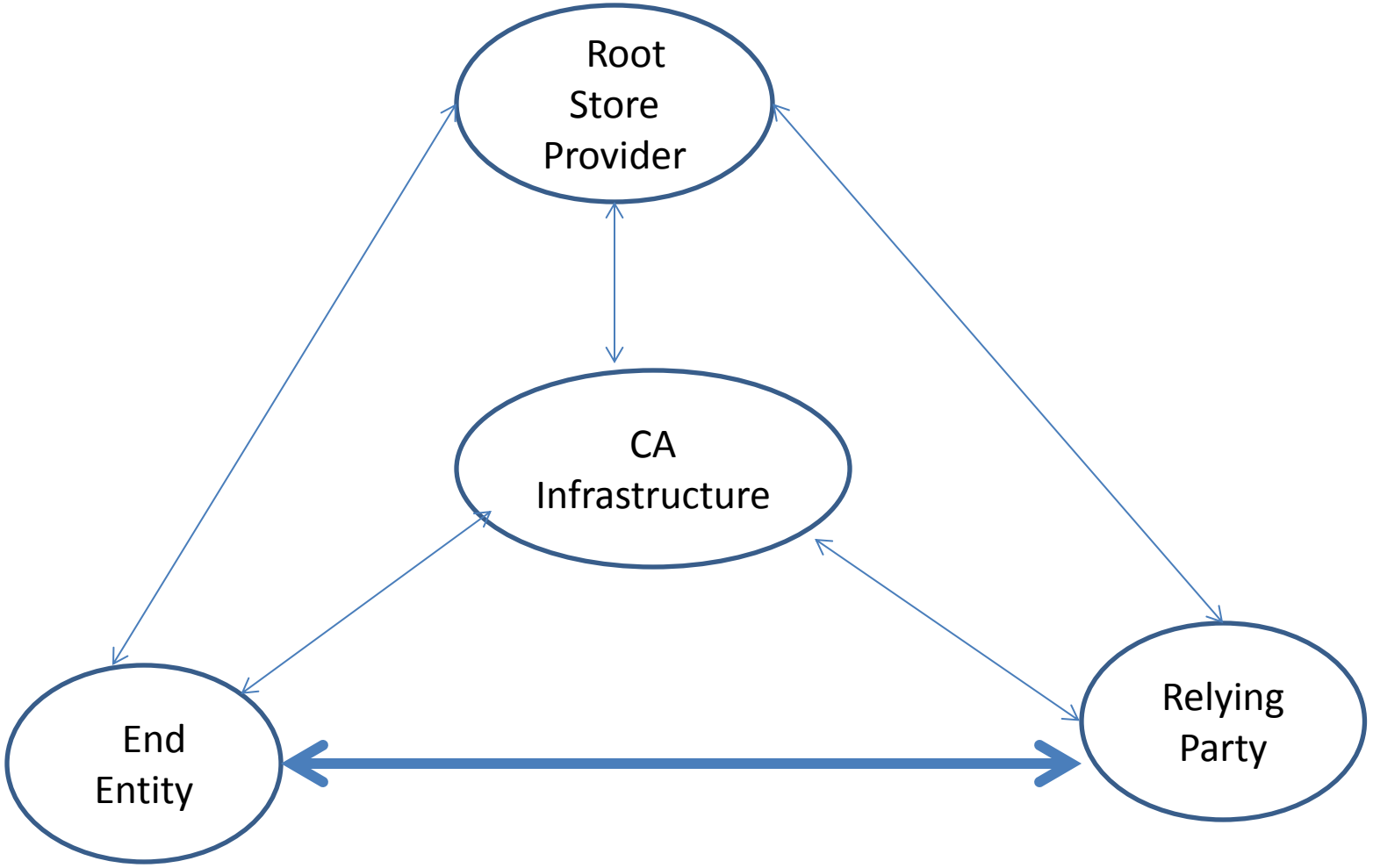
Trust models of the web PKI

March 2013

Introduction

- Cover basic trust model
- Cover all variants to the basic trust model

Basic Trust Model



Basic trust model

- Certificate-using product has root store containing root CA public keys
- Certificate policy associated with product
- Root CAs issue certificates to own issuing CAs
- Issuing CAs issue certificates to applicants
- Issuing CAs issue certificate status
- Certificate user accepts policy of certificate-using product
- All CAs audited per certificate policy

Trust model variants

1. Certificate-using product adopts root store
2. Certificate-using product uses OS root store
3. Certificate-using product uses trust service status list
4. Certificate holder certificates issued by root CA
5. Root CA cross-certifies another root CA
6. Issuing CA is an affiliate
7. Registration authority is an affiliate

Trust model variants cont'd

8. Root CA is operated by a government
9. Certificate user directly trusts issuing CA
10. Certificate user directly trusts certificate holder key
11. Certificate holder operates issuing CA
12. Certificate holder sources management of issuing CA
13. Certificate holder manages RA