

Web PKI Trust Model

Bruce Morton

WPKOPS, IETF 88

Trust Model

- WG draft has been released
- Addresses basic Trust Model
- Discusses roles of Root Store, CA, Subscriber and Browser
- Discusses variants to the roles
- What else is needed?

Root and Trust Anchor

- Plan to use Root (Root Certificate, Root CA)
 - This is the reference Web PKI policy and standards from: Apple, CAB Forum, Google, Microsoft, Mozilla, Opera, Oracle and WebTrust
- Plan to use Trust Anchor where a non-root is used as an authority
 - Subscriber adds CA
 - Subscriber directly trusts entity key

Next Steps

- WG to review and provide comments
- Create updated release