Building Online Trust

Jeremy Rowley
DigiCert
The Great Divide: Perspective
Initiatives

- **OCSP Stapling**
  - Better revocation
  - Faster handshakes
  - Require mustStaple
- **Certificate Authority Authorization**
  - Prevents fraud
  - Easy to implement
- **Certificate Transparency**
  - Detects mis-issuance
  - Prevents government MITM
- **Key Pinning**
  - Limits issuance
  - Potential bricking problem
New Developments and Discussions

• Technology Changes
  • 1024 bit deprecation
  • SHA2 requirement
  • Internal name phase out
  • SSL beyond logins and shopping carts

• Implementations
  • CAA deployment
  • CT deployment

• Projects
  • EV certificate expansion
  • Performance working group
  • Code signing baseline standards
  • Certificate lifecycles
  • OCSP Stapling push
Building Trust

CAs
- Better issuance practices
- Better standards
- New technology

Browsers
- Enforce good practices
- Set high standards
- Deploy new technology

Server Software Providers
- TLS 1.2
- OCSP Stapling
- Other enhancements

ICANN community
- Accurate WHOIS
- Push changed information
The Path Ahead

Improved Online Security
- New technologies
- Better standards & enforcement

Bumps in the Road
- Legacy devices/software
- Old paradigms

Chicken vs. Egg
- Early, voluntary adoption vs. mandatory

Transparency, Accountability & Self-Selection
- More visibility into certificate issuance
- Enhanced information
Questions?

Contact me:
Jeremy.rowley@digicert.com

Resources:
• https://www.cabforum.org/
• https://casecurity.org/