WPKOPS
TLS Stack
Document Preview

Adam Langley
Paul Hoffman

What the charter says

- How the TLS stack deals with PKI, including varying interpretations and implementation errors, as well as state changes visible to the user.
- The working group's goal is to describe how the Web PKI "actually" works in the set of browsers and servers that are in common use today.

Common PKIX issues for the TLS stack

- No chain to a trust anchor
  - Subcategory: no chain at all
- Non-matching names
- Expired certificates
- Expired intermediates, even “expired” trust anchors

Less common PKIX issues for the TLS stack

- Revoked certificates
- Uncommon field and extension issues
  - Also covered in *Field and Extension Processing for Certificates, CRLs, and OCSP*, but this document covers the state changes visible to the user

TLS protocol considerations for interoperability

- Document several TLS protocol tweaks that common SSL libraries use in order to achieve interoperability

How are these issues visible to the user

- Alerts that are dealt with and then disappear
- Long-lived icons and indicators in the navigation bar

PKI-related choices made by the browser user

- Some dialogs give choices, other are simply informational
- Some make users go a few layers deep in the UI