EMU and DANE

Jim Schaad
August Cellars
EMU TLS Issues

• Trust Anchor
• Matching PKIX cert to EMU Server Name
• Certificate Revocation Checking
  – CRLs
  – OCSP
DANE Review

• Use DNS as alternative or secondary trust framework

• New Records for cert/public key information
  – Naming: _<port>._<protocol>..<Domain Name>
  – Matching:
    • Trust Anchor (Root)
    • CA
    • EE
DANE Stapling

• Addresses Trust Anchor Issue
• Addresses matching Certificate Name
• Create a new _teap._emu.<Domain Name> DNS record set
• Use existing TLSA records
• Build list of DNSSEC records and pass in TLS extension
• If necessary – new record for name matching
OCSP Stapling

- Addresses certificate chain validation
- Pass OCSP responses in TLS extension
- Need to establish trust in OCSP responder
  - Maybe fix with DANE record
  - Maybe fix by returning CRLs
  - Maybe fix by making the Trust Anchor the OCSP responder
Work List

- Need DANE naming convention done in EMU
- Need DANE stapling TLS extension – Probably done in DANE
- Need OCSP stapling TLS extension done in TLS
  – Draft-pettersen-tls-ext-multiple-ocsp-03.txt
Questions?