Must Staple OCSP
Objective

• Stapling OCSP responses to TLS is efficient
  – If OCSP token is stapled, HTTP lookup is saved
  – But a HTTP get is required otherwise
    • Even if the valid server staple
    • Browsers will not hard fail if lookup fails
Solution

• Flag in Cert and CSR specifies must be stapled’
  – Clients can now hard fail if OCSP token not stapled

• Applicability
  – Revocation for administrative reasons (99.99%)
    • Works
  – Revocation due to mis-issue
    • Unlikely attacker will request flag
    • But other controls (e.g. CAA) designed to address this