THE OVERALL CLASSIFICATION OF THIS BRIEFING IS:
DRAFT

ALIE BECKER, REBECCA GUTHRIE, MIKE JENKINS
CENTER FOR CYBERSECURITY STANDARDS
CYBERSECURITY COLLABORATION CENTER
NATIONAL SECURITY AGENCY
CHANGES SINCE DRAFT-BECKER-GUTHRIE-CERT-BINDING-FOR-MULTI-AUTH-02

4.1 language:
- becker-guthrie-02: RelatedCertificate extension is a list of entries ...
- lamps-00: RelatedCertificate extension is an octet string that contains the hash of a single end-entity certificate

3.1 language:
- becker-guthrie-02: accessLocation value URI SHOULD be a dataURI ...
- lamps-00: accessLocation value URI MAY be a dataURI

lots of nits!
OPEN QUESTIONS FOR LAMPS WG

- In RelatedCertificate attribute:
  - Currently using BinaryTime for freshness
  - Use another type (or something else)?

- In RelatedCertificate attribute:
  - Currently includes IssuerAndSerialNumber
  - Hash entire certificate instead?

- Hash of certificate in RelatedCertificates extension:
  - Currently MUST match hash used to sign certificate that contains extension
  - Add option to use different hash algorithms?
Context
Draft specifies how to use RelatedCertificates extension if it is included in PQ cert. Some in WG are interested in having the option to use the extension in the traditional cert as well.

Proposal
Generalize draft to specify attribute and extension for cert A and cert B rather than PQ cert and traditional cert.

Does the group support this proposal?