DRAFT HISTORY

DRAFT-BECKER-GUTHRIE-CERT-BINDING-FOR-MULTI-AUTH

March 21 -00 version uploaded
April 4 presented at LAMPS Interim
June 29 -01 version uploaded
General Changes:

- Changed title of document to “Related Certificates for Use in Multiple Authentications within a Protocol”
- Added Section 1.1: Overview to describe use case for document
- Narrowed the scope of the document to focus on two certificate case instead of an arbitrary number of certificates
Changes to relatedCertRequest Attribute:

- Changed attribute name to relatedCertRequest
- Added requestTime (BinaryTime [RFC6019]) to ensure freshness
- Added locationInfo (AccessDescription [RFC5280]) to point to location of other certificate
- Changed signature to a digital signature over the concatenation of certID with requestTime
Changes to RelatedCertificate Extension:

• Changed extension name to RelatedCertificate
• Changed hash to be of entire certificate instead of certID