ChangeLog SM-Beta-PKI

Aktualisiert: 2015-11-10

Einleitung

Dieses ChangeLog wird im Auftrag des BSI veröffentlicht und enthält abgestimmte Informationen zu Klarstellungen und Korrekturen bzgl. der aktuell gültigen Spezifikationen. Soweit nicht anders angegeben, sind diese Anpassungen ab dem Zeitpunkt der Veröffentlichung gültig und verbindlich und werden in das nächste Release der jeweiligen Spezifikation übernommen.

Des Weiteren wird in diesem Dokumente über konkrete Systemänderungen bei der SM-Beta-BSI-Root- und -Sub-CA informiert.

Struktur

Das Dokument wird fortlaufend, umgekehrt chronologisch erweitert. Die Einträge sind einheitlich wie folgt aufgebaut:

Datum des Eintrags [Format: JJJJ-MM-DD]
Art des Eintrags [Systemänderung / Information]

Überschrift
Erklärender Kurztext

Ursprung, Quelle, Referenz

Konkretisierung der Umsetzung, Auswirkung (optional)

Inhalt

2015-11-10
Information / Systemänderung

Geänderte Validierung von Zertifikatsrequests mit Autorisierungssignatur SM-Beta-BSI-Sub-CA

Ein Zertifikatsrequest mit Autorisierung durch eine dritte Partei
muss in EncapsulatedContentInfo entweder den content type
id-CertReqMsgs-with-outerSignature oder id-CertReqMsgs enthalten.
Daraus folgt: signedAttrs MUSS gemäß RFC 5652 verwendet werden, da
die TR-03109-4 als content type von EncapsulatedContentInfo nicht id-data,
sondern id-CertReqMsgs bzw. id-CertReqMsgs-with-outerSignature verlangt.

- TR-03109-4, Version 1.2, Stand 09.12.2016

* Es wurde eine Valdierung bzgl. der Verwendung von SignedAttr implementiert.
  Requests, die SignedAttrs nicht berücksichtigen, werden vom System abgelehnt.