SRQ - Specification Related Question

SRQ-ID: 1108

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	OID als Algorithmen Identifier für RSA
zu Dokument / Datei (evtl. ersetzt SRQ)	gemSpec_Krypt
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	5.1.1

Stichwort: OID als Algorithmen Identifier für RSA.

Frage:

In dem Dokument gemSpec_Krypt muss für die RSA Schlüssel in X.509 Zertifikaten eine OID aufgenommen werde, die innerhalb der X.509 Zertifikate als SubjectPublicKeyInfo aufgenommen wird. Bislang ist keine OID angegeben. Welche OID muss verwendet werden?

Betrifft:

Gültig ab	16.10.2008	Verbindlichkeit	normativ
Zulassungsrelevanz			
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	1.5.0	voraussichtl. Zeitpunkt	offen
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Für alle RSA Schlüssel in Abschnitt 5.1.1 und Unterabschnitten gilt als OID für die Verwendung des Schlüssels 1.2.840.113549.1.1.1