SRQ - Specification Related Question

SRQ-ID: 1107

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Referenz für ISO10126 Padding
zu Dokument / Datei (evtl. ersetzt SRQ)	gemSpec_Krypt
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	

Stichwort: Referenz für ISO 10126 Padding

Frage:

Innerhalb des Dokumentes gemSpec_Krypt wurde auf Padding gemäß ISO Standard 10126 verwiesen. Der ISO Standard 10126 wurde kürzlich vom Ausschuss ISO TC68 widerrufen, da er auf der Verwendung des nicht mehr als sicher eingestuften DES Algorithmus basiert. Welches Paddingverfahren soll stattdessen verwendet werden?

Betrifft:

Gültig ab	16.10.2008	Verbindlichkeit	informativ
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:

Zur Beantwortung der Frage wurde der folgende Abschnitt in [gemSpec_Krypt] aufgenommen und alle Referenzen auf ISO10126 Padding verweisen nun auf diesen Abschnitt.

5.3.1 Zufalls-Padding für Blockchiffrieralgorithmen

Viele XML-Frameworks und Standards verwenden das Padding Verfahren ISO-10126. Der zugehörige ISO Standard 10126 wurde kürzlich vom Ausschuss ISO TC68 widerrufen, da er auf der Verwendung des nicht mehr als sicher eingestuften DES Algorithmus basiert. Eine Referenzierung dieser Beschreibung ist aus diesem Grund nicht mehr möglich, obwohl das Verfahren weiterhin zulässig und gewünscht ist. Bislang existiert kein eigener Standard, in dem das Zufalls-Padding beschrieben wird und der als Basis für die Referenzierung dienen kann.

Das in ISO-10126 definierte Verfahren ist identisch zu dem in [XMLEnc] Abschnitt 5.2 beschriebenen Paddingverfahren. Auch wenn [XMLEnc] XML spezifisch ist, ist das in Abschnitt 5.2 beschriebene Zufalls-Padding auch für nicht XML Daten anwendbar. Das in [XMLEnc] Abschnitt 5.2 beschriebene Paddingverfahren gilt aus diesem Grund als normative Beschreibung des Zufalls-Paddings. Die Anpassung der Implementierung aufgrund dieses Wechsels ist nicht notwendig, da sich lediglich die Referenz, nicht aber das Verfahren selbst geändert hat. Sollten sich aus der nachfolgenden Beschreibung Abweichungen zu den genannten Verfahren ergeben, so sind diese nicht beabsichtigt.

Das referenzierte Paddingverfahren verwendet Zufallszahlen zur Auffüllung des Ciphertextes. Die Vertraulichkeit der Daten hängt nicht von der Qualität des Zufalls ab und es werden keine Anforderungen an die Qualität der Zufallszahlen gestellt.