SRQ - Specification Related Question

SRQ-ID: 1110

Betrifft:

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Zufallszahlen bei der Schlüsselerzeugung
zu Dokument / Datei (evtl. ersetzt SRQ)	gemSpec_Krypt
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	5.2

Stichwort: Zufallszahlen bei der Schlüsselerzeugung

Frage:

In Kapitel 5.2 der gemSpec_Krypt wird ausführlich auf Zufallsgeneratoren eingegangen. Es fehlt aber ein Hinweis darauf, an welcher Stelle Zufallszahlen benötigt werden und insbesondere, ob besondere Anforderungen an Zufallszahlen bei der Erzeugung kryptografischer Schlüssel bestehen. Welche Anforderungen an Zufallszahlen bestehen im Zusammenhang mit der Erzeugung kryptografischer Schlüssel?

Betrifft:

Gültig ab	07.04.2011	Verbindlichkeit	normativ
Zulassungsrelevanz			
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version	1.4.0	voraussichtl. Zeitpunkt	10.07.2008
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Zur Beantwortung der Frage wurden folgende Ergänzungen in [gemSpec_Krypt] aufgenommen.

1) Aufnahme des folgenden Abschnitts

5.2.3 Erzeugung von Zufallszahlen

Der nachfolgende Abschnitt entspricht inhaltlich dem Abschnitt 3.4 aus [BSI-TR03116], wurde jedoch leicht angepasst.

Die Erzeugung von Zufallszahlen ist erforderlich für die Erzeugung von:

- Challenges in Authentisierungsprotokollen,
- zufälligen Paddingbits bzw. Saltwerten sowie
- kryptographischen Schlüsseln bzw. Systemparametern.

Grundsätzlich können für die Erzeugung von Zufallszahlen physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden. Entsprechend des gewählten Generators sind die Anforderungen gemäß [AIS20] für Pseudozufallszahlengeneratoren und [AIS31] für physikalische Zufallszahlengeneratoren einzuhalten.

Die Erzeugung von kryptographischen Schlüsseln und Systemparametern wird in Abschnitt 5.2.4 behandelt.

Für die Erzeugung einer Challenge in Authentisierungsprotokollen und von zufälligen Padding- und Saltbits sind die folgenden Anforderungen einzuhalten:

- Ein Pseudozufallszahlengenerator muss mindestens ein K3-DRNG mit Stärke der Mechanismen „Hoch“ im Sinne der AIS 20 [AIS20] sein. Bis Ende 2009 ist ein Seed von mindestens 80 Bit erforderlich; ab Anfang 2010 muss der Seed mindestens 100 Bit Entropie besitzen.
- Ein physikalischer Zufallszahlengenerator muss mindestens ein P2-TRNG mit Stärke der Mechanismen „Hoch“ im Sinne der AIS 31 [AIS31] sein.

5.2.4 Schlüsselerzeugung

Der nachfolgende Abschnitt entspricht inhaltlich dem Abschnitt 3.5 aus [BSI-TR03116], wurde jedoch leicht angepasst.

Bei der Schlüsselerzeugung für Sicherheitsverfahren werden Zufallszahlen benötigt, an die entsprechende kryptographische Anforderungen zu stellen sind, um die Sicherheit des Gesamtsystems zu gewährleisten. Für die Schlüsselerzeugung können physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden. Für Zufallszahlen zur Schlüsselerzeugung gelten die Anforderungen gemäß [ALGCAT], Kapitel 4 „Erzeugung von Zufallszahlen“. D.h. insbesondere: Bis Ende 2009 muss jeder erzeugte Schlüssel mindestens 80 Bit Entropie besitzen; ab Anfang 2010 muss jeder erzeugte Schlüssel mindestens 100 Bit Entropie besitzen. Über die Anforderungen gemäß [ALGCAT] hinaus gilt Folgendes:

Es wird empfohlen, zur Schlüsselerzeugung einen physikalischen Zufallszahlengenerator zu verwenden, der dann ein P2-TRNG mit Stärke der Mechanismen und Funktionen

„Hoch“ im Sinne der AIS 31 [AIS 31] sein sollte, und schon vor Anfang 2010 zu gewährleisten, dass jeder erzeugte Schlüssel mindestens 100 Bit Entropie besitzt.

Pseudozufallszahlengeneratoren für die Erzeugung von Verschlüsselungsschlüsseln müssen K4-DRNGs mit Stärke der Mechanismen und Funktionen „Hoch“ im Sinne der AIS 20 [AIS20] sein. Physikalische Zufallszahlengeneratoren für die Erzeugung von Verschlüsselungsschlüsseln müssen P2-TRNGs mit Stärke der Mechanismen und Funktionen „Hoch“ im Sinne der AIS 31 [AIS31] sein. Für symmetrische Verschlüsselungsschlüssel muss die Seedlänge mindestens gleich der Schlüssellänge sein und die Entropie des Seeds i. wes. so groß wie seine Länge, derart, dass die Entropie des Schlüssels i. wes. seiner Länge entspricht. Jeder asymmetrische Verschlüsselungsschlüssel muss mindestens 100 Bit Entropie besitzen; empfohlen wird aber auch hier eine wesentlich höhere Entropie von mindestens 120 Bit. Bei hybrider Verschlüsselung wird empfohlen, die Entropie für den asymmetrischen Schlüssel mindestens in der Größenordnung der Entropie des symmetrischen Schlüssels zu wählen. Diese Anforderungen begründen sich in der langfristigen Speicherung verschlüsselter Dokumente. Hierbei handelt es sich um verschlüsselte Dokumentationen, die auf zentralen Servern gespeichert werden.

5.2.4.1 Symmetrische Schlüssel

Die Erzeugung von symmetrischen Schlüsseln erfolgt durch die Erzeugung „kryptographisch sicherer“ Zufallszahlen (im Sinne obiger Ausführungen zu [ALGCAT] Kapitel 4 inklusive einer Nachbehandlung der Zufallszahlen zur Schlüsselformatierung (z.B. Anpassung an die Schlüssellänge).Im Weiteren gelten die folgenden algorithmenspezifischen Anforderungen:

Tabelle 1: Anforderung an die Generierung symmetrischer Schlüssel

Algorithmus	Anforderung an den Algorithmus zur Schlüsselgenerierung
3TDES	Die Verwendung von schwachen sowie von semi-schwachen Schlüsseln als Teilschlüssel eines 3TDES Schlüssels (s. z. B. [SP800-67], Kapitel 3.4.2) ist praktisch auszuschließen. Darüber hinaus sind je zwei Teilschlüssel verschieden zu wählen.
AES	Für den AES sind weder schwache noch semi-schwache Schlüssel bekannt, es gibt keine Einschränkung bei der Schlüsselauswahl (vgl. [FIPS 197], Kapitel 6.2)

5.4.2.2 Asymmetrische Schlüssel

Für die Erzeugung von asymmetrischen Schlüsseln werden „kryptographisch sichere“ Zufallszahlen (im Sinne obiger Ausführungen zu [ALGCAT] Kapitel 4 benötigt. Im Weiteren gelten die algorithmenspezifischen Anforderungen aus [ALGCAT]

2) Ergänzung der referenzierten Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[AIS20]	BSI (1999): Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1 http://www.bsi.bund.de/zertifiz/zert/interpr/aisitsec.htm (zuletzt geprüft am 06.02.07)
[AIS31]	BSI (2001): Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1 http://www.bsi.bund.de/zertifiz/zert/interpr/ais31.pdf (zuletzt geprüft am 06.02.07)