FaQ-ID: 0054

Betrifft (wird vom FLS (optional vom Erfasser) ausgefüllt):

Themenkreis	Architektur und übergreifende Dokumente
Schlagwort	Güte Zufallszahlengeneratoren
zu Dokument / Datei	[gemSpec_Krypt], SRQ 1110
Version	1.3.0
Bezug (Kap., Abschnitt, Tab., Abb.)	5.2.3

Stichwort: Güte Zufallszahlengeneratoren

Frage:

Welche kryptographische Güte besitzen die in [FIPS-186-2+CN1] und [ANSI-X9.31] aufgeführten deterministischen Zufallszahlengeneratoren?

Betrifft (wird vom PB ausgefüllt):

gültig ab (Datum)	22.11.2011	Verbindlichkeit	informativ
zusätzlicher Download-Link zu Datei:			
Herstellerbefragung durchgeführt		am	
Wird behoben mit Version		voraussichtl. Zeitpunkt	
Anmerkungen:			
Status	☒ erfasst ☒ intern abgestimmt ☐ extern abgestimmt ☐ zurückgezogen ☒ freigegeben ☐ eingearbeitet in Folgeversion		

Antwort:

Die Sicherheit eines deterministischen Zufallszahlengenerators (DRNGs) hängt maßgeblich von drei Faktoren ab:

- von der Entropie des Seeds,
- vom algorithmischen Anteil (generelles Design) und
- dem Schutz des inneren Zustands (und der zur Ausgabe vorgesehenen Zufallszahlen).

Der Nachweis, dass der algorithmische Anteil eines DRNGs den Anforderungen einer bestimmten Funktionalitätsklasse genügt, kann schwierig und aufwändig sein. Deshalb wurde das BSI gebeten, die DRNGs in [FIPS-186-2+CN1] und [ANS-X9.31] in Bezug auf die kryptographische Güte ihres algorithmischen Anteils zu bewerten.

Das Ergebnis ist:

A) [FIPS-186-2+CN1]: Lässt man in dem DRNG aus Appendix 3.1 (S. 16f.) in Schritt 3c bzw. in dem DRNG aus Algorithmus 1 (Change Notice 1, S. 72f.) in Schritt 3.3 den Term "mod q" weg, so werden gleichverteilte 160-Bit Zufallszahlen bzw. 320-Bit Zufallszahlen erzeugt (vgl. Abschnitt „General Purpose Random Number Generation“ (Change Notice 1,S.74)).
Beide DRNGs sind dann

1) algorithmisch geeignet für die Klasse K4 [AIS-20-1999] und

2) erfüllen die algorithmischen Anforderungen aus DRG.3 [AIS-20-2011].

Ob eine konkrete Implementierung eines dieser DRNG bspw. Teil der Klasse DRG.3 ist, bleibt im Einzelfall zu prüfen, da dazu u. a. auch Fragen über die Initialisierung zu beantworten sind (vgl. (DRG.3.1) [KS2011]).

Das BSI empfiehlt bei den Zufallsgeneratoren aus [FIPS-186-2+CN1] nach Möglichkeit SHA-256 [FIPS-180-3] anstatt SHA-1 zu verwenden. Folgt man der Empfehlung, so ist der Algorithmus dem entsprechend zu adaptieren.

B) [ANSI-X9.31]: Der Zufallsgenerator aus Appendix A.2.4 ist

1) algorithmisch geeignet für die Klasse K3 [AIS-20-1999] und

2) erfüllt die algorithmischen Anforderungen aus DRG.2 [AIS-20-2011].

Literaturverzeichnis:

[AIS-20-1999]
W. Schindler: Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators. Version 1.0, 02.12.1999, ehemalige mathematisch technische Anlage zur AIS20,
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Zertifierung/Interpretation/AIS20_Functionality_Classes_Evaluation_Methodology_DRNG.pdf?__blob=publicationFile

[AIS-20-2011]
AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 2.0, 19.09.2011,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/ais20_pdf.pdf?__blob=publicationFile

[ANSI-X9.31]
National Institute of Standards and Technology, NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 31, 2005.
http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf

[FIPS-180-3]
Federal Information, Processing Standards Publication 180-3, Specifications for the SECURE HASH STANDARD, Oktober 2008
http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf

[FIPS-186-2+CN1]
FIPS 186-2 - National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 – Appendix 3.1 unter der Beachtung des Change Notice 1, vom 5. Oktober 2001
http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2-change1.pdf

[KS2011]
W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, Version 2.0, September 2011
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Zertifierung/Interpretation/AIS31_Functionality_classes_for_random_number_generators.pdf?__blob=publicationFile