Bundesamt
für Sicherheit in der
Informationstechnik

Anwendungshinweise und Interpretationen zum Schema (AIS)

AIS 31, Version 3

Stand:	**15.05.2013**
Status:	**Verbindlich**
Thema:	**Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren**
Herausgeber:	**Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas**
Verteiler:	**Anerkannte Prüfstellen[1]** **Bundesnetzagentur (BNA)** **Private Bestätigungsstellen[2] über BNA** **BSI-intern** **Internet-Seite des BSI**

Änderungshistorie:

Version	Datum	Status	Änderung	Bemerkung
2.0	19.09.11	Verbindlich	Generelle Überarbeitung	
3.0	15.05.13	Verbindlich	- Kap. 1, 3 und 4 angepasst - Kap. 5 eingefügt - Kap. 6 upgedated - Deckblatt angepasst - Feldfunktionen korrigiert	

1 Alle Evaluatoren in den vom BSI für Evaluierungen nach ITSEC oder CC anerkannten Prüfstellen

2 Alle Zertifizierer der privaten Bestätigungsstellen, die Bestätigungen nach dem deutschen Signaturgesetz herausgeben

Inhaltsverzeichnis

1. Hintergrund

1 Physikalische Zufallszahlengeneratoren werden in vielen Anwendungsfällen benötigt, bei denen die Sicherheit von Geheimnissen auf deren Zufälligkeit beruht und die daher nicht oder nur sehr schwer zu erraten sind. Dazu gehört insbesondere die Schlüsselgenerierung bei symmetrischen oder asymmetrischen Verschlüsselungsverfahren.

2 Im Zuge der der Evaluierung von Produkten, bei denen die Zufälligkeit von Geheimnissen eine wesentliche Rolle der Sicherheitsfunktionalität darstellt (z.B. bei der Schlüsselgenerierung von Signaturschlüsseln durch Sichere Signaturerstellungseinheiten), ist eine Analyse und Bewertung des Zufallszahlengenerators notwendig.

3 Die Evaluationsmethodologie der Common Criteria [CEM31] oder der ITSEC [ITSEM] liefern hierzu keine ausreichende Information. Eine weitgehend einheitliche Evaluierungsmethodik durch alle nach ITSEC oder CC evaluierenden, zertifizierenden oder bestätigenden Stellen ist daher notwendig.

4 Das BSI hat im Dokument [AIS31V1] einen Ansatz zur Beschreibung und Evaluierung von physikalischen Zufallszahlengeneratoren formuliert. Nachdem die darin beschriebene Methodologie über mehrere Jahre hinweg angewendet wurde, erfolgte eine weitgehende Überarbeitung des Grundlagendokuments in [KS2011] sowie der Methodologie (siehe [RNGEV], [PTGEV] und [PTGDEV]).

2. Fundstellen

1. [ITSEC]: 3.23
2. [ITSEM]: 6.C.34
3. [CC31]: Teil 2, Anhang E1, Anhang E2
4. [CEM31]: Kap. 11, Anhang B.2
5. [CC23]: Teil 1, Kap. 1, Abs.6
6. [CEM23]: Kap. 6.9.1.2, 7.10.2.2, 8.10.2.2, Anh. B.9 Abs. 1886

3. Anwendungshinweise und Interpretation

5 Die Methodologie zur Evaluierung von physikalischen Zufallszahlengeneratoren im deutschen Schema setzt sich aus mehreren Dokumenten zusammen:

1. Das Dokument [RNGEV] beschreibt Anforderungen in Bezug auf Zufallszahlengeneratoren, die bei der Evaluierung eines Security Targets bzw. Protection Profiles zu beachten sind, sowie generelle Regelungen zur Verwendung von Zufallszahlengeneratoren im deutschen Schema. Es beinhaltet darüber hinaus eine zusammenfassende Beschreibung von Dokumenten im deutschen Zertifizierungsschema, die sich mit der Evaluierung von Zufallszahlengeneratoren befassen. Neben den physikalischen Zufallszahlengeneratoren, auf die sich diese AIS bezieht, gehören dazu noch die deterministischen und die nicht-physikalischen echten Zufallszahlengeneratoren (s. [AIS20] oder [KS2011], Kapitel 4).
2. Das Dokument [KS2011] beschreibt zum einen die mathematische Grundlagen, Tests und Beispiele für Zufallszahlengeneratoren. Zum Anderen beinhaltet es die

Klasse FCS_RNG als explizites SFR zur Formulierung von Anforderungen an Zufallszahlengeneratoren in der Terminologie der CC sowie die im deutschen Schema vorgegebenen, vordefinierten RNG-Klassen, die in Security Targets bzw. Protection Profiles zu verwenden sind. Im Vergleich zu [AIS31V1] haben sich die Formulierung der expliziten SFRs in der Terminologie der CC sowie die vorgegebenen RNG-Klassen geändert, wobei [KS2011] eine Abbildung der neuen RNG-Klassen auf die RNG-Klassen aus [AIS31V] beinhaltet.

3. Das Dokument [PTGEV] ist ein Template, das im Rahmen der Evaluierung von physikalischen Zufallszahlengeneratoren von Evaluatoren entsprechend ausgefüllt werden muss. Es beinhaltet in Form von Workunits die Arbeitsschritte, die analog zu [CEMV31] jeweils mit weitergehenden Erläuterungen versehen sind.
4. Das Dokument [PTGDEV] ist für Hersteller von Produkten bestimmt, deren Sicherheitsfunktionalität die Erzeugung von physikalischen Zufallszahlengeneratoren umfasst. Es beschreibt, welche Informationen ein Hersteller zur Verfügung stellen muss, damit ein Evaluator die entsprechende Evaluierung durchführen kann.

4. Bemerkungen

6 Mit dieser AIS werden die Dokumente [RNGEV], [KS2011] und [AIS31V1] in den formalen Rahmen eingegliedert, den das deutsche CC-Zertifizierungsschema für Anwendungshinweise und Interpretationen vorsieht. Die Dokumente werden damit im Zertifizierungsschema eindeutig referenzierbar.

7 Die zu verwendende Beschreibung und Evaluierung von physikalischen Zufallszahlengeneratoren wird durch folgende Dokumente definiert, die bei widersprüchlichen oder fehlenden Festlegungen in der Rangfolge dieser Aufzählung gelten:

1. [RNGEV]
2. [KS2011]
3. [PTGDEV]
4. [PTGEV]
5. [AIS31V1]

8 Abweichungen von dieser Rangfolge müssen vorher mit der Zertifizierungsstelle abgestimmt werden.

9 Eine Überarbeitung und Ergänzung ist auf der Grundlage weitergehender Erkenntnisse oder Erfahrungen aus der Anwendung geplant. Insbesondere bei Widersprüchen oder fehlenden Festlegungen wird das BSI neue Versionen der Dokumente veröffentlichen. Ziel des BSI ist es mittelfristig alle Regelungen aus [AIS31V1] in andere Dokumente (siehe Aufzählungspunkte 1 bis 4) zu überführen.

10 Elektronisches Format: Die Dokumente [RNGEV], [KS2011], [PTGEV], [PTGDEV] und [AIS31V1] sind im PDF-Format verfügbar.

5. Inkrafttreten der AIS

11 Die AIS ist grundsätzlich ab sofort gültig und bei allen Zertifizierungsverfahren verbindlich anzuwenden.

6. Referenzdokumente

CC31 Common Criteria for Information Technology Security Evaluation
Comprising Parts 1-3:
Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012
Part 2: Security functional components, Version 3.1, Revision 4, September 2012
Part 3: Security assurance components, Version 3.1, Revision 4, September 2012

CEM31 Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 4, September 2012

CC23 Common Criteria for Information Technology Security Evaluation
Comprising Parts 1-3:
Part 1: Introduction and General Model, Version 2.3, August 2005
Part 2: Security Functional Requirements, Version 2.3, August 2005
Part 3: Security Assurance Requirements, Version 2.3, August 2005

CEM23 Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005

ITSEC Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Version 1.2, Juni 1991

ITSEM Information Technology Security Evaluation Manual (ITSEM), Version 1.0, September 1993

ITSEC-JIL ITSEC Joint Interpretation Library (ITSEC JIL), Version 2.0, November 1998

BSI-7125 BSI-Zertifizierung: Verfahrensbeschreibung, BSI 7125

AIS 32 Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema

AIS31V1 Ein Vorschlag zu: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.1, 25.09.2001

RNGEV Evaluation of random number generators, Version 0.10

KS2011 W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, Version 2.0, September 18, 2011

PTGDEV Developer evidence for the evaluation of a physical true random number generator, Version 0.8, February 28, 2013

PTGEV Evaluation Report as part of the Evaluation Technical Report, Part B, ETR-Part, True Physical and Hybrid Random Number Generator, Version 0.7, February 28, 2013

AIS20 Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013